The Federal Reserve Board

# Remarks by Governor Susan Schmidt Bies

**At the Institute of Internal Auditors Financial Services Conference, Arlington, Virginia**
**May 19, 2004**

## Corporate Governance: Where Do We Go From Here?

### Introduction

Good morning. Thank you for the invitation to speak to this Institute of Internal Auditors' Financial Services Conference. I understand by looking at the IIA's website that May marks the second annual global celebration of Internal Audit Awareness Month which gives you an opportunity to promote your profession within individual organizations and throughout the business community. Before becoming a Federal Reserve Governor, I was at various times the chief internal auditor and chief financial officer of a bank, so I understand and appreciate the work you perform.

Today, I will share some of my views on effective corporate governance and risk management with a special focus on certain aspects of the current risk environment. I will also talk about the role of internal auditing in both the enterprise-wide risk-management environment and under the Public Company Accounting Oversight Board's standards. Finally, I will mention a couple of specific areas where you can have an important role in assessing the adequacy of controls.

### Corporate Governance

Events at some corporations over the past three years have called into question the effectiveness of operational, financial reporting, and compliance controls; corporate governance practices; and the professionalism of auditors. Governance issues have also been raised concerning securities underwriting, bank lending practices, mutual funds, and a major stock exchange. Revelations of significant corporate governance and accounting failures, with Parmalat and Shell serving as recent examples, demonstrate that these are serious concerns worldwide, not just here in the United States. Events at the international level have renewed the resolve of companies around the globe to implement high-quality corporate governance practices and accounting and disclosure standards, and for auditors to employ rigorous and sound auditing techniques.

### Internal Control Fundamentals and Enterprise Risk Management

When we talk about corporate governance, we typically start at the top of the organization, with the board of directors and senior management, and work downward. We do this for good reason. The directors and senior management set the governance tone within organizations and lead the way. It's apparent that boards of directors and senior management have a very full plate these days. They must assess the quality of corporate governance within their organization and ensure that the firm has effective accounting practices, internal controls, and audit functions. They must respond to the new requirements of the Sarbanes-Oxley Act. They must establish more stringent anti-money-laundering programs and comply with the USA Patriot Act. Some large financial institutions must address issues relating to Basel II and the implementation work that needs to be done. Firms are

considering how they can be more effective in managing the business risks they face, including the rise in operational risks due to increased homeland security issues and reliance on technology. And, of course, they must still find the time and resources to run their businesses profitably.

The Committee of Sponsoring Organizations (COSO) *Internal Control Integrated Framework* is still the U.S. standard on internal controls. [1] The COSO model serves as the basis for meeting the internal control assessment and reporting requirements for depository institutions laid out in section 112 of the Federal Deposit Insurance Corporation Improvement Act (FDICIA 112). This model is also broadly applicable to public companies in complying with section 404 of the Sarbanes-Oxley Act.

Under COSO, directors have responsibility for overseeing internal control processes so that they can reasonably expect that their directives will be followed. Although directors are not expected to understand the nuances of every line of business or to oversee every transaction, they are responsible for setting the tone regarding their corporations' risk-taking and for establishing an effective monitoring program. The implication is that directors should be vigilant in maintaining a clear understanding of how COSO is being implemented in their organizations.

Directors should also keep up with innovations in corporate governance. For example, directors should be aware that a new COSO framework has been proposed to encompass Enterprise Risk Management.[2] A draft of the updated COSO framework was released for comment last summer, and a final document is expected later this year.

For those of you not familiar with the new COSO framework, let me briefly explain that enterprise-wide risk management is a discipline that an organization can use to identify events that may affect its ability to achieve its strategic goals and to manage its activities consistent with its risk appetite. Such events include not only those that may result in adverse outcomes, but also those that give rise to opportunities. When embraced, an enterprise-wide risk management framework improves the quality and flow of information for decisionmakers and stakeholders, focuses attention on the achievement of organizational goals, and improves the overall governance of an organization.

Some key steps in effective enterprise-wide risk management include identifying and assessing the key risks within an organization and determining the appropriate response to those risks. Companies should determine the level of risk they are willing to accept given the return they can achieve. Management then must implement effective processes to limit risk to the acceptable level. Once these steps have been taken, business line managers are expected to monitor actual risk levels and test the effectiveness of the risk responses.

Several elements are essential to the successful implementation of enterprise-wide risk management. One is clearly articulated risk-management goals which provide a foundation for the enterprise-wide risk management program and for related training and communication. A second is a common risk language which is critical because it enables individuals throughout the organization to conduct meaningful cross-functional discussions about risk. A third essential element is that individuals clearly understand their roles in the risk-assessment and risk-management framework. In today's environment, all organizations should consider embracing this discipline. Indeed, the Federal Reserve is currently considering how enterprise-wide risk management can better be integrated into its management processes.

**Tone at the Top**

It is also important that a strong culture of compliance be established at the top of the organization and that a proper ethical tone be set for governing the conduct of business. In many instances, senior management must move from thinking about compliance as chiefly a cost center to considering the benefits of compliance in protecting against legal and reputational risks that can have an impact on the bottom line. The board and senior management are obligated to deliver a strong message to others in the firm about the importance of integrity, compliance with the law, fair treatment of customers, and overall good business ethics. Leaders should demonstrate their commitment through their individual conduct and their response to control failures.

While the ethical tone of a financial institution comes from the top, a successful ethics program must be demonstrated by staff members at all levels and throughout the organization. The environment should empower any employee to elevate ethical or reputational concerns to appropriate levels of management without fear of retribution. In other words, the culture of the organization should permit issues to be raised to senior management; management can then demonstrate their commitment by responding appropriately.

**Role of Internal Audit**

This leads me to the importance of the role of the internal audit function within an organization. The Federal Reserve very much supports a strong, independent audit function at financial services companies. As indicated in our amended interagency policy statement[3] released last year, the audit committee is responsible for providing an independent, objective, and professional internal audit process. The audit committee, in its oversight of the internal audit staff, should ensure that the function's consulting activities do not interfere or conflict with the objectivity it should have with respect to monitoring the institution's system of internal control. In order to maintain its independence, the internal audit function should not assume a business-line management role over control activities, such as approving or implementing operating policies or procedures, including those it helped design in connection with its consulting activities.

To support this goal, the audit committee should ensure that internal audit has an effective quality assurance process. This becomes increasingly important as organizations grow in scale, enter new lines of business, become more complex, or acquire organizations with different cultures. As organizations grow, internal auditors must learn new technical skills, manage larger staffs, and be continually alert for emerging gaps or conflicts of interest in the system of internal controls. This often requires that the quality assurance process around the internal audit process become better defined and promptly alerts the general auditor and the audit committee to weaknesses in the internal audit program.

Risk-focused audit programs should be reviewed regularly to ensure that audit resources are focused on the higher-risk areas as the company grows and products and processes change. As lower-risk areas come up for review, auditors should do enough analysis to be confident of their risk rating. Audit committees should receive reports on all breaks in internal controls in a form that will help them determine where the controls and the auditing process can be strengthened.

Before a company moves into new or higher-risk areas, the board of directors and senior management should receive assurances from appropriate management and internal audit that

the tools and metrics are in place to ensure adherence to the basics of sound governance. The audit committee should actively engage the internal auditor to ensure that the bank's risk assessment and control process are vigorous.

Many of the organizations that have seen their reputations tarnished in the past few years have simply neglected to consider emerging conflicts of interest when adding new products and lines of business. It is important to make sure that appropriate firewalls and mitigating controls are in place before the product or activity begins.

Some institutions seek to coordinate the internal audit function with several risk monitoring functions (for example, loan review, market risk assessment, and legal compliance departments) by establishing an administrative arrangement under one senior executive. Coordination of these other monitoring activities with the internal audit function can facilitate the reporting of material risk and control issues to the audit committee, increase the overall effectiveness of these monitoring functions, better use available resources, and enhance the institution's ability to comprehensively manage risk.

But I want to add a word of caution. The internal audit function must remain independent of all control processes to be effective. In addition, when an auditor becomes part of the management process subject to internal audit review, the independent view is lost. Internal auditors are in the unique position to understand the evolution of all forms of risks and controls across the organization. If internal audit administratively reports to a chief risk officer, the relationship should be designed to avoid interfering with or hindering the manager of internal audit's direct functional reporting relationship to the audit committee. Also, the audit committee should ensure that efforts to coordinate these monitoring functions do not result in the manager of internal audit conducting control activities. Furthermore, the internal audit manager should have the ability to independently audit these other monitoring functions.

I would also like to add that internal auditors are the eyes and ears of the audit committee around the organization. As the complexity of financial products and technology has grown, the financial services industry has increased its reliance on vendors and third-party service providers for a host of technological solutions. Be mindful that these outsourcing arrangements may pose additional types of risks for the organization, such as security or data privacy risks. Internal auditors should remain vigilant in identifying risks as the organization changes or new products are delivered to the marketplace.

**The Compliance Function**

I also want to mention that an integral part of enterprise-wide risk management is an enterprise-wide compliance program that looks at how activities in one area of the firm may affect the legal and reputational risks of other business lines and across the enterprise as a whole. It should consider how compliance with laws, regulations, and internal policies, procedures, and controls should be enhanced or changed in response. This approach is in marked contrast to the silo approach to compliance, which considers the legal and reputational risks of activities or business lines in isolation without considering how those risks interrelate and affect other business lines. With banking organizations offering a wider variety of products, the possibility of breaks in consumer, legal and regulatory compliance grows. A paradigm shift to an enterprise-wide compliance structure is an integral part of effective enterprise-wide risk management.

While the compliance function will vary by the size and complexity of the organization, the compliance function should be independent of other functions in the organization, including

the internal audit function. Compliance officers should have access to all operational areas. An independent compliance function can help identify compliance weaknesses that cross management lines of responsibilities and may not be effectively managed. In larger organizations, this may require both business-line and enterprise-wide compliance committees to prioritize resources.

The internal audit function should perform independent reviews of the effectiveness of the compliance function. These reviews should examine the quality of information in compliance reports, the adequacy of training programs, whether deficiencies are promptly corrected, and how compliance risk management is implemented by product managers. The internal auditor can also assess whether sufficient resources are available to meet the changing needs of the organization.

**The U.S. Public Company Accounting Oversight Board**

While we are discussing the importance of effective internal controls, let me point out that the Public Company Accounting Oversight Board (PCAOB) has recently approved Auditing Standard No. 2, *An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements*. [4] The new standard is clearly an improvement over the previous one. It highlights the benefits of strong internal controls over financial reporting and furthers the objectives of the Sarbanes-Oxley Act. This standard requires external auditors of public companies to evaluate the process that management uses to prepare the company's financial statements. External auditors must gather evidence regarding the design and operations effectiveness of the company's internal controls and determine whether the evidence supports management's assessment of the effectiveness of the company's internal controls. While the new standard allows external auditors to use the work of others, including that performed by internal auditors, it emphasizes that external auditors must perform enough of the testing themselves so that their own work provides the principal evidence for making a determination regarding the company's controls. Based on the work performed, the external auditor must render an opinion as to whether the company's internal control process is effective, which is a relatively high standard.

In addition, as part of its overall assessment of internal controls, the external auditor is expected to evaluate the effectiveness of the audit committee. If the audit committee is deemed to be ineffective, the external auditor is required to report that assessment to the company's board of directors.

This new standard will certainly put more demands on external auditors and public companies alike. But this is the price to be paid for "raising the bar" to achieve greater reliability in corporate financial statements and to regain the confidence of the public and the trust of financial markets.

**Operations Risk**

Since the mid-1990s, the concept of operations risk has received increasing attention in connection with the evolution of enterprise risk management. By "operations risk" I mean any risk that arises from inadequate or failed internal processes, people, or systems or from external events. Examples of operations risk include employee fraud, failed information system conversions, mis-sent wires, and weaknesses in security procedures for protecting assets and information.

In February 2003, the Basel Committee on Banking Supervision released a paper titled "Sound Practices for the Management and Supervision of Operational Risk" that outlines a

set of broad principles that should govern the management of operational risk at depository institutions of all sizes. [5] These principles will likely play a key role in shaping our ongoing supervisory efforts in the United States with regard to operations risk management. As with COSO's enterprise risk management framework, I encourage you to read the operations risk paper.

Operations risk has always been a part of the financial services industry. But the increasing complexity of financial organizations, an increase in the number and variety of products and services they provide, the evolution of business processes (including substantially greater reliance on information technology and telecommunications), and changes in the ethical environment in which we live have all contributed to more observable exposures to this type of risk. Many of the community bank failures in recent years have been due to operations risks. In a few cases, dominant chief executives perpetrated fraud by manipulating the internal controls. In others, the management information systems necessary to monitor exposures in riskier lines of business were never built. As a result, other managers and the boards of directors did not have the information necessary to monitor and understand the growing risks inherent in what appeared to be profitable strategies.

Operations risk was a primary focus of Y2K preparations a few years ago. Identification of critical computer-reliant systems and infrastructures gave us a much clearer understanding of the financial system's dependence on technology and of the complexities of managing operations risk. Once institutions understood the considerable business risks that would result if they could not serve customers, they moved the management of Y2K preparations out of the back office and onto the desks of product-line and senior managers--where it belonged.

Moreover, it became clear that financial institutions needed to plan for the possibility that an external threat--a failure in the critical infrastructure or by a major service provider or material counterparty--might severely impact a financial institution's business operations. There was an increased understanding of the interdependencies across market participants and of how credit, liquidity, and operations risks at one organization could have a cascading impact on other financial institutions.

**Complex Structured Finance Transactions**

Let's turn our attention to a couple of important areas where internal auditors can have a critical role in assessing the adequacy of controls. Innovation has occurred in the development of complex structured finance transactions, which have received quite a bit of negative press of late. While we are all too aware that recent events have unfortunately highlighted the ways in which complex structured transactions can be used for improper or even fraudulent purposes, these transactions, when designed and used appropriately, can play an important role in financing businesses and mitigating various forms of financial risks.

Although deal structures vary, complex structured finance transactions generally have some common characteristics. Perhaps the most important characteristic is that they may expose the financial institution to elevated levels of market, credit, operations, legal, or reputational risk.

First, they typically result in a final product that is nonstandard and is structured to meet a customer's specific financial objectives. Second, they often involve professionals from multiple disciplines and may involve significant fees. Third, they may be associated with the creation or use of one or more special-purpose entities designed to address the customer's

economic, legal, tax, or accounting objectives or the use of a combination of cash and derivatives products. Financial institutions may assume substantial risks when they engage in a complex structured finance transaction unless they have a full understanding of the economic substance and business purpose of the transaction. These risks are often difficult to quantify, but the result can be severe damage to the reputations of both the companies engaging in the transactions and their financial advisers--and, in turn, impaired public confidence in those institutions. These potential risks and the resulting damage are particularly severe when markets react through adverse changes in pricing for similarly structured transactions that are designed appropriately.

Assessments of the appropriateness of a transaction for a client traditionally have required financial firms and advisers to determine if the transaction is consistent with the market sophistication, financial condition, and investment policies of the customer. Given recent events, it is appropriate to raise the bar for appropriateness assessments by taking into account the business purpose and economic substance of the transaction. When banking organizations provide advice on, arrange, or actively participate in complex structured finance transactions, they may assume legal and reputational risks if the end user enters into the transaction for improper purposes. Legal counsel to financial firms can help manage legal and reputational risk by taking an active role in the review of the customer's governance process for approving the transaction, of financial disclosures relating to the transaction, and of the customer's objectives for entering into the transaction.

As in other operational areas, strong internal controls and risk-management procedures can help institutions effectively manage the risks associated with complex structured finance transactions. Here are some of the steps that financial institutions, with the assistance of counsel and other advisers, should take to establish such controls and procedures:

- Ensure that the institution's board of directors establishes the institution's overall appetite for risk (especially reputational and legal) and effectively communicates the board's risk tolerances throughout the organization.

- Implement firm-wide policies and procedures that provide for the consistent identification, evaluation, documentation, and management of all risks associated with complex structured finance transactions--in particular, the credit, reputational, and legal risks.

- Implement firm-wide policies and procedures that ensure that the financial institution obtains a thorough understanding of the business purposes and economic substance of those transactions identified as involving heightened legal or reputational risk and that those transactions are approved by appropriate senior management.

- Clearly define the framework for the approval of individual complex structured finance transactions as well as new complex structured finance product lines within the context of the firm's new-product approval process. The new-product policies for complex structured finance transactions should address the roles and responsibilities of all relevant parties and should require the approval of all relevant control areas that are independent of the profit center before the transaction is offered to customers.

- Finally, implement monitoring, risk-reporting, and compliance processes for creating, analyzing, offering, and marketing complex structured finance products. Subsequent to new-product approval, the firm should monitor new complex structured finance products to ensure that they are effectively incorporated into the firm's risk-control

systems.

Of course, these internal controls and risk-management processes need to be supported and enforced by a strong "tone at the top" and a firm-wide culture of compliance as mentioned earlier.

**Allowance for Loan and Lease Losses**

Finally, another area where your work on assessing controls can be very important is in reviewing the assessment of the adequacy of the allowance for loan and lease losses (ALLL). Financial regulators want to encourage banking organizations to strengthen their processes and documentation associated with their determination of the adequacy of their ALLL. As you know, accounting standard setters recently questioned the methodology for loan loss reserves and proposed new guidance. The good news is that they now recognize that reaffirming existing guidance could address many of the questions raised. But the fact that loan loss reserve methodology is a recurring issue reflects the reality that concerns about how the ALLL is being estimated and its impact on earnings do arise from time to time. In general, these situations can be addressed through strengthened audit procedures rather than changes in accounting standards. Furthermore, management of financial institutions should be reminded to take the time to review the estimation procedures for determining their loan-loss reserves.

Banking institutions should be applying an ALLL methodology that is well defined, consistently applied, and auditable. Institutions are required to maintain written documentation to support the amounts of the ALLL and the provision for loan and lease losses reported in the financial statements. This methodology should be validated periodically and should be modified to incorporate new events or findings as needed. Interagency supervisory guidance specifies that management, under the direction of the board of directors, should implement appropriate procedures and controls to ensure compliance with the institution's ALLL policies and procedures. Given that many banks use credit models, it is important that those models be validated periodically. Institutions should be vigilant to ensure the integrity of their credit-related data and that the loan review process provides the most up-to-date and accurate information possible for management to consider as part of its ALLL assessment.

**Conclusion**

I have touched on a number of important topics today. While some of them, such as structured finance transactions and loan loss reserve accounting, are rather specific, these risk issues cannot be viewed in isolation. I want to note that these are just aspects of the broader issues of corporate governance and enterprise-wide risk management. Successful risk management should be integrated into an organization's corporate governance processes, with appropriate controls, testing, and oversight.

Boards of directors and senior management have the responsibility to establish effective risk-management and assessment processes across their organizations and to integrate the results of those efforts into their strategic and operating planning processes. Because of its unique, firm-wide perspective and its independence, the internal audit function can play an important role in reviewing the quality of corporate governance, internal control, and enterprise-wide risk management.

---

**Footnotes**

1. COSO 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." *Internal Control Integrated Framework* is available for purchase from the American Institute of Certified Public Accountants; COSO also provides an executive summary. Return to text

2. A copy of the draft can be obtained at the COSO web site. Return to text

3. A copy of the interagency policy statement (286 KB PDF) was released on March 17, 2003. Return to text

4. A copy of the auditing standard can be obtained at the PCAOB web site. Return to text

5. The paper can be obtained on the BIS web site. Return to text

▲ Return to top

2004 Speeches

---

Home | News and events
Accessibility | Contact Us
**Last update: May 19, 2004**