Susan S Bies: Corporate governance

Speech by Ms Susan S Bies, Member of the Board of Governors of the US Federal Reserve System, at the Institute of Internal Auditors Conference, Philadelphia, Pennsylvania, 7 May 2003.

* * *

Good morning. Thank you for the invitation to speak to the Institute of Internal Auditors (IIA) membership at this timely and important conference. My remarks this morning will focus on issues relating to corporate governance and underscore the critical role of internal auditors in the Sarbanes-Oxley era.

Introduction

Over the past two years, we have been shocked by the headlines announcing corporate governance or accounting problems at a variety of companies, such as Enron, Worldcom, and HealthSouth. As we read these headlines, the question that comes to mind is, "What were the underlying deficiencies in the internal control processes of these companies that rendered their governance practices ineffective?" As the details about the scandals have been made public, it has become clear that they are examples of breakdowns in internal controls that all of us learned about in Accounting and Auditing 101. Why, then, have we seen so many headlines highlighting corporate governance and accounting problems? The explanation is that these companies lost track of the basics of effective corporate governance--internal controls and a strong ethical compass to guide the organization. While most companies have effective governance processes in place, these events remind all of us of the importance of doing the basics well.

Internal control framework

After an earlier series of corporate frauds, the National Commission on Fraudulent Financial Reporting, also known as the Treadway Commission, was created in 1985 to make recommendations to reduce the incidence of these frauds. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission issued a report titled *Internal Control--Integrated Framework* that has become the most referred to standard on internal control.

If one re-reads that report, the lesson of returning to focus on the basics becomes clear. 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*
- *Compliance with applicable laws and regulations.*

The COSO framework was the model considered when the Federal Deposit Insurance Corporation Improvement Act was enacted in 1991. FIDICIA 112 requires that management report annually on the quality of internal controls and that the outside auditors attest to that control evaluation.

Control assessments

COSO requires all managers to, at least once a year, step back from their other duties and evaluate risks and controls. Each manager should consider the current and planned operational changes, identify the risks, determine the appropriate mitigating controls, establish an effective monitoring process, and evaluate the effectiveness of those controls. Managers are then supposed to 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 their responsibility. The results of this process are ultimately to be reported to the audit committee of the board of directors. In the case of banks, 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. 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 the risks and controls from various lines of business when formulating business strategies. But not all corporations and boards consider risk as a part of their annual strategic planning or other evaluation processes. The 2002 survey of 178 corporate directors conducted jointly by you (the IIA) and the National Association of Corporate Directors showed that directors are 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 there are companies out there that 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 the responsibility for setting the tone regarding their corporations' risk-taking and establishing an effective monitoring program. They also have the 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 FDICIA annual report can be an effective tool for the auditor to communicate risks and control processes to the audit committee. Members of that committee should use the reports to be sure their understanding of business strategy, changing business processes, management reorganizations, and positioning for future growth are done within the context of a sound system of internal controls and governance. The report should identify those areas for which priorities should be established to strengthen the effectiveness of internal controls.

Indeed, beyond legal requirements, boards of directors of all firms should periodically assess where management, which has stewardship over shareholder resources, stands on 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? Internal auditors should ensure that processes are in place for employees to raise ethical and control concerns in an environment that protects them from retribution from affected managers.

Internal controls

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 lessons learned from those headline cases cited violations of the fundamental tenets of internal control, particularly those pertaining to operating risks. Based on the headlines, it seems that boards of directors, management, and auditors desperately 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 management are simple. Directors do not serve full time, so it is important that the auditor establish an annual agenda for boards and audit committees 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. The challenge of the auditor is to ensure that the internal audit staff has the expertise and ongoing training to meet the specific and changing risks of the organization.

Before a company moves into new and higher risk areas, the boards of directors, management, and the auditors need assurances that they have the tools in place to ensure that the basics of sound

governance are being adhered to. Many of the organizations that have seen their reputations tarnished in the past two years have also neglected to consider emerging conflicts of interest when the organization adds new products and lines of business. It is important that if a customer service or control function must be done in an independent, fiduciary, or unbiased manner relative to other activities, appropriate firewalls are in place before the product or activity begins, to ensure that the integrity of the process is not compromised.

Boards of directors are responsible for ensuring that their organizations have an effective audit process and that internal controls are adequate for the nature and scope of their businesses. The reporting lines of the internal audit function should be such that the information that directors receive is impartial and not unduly influenced by management. Internal audit is a key element of management's responsibility to validate the strength of internal controls.

Internal controls are the responsibility of line management. Line managers must determine the acceptable level of risk in their line of business and must assure themselves that the combination of earnings, capital, and internal controls is sufficient to compensate for the risk exposures. Supporting functions such as accounting, internal audit, risk management, credit review, compliance, and legal 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 auditors conducting the reviews can speak freely. Directors must demand that management fix problems promptly and provide appropriate evidence to internal audit confirming this.

While we have been focused on mid-sized and larger organizations, internal controls are also important to smaller organizations. Many failures of community banks are due to breakdowns in internal controls, thus increasing operational risk. In smaller organizations, the segregation of duties and ability to hire expertise for specialized areas is more difficult. But smaller organizations still must go through the process of assessing risks and controls and ensuring that they are appropriate for the culture and business mix of the organization. A faster growing financial services company in riskier lines of business will need a stronger, more formalized system of internal controls than a well-established company engaged broadly in traditional financial services.

Internal audit

The Federal Reserve is very supportive of independent internal audit functions at financial services companies. Earlier this year, along with the other federal banking agencies, we issued an amended policy statement on the internal audit function that called for each regulated institution to have an internal audit function that is appropriate to its size and the nature and scope of its activities. This amended policy statement addresses several different areas of internal audit in general, including

Director and senior management responsibilities. In our view, the board of directors and senior management cannot delegate the responsibility for having an effective system of internal control. Certain portions of the implementation of the control system may be conducted by more junior management, but this does not relieve the board and senior management of responsibility for the design and effectiveness of the system.

We also describe the four areas that we believe must be included in the internal audit function. Those areas address the structure, management, scope, and communications of the internal audit function.

Structure. The internal audit function must be independent from day-to-day operations. The structure section of the policy statement specifically states, "The manager of internal audit should report directly to the board of directors or its audit committee, which should oversee the internal audit function." It also states that the board should develop objective performance criteria to evaluate the work of internal audit. The auditor should meet periodically with the chair of the audit committee outside of formal meetings to review audit plans and the results of audits, determine issues of concern to the committee, and create an agenda that engages audit committee members in effective oversight of the internal audit process.

Management, staffing, and audit quality. Directors should assign responsibility for the internal audit function to an internal audit manager. The audit manager should be responsible for control risk assessments, audit plans, audit programs, and audit reports. The management section states that institutions should follow professional standards, such as the IIA's standards. One of the most

important roles of the auditor is to identify emerging areas of risk and report management's progress in implementing mitigating controls and monitors of changing exposures.

Scope. We take the position that frequency and extent of internal audit review and testing engaged in during the audit "should be consistent with the nature, complexity, and risk of the institution's on- and off-balance-sheet activities." We also state that the audit committee should at least annually review and approve the internal audit manager's control risk assessment, the scope of the audit plan, including how much the manager relies on the work of an outsourcing vendor, and adherence to the audit plan. At the end of each audit plan year, a critical assessment of the validity of the initial assumptions should be made and appropriate re-allocations of resources scheduled for the new plan.

Communications. We advise the board and senior management to foster communication with the internal auditors so that they are aware of pertinent issues and the board is aware of all significant matters. Just as the auditor should have regular communications with the audit committee, the auditor should have senior-enough stature within the organization to be aware of significant initiatives and be able to influence management as needed to adopt appropriate control processes.

The policy statement advises banking organizations that the auditor independence rules of the Securities and Exchange Commission apply to institutions covered by FDICIA 112. As a result, internal audit outsourcing to the external auditor is prohibited for such institutions. Nonpublic, non-FDICIA 112 institutions are encouraged to adhere to this prohibition.

Sarbanes-Oxley Act

Now let's turn to Sarbanes-Oxley. At its core, the Sarbanes-Oxley Act is a call to get back to the basics that we have been discussing. Since you have other speakers on the program who are planning to provide you with an update on the status of rulemakings currently under way, I won't cover the act's provisions in any detail. However, as I'm sure you know, the IIA research foundation published a Sarbanes-Oxley status report just last month. The summary was entitled *Assessment Guide for U.S. Legislative, Regulatory, and Listing Exchanges: Requirements Affecting Internal Auditing*. As I recall, the guide compares the key requirements of the

- Sarbanes-Oxley Act of 2002,
- Proposed and final Securities and Exchange Commission rules and interpretations related to the Act, and
- Regulations proposed by the listing exchanges and associations.

Although the guide identifies 58 separate provisions that affect internal auditing, I think it is also important to stress the fundamental underlying sentiment of the act. **Simply stated, the current status quo for corporate governance is unacceptable and must change.**

This message is applicable to both public and private companies alike and affects everyone within a company.

- The message for boards of directors is: Uphold your responsibility for ensuring the effectiveness of the company's overall governance process.
- The message for audit committees is: Uphold your responsibility for ensuring that the company's internal and external audit processes are rigorous and effective.
- The message for CEOs, CFOs, and senior management is: Uphold your responsibility to maintain effective financial reporting and disclosure controls and adhere to high ethical standards. This requires meaningful certifications, codes of ethics, and conduct for insiders that, if violated, will result in fines and criminal penalties, including imprisonment.
- The message for external auditors is: Focus your efforts solely on auditing financial statements and leave the add-on services to other consultants.
- The message for internal auditors is: You are uniquely positioned within the company to ensure that its corporate governance, financial reporting and disclosure controls, and risk-management practices are functioning effectively. Although internal auditors are not specifically mentioned in the Sarbanes-Oxley Act, they have within their purview of internal control the responsibility to examine and evaluate all of an entity's systems, processes, operations, functions, and activities.

If you are feeling a little sensitive or uneasy right now as an internal auditor, that's good. Because the question you should be asking yourself is whether you are up to this challenge presented by Sarbanes-Oxley.

What are the challenges for internal auditors in the Sarbanes-Oxley era?

First, internal auditors must step up to the plate and help corporate risk officers and managers reinvigorate the risk assessment and control process over financial reporting and now, under Sarbanes-Oxley, other public disclosures.

Before becoming a Federal Reserve Governor, I was at various times the auditor and the CFO of a bank. As a result of this experience, I'm very familiar with the types of internal control risk assessments that are required by FDICIA 112. For the past decade, I've worked with both internal and external auditors to ensure that the risk management and reporting functions at banks produce reliable and accurate information. Recently, the Fed has been looking at the management reports on internal controls for several banks that have had significant breaks in internal controls. From these banks, we have identified several whose FDICIA 112 processes were not effective. A closer look at these situations indicates that management had essentially put this process on autopilot. Further, the external auditor had not done an effective review of the basis of management's report.

Before you say, "That could not happen at my company," let me remind you how we started our discussion today. In each of the cases involving banks, the internal auditor seemed to be content with the loss of vigor in the process and the external auditor was apparently satisfied to simply collect a fee. This type of situation is totally unacceptable. Further, as the organization evolves over time by offering new products, changing processes, outsourcing services, complying with new regulations, or growing through mergers, the controls need to be modified to reflect the changes in risks. In some cases, the controls failed with respect to newer risk exposures that were not identified, or growth put strains on existing control processes that were not suitable for a larger organization.

Section 302 of Sarbanes-Oxley requires senior management to assess and report on the effectiveness of disclosure controls and procedures as well as on internal controls for financial reporting. This broader certification addresses controls and procedures related to public disclosure, including financial information, such as Management's Discussion and Analysis, that is reported outside of the financial statements. To address these new disclosure control certifications, companies are undertaking steps to

- Set up disclosure committees composed of the CFOs, the corporate risk officers, in-house counsels, chief internal auditors, and other members of senior management,
- Identify the controls and procedures necessary for gathering information and preparing periodic reports,
- Determine whether the controls and procedures capture the appropriate information for disclosures and enable the necessary information to be recorded, processed, summarized, and reported on a timely basis, and
- Establish an audit program that includes quarterly evaluations of the assessment, control activities, information and communication, and monitoring elements of the disclosure control framework.

We have not had enough experience to assess the effectiveness of these new certifications. However, for any framework to be successful, the CEOs and CFOs need to establish strong controls for maintaining and enforcing procedures for collecting, processing, and disclosing information in their securities filings.

Now here's the challenge for you. **First, as the company's internal auditor, you should be proactive in ensuring that your company's risk assessment and control process over financial reporting and disclosures are vigorous.** In this regard

- If you are an internal auditor of a financial services company that is subject to FDICIA 112, you should seize this opportunity to take a fresh, objective look at the risk assessment and control process in your company's internal control framework.
- If you are an internal auditor of a publicly traded financial services company, you now have the same responsibility, since section 404 of Sarbanes-Oxley is modeled after FDICIA 112.

However, don't assume that what was acceptable in the past is good enough for the future. Remember, there is a tendency for an organization to go on autopilot if the internal auditor is not vigilant. As for the certifications required by section 302 of Sarbanes-Oxley, you should be part of the disclosure committee. You should also establish a robust audit program for the company's disclosure controls framework.

- If you are an internal auditor of a nonpublic financial services company, you should view this as an opportunity to convince the board and management to adopt a rigorous self-assessment process for controls covered by sections 302 and 404 of Sarbanes-Oxley as a best practice.

Second, internal auditors must be willing to sacrifice everything to maintain their independence within the organization.

You are not going to be effective unless you report directly to the audit committee. Your company's entire quality assurance and monitoring program will be tainted if you are not accountable to the audit committee. Most audit committees already know this and are looking for ways to strengthen this area. If the audit committee asks you for recommendations on how to improve independence, your typical response should be that the test for any recommended change is whether it makes management more accountable for the ongoing effectiveness of internal controls and makes the internal audit function more effective in monitoring and process validation. If the audit committee is not ready to accommodate you on this point, you should raise the issue to the full board of directors and the outside auditor. If needed changes do not occur, then your professional standards should compel you to look for a new employer.

In this regard, there are several ways that you as the internal auditor can demonstrate independence (not just in appearance) from management and your loyalty to the audit committee:

- If you are an internal auditor of a financial services company that is subject to FDICIA 112, you should already have a good working relationship with the audit committee. But if that relationship has grown cold over the years, it is time to break the ice. Explain to the committee how this level of independence reduces the chances of the company's becoming the next headline.
- If you are an internal auditor of a publicly traded financial services company, Sarbanes-Oxley will make management very sensitive to your request for greater independence, given the threat of fines and possible imprisonment.
- If you are an internal auditor of a nonpublic financial services company, you should view this as an opportunity to convince the board to establish an audit committee with authority similar to that established for audit committees under Sarbanes-Oxley as a best practice.

Further, for all financial institutions, your primary federal banking regulator supports a strong, independent internal audit process at your company. Examinations of the internal audit process, organization structure, and audit committee agenda can provide outside support to the importance of a strong, independent internal audit function.

Third, internal auditors must abandon the idea of becoming the roaming general management consultant within the company.

Many of the proposed revisions to the IIA's professional standards focus on adding value by meeting the needs of management and the board. The focus needs to be on making sure the board has no surprises. Internal auditors add value by being effective, independent assessors of the quality of the internal control framework and processes. Auditors lose their independence when they perform management consulting roles for which they later will have to render an opinion. You are one of the few corporate officers that has both the ability and the responsibility to look across all of the management silos within the corporation and make sure that the system of internal controls has no gaps and that the control framework is continually reviewed to keep up with corporate strategic initiatives, reorganizations, and process changes. When an auditor becomes part of management, the independent view is lost.

Further, you are the independent eyes and ears of the audit committee around the organization. As you work throughout the organization, you know which managers and which projects are likely to entail greater weaknesses in controls. By helping senior management address these risks before losses occur, you can help protect the reputation of managers and the bank and increase your credibility. Prompt reporting to the audit committee and timely resolution of audit findings will build your credibility

with the committee, provided that you follow through on their behalf to ensure that managers are taking control and governance issues seriously.

Conclusion

My objective in talking to you today was to exhort you to take a stand and make a difference for the better in the corporate governance of your company. The Institute of Internal Auditors is the recognized world leader for the internal auditing profession. You should use the resources of this organization to support your efforts to make the internal audit division an even more effective force to improve the quality of internal controls in your organization. And you should take a leadership role in shaping the dialogue on corporate governance. Although I recognize that some of you are internal auditors of companies that are not subject to Sarbanes-Oxley, I believe the act is a wake-up call more generally for the internal auditing profession.