The Federal Reserve Board

Remarks by Governor Susan Schmidt Bies

At the Bank Administration Institute's Fiduciary Risk Management Conference 2004, Las Vegas, Nevada
April 26, 2004

Current Issues in Corporate Governance

Introduction

Good morning. Thank you for the invitation to open the Bank Administration Institute's important and timely conference on audit, compliance, and e-security. 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 enterprisewide risk-management environment and the new world of the Public Company Accounting Oversight Board's standards. Finally, I will mention two current accounting and reporting developments.

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 reliance on technology and homeland security issues. 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 enterprisewide 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 enterprisewide 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 enterprisewide 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 enterprisewide risk management. One is clearly articulated risk-management goals which provide a foundation for the enterprisewide 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 element essential to the implementation of successful enterprisewide risk management 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 enterprisewide 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 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 raise issues to senior management that they may not be aware of; 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 is very supportive of an independent audit function at financial services companies. As indicated in our amended interagency policy statement released last year, the audit committee should provide for an independent, objective, and professional internal audit process.[3] The audit committee must set the tone for the internal audit function.

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 alerts the general auditor and the audit committee to weaknesses in the internal audit program promptly.

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 produces and as processes change. As lower-risk areas come up for review, auditors should do enough transaction testing to be confident in 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 that the basics of sound governance will be adhered to. 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.

The audit committee should also require the highest possible level of independence for the internal audit process and eliminate any threats to this independence, such as the tendency for some internal auditors to act as management consultants within the organization. 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. Internal audit is one of the few corporate functions with 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 the management process subject to internal audit review, the independent view is lost.

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 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 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.

Risk Management in the e-Commerce Environment

Let's now turn our focus to risk management in today's e-commerce environment. We know that an important component of risk management involves monitoring and managing environmental and external risks. This is an area in which business and operations risk are increasing. Over the past few years, the global community has experienced a series of

"cyberincidents"--primarily in the form of increasingly virulent viruses and worms, and some hacking incidents have involved company insiders. The extensive electric power outages experienced by a large section of the United States and parts of Canada last August, along with collateral effects involving the telecommunication, transportation, and water sectors, further underscore the need for financial institutions to integrate the risk of a wide-scale disruption into their risk- management strategies.

Let me say at the outset that the financial sector has performed extraordinarily well in responding to these incidents. Moreover, we are extremely proud that financial markets and participants have been able to meet these challenges and continue critical operations without any systemic effects or loss of confidence in our financial system. This is no accident. Financial institutions have increasingly devoted resources to addressing operations risk, business continuity, security (physical and cyber), and information-sharing. I would like to highlight some of the key developments we have observed and discuss where our business-risk-management efforts should be focused.

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, missent 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 banking. 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 belongs.

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.

IT and Physical Security

As a former banker, I can attest to the fact that banking organizations have long understood the need for strong internal IT controls and physical security. The trust and confidence consumers have that their assets and confidential information are completely secure is a pillar of the U.S. financial system.

The increasing role of information system networks and the Internet in business operations as a means of conducting business with customers has engendered new cybersecurity risks for financial institutions. Thankfully, banking organizations recognized these risks from the outset and became leaders in addressing cyberprotection issues. For example, financial services was the first private sector to incorporate encryption into business processes on a wide scale. Nevertheless, each year the continuous stream of cyberattacks, such as the Bugbear.B virus (which targeted banks) and the SoBig.F worm, demonstrate that cybersecurity will need to be an ongoing battle. Experience to date shows that banking organizations are effectively managing cybersecurity risk. There have been relatively few serious intrusions, and there have been virtually no disruptions of critical systems. Nevertheless, financial institutions can expect to remain a target of cyberattacks. I believe there is a need for heightened attention to managing this risk. This includes monitoring warnings carefully, acting quickly to apply patches in a controlled environment, and taking other steps necessary to preclude any damage to information systems.

Moreover, I urge you to review your internal security requirements to make sure that effective controls are in place and being followed. You may recall that my definition of operations risk includes employee fraud. We are still seeing evidence that most successful--or nearly successful--hacking incidents can be traced back to current or former employees.

We regulators have been mindful of the tremendous growth in your reliance on information technology, such as the shift from mainframe computing to the use of distributed systems and the Internet, increased reliance on commercial off-the-shelf software, and a general expansion of potential external access to enterprise data. This increase in operations risk raises significant safety and soundness concerns for financial institutions and privacy concerns for consumers. In January 2003, the FFIEC (Federal Financial Institutions Examination Council) issued revised guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk-management practices.[6] The guidance, contained in the Information Security Booklet, describes how an institution should protect and secure the systems and facilities that process and maintain information. It calls on financial institutions and technology service providers to maintain effective security programs that are tailored to the complexity of their operations. Several years ago, as part of the shift to a risk-focused approach to supervision, the Federal Reserve integrated information technology reviews into safety and soundness examinations. This assures that our evolving understanding of the elements of operations risk is reflected in supervisory assessments of the adequacy of risk management

across the entire enterprise. I hope that you are already familiar with the supervisory expectations in the Information Security Booklet.

I would also like to remind everyone of the importance of securing customer information. This privacy requirement goes beyond the IT systems themselves to the output of those systems. Distributed processing means paper copies of customer information tend to proliferate. Information security should include protection of paper documents, including their safe disposal, so that customers' private information does not inadvertently fall into the wrong hands.

On the physical security side, I am aware that some of you have had to step up physical security protocols to ensure that your facilities and staff are protected. Over the past year, we have had several occasions when the government raised the threat level to Orange (High). Responding responsibly to physical threat warnings is costly and can be confusing, but it cannot be avoided. The Department of Homeland Security has provided some general guidelines on how to adjust security measures to its threat-level warning system. Industry groups have been sharing information on the measures they plan to take at various threat levels--including measures to protect staff by conducting operations from homes or back-up locations. This discussion has led to a greater awareness and commitment by financial institutions to ensure that all practical measures are taken to protect employees and facilities. I commend the industry for the work it has done in responding to homeland security issues. I hope you will continue to share information on ways to protect your businesses in the post-September 11 environment. I also suggest that you make every effort to coordinate with local protection authorities so that they are aware of your special needs and you understand their emergency protocols.

Allowance for Loan and Lease Losses

Finally, I want to talk about two accounting and reporting issues. Financial regulators want to encourage banking organizations to strengthen their processes and documentation associated with their determination of the adequacy of their allowance for loan and lease losses (ALLL). As you know, accounting standardsetters 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.

Call Report Modernization
I also want to mention that the federal banking agencies are using advances in technology in their own business practices. One example is a project that is currently under way to improve the collection, validation, distribution, and use of the Call Report data that is submitted by banks to the banking agencies. This effort is referred to as the Call Report Modernization Initiative. Under the sponsorship of the FFIEC, the banking agencies are developing a central data repository to be a shared resource for all those who provide Call Report data or rely on these data in their business. A primary goal of the project is to allow for faster validation of the Call Report data, which will ultimately allow for faster release of these data to the public. This project has been under way for a couple of years now and is scheduled to go "live" in September 2004. You can find more information about the Call Report modernization project on the FFIEC web site (www.ffiec.gov/find/).

The Federal Reserve is also making improvements in the reporting process for bank holding companies (BHCs). All BHCs are now required to file the Y-9 financial reports electronically, thereby eliminating paper-copy reporting. In addition, similar to the Call Report modernization effort that has been undertaken on an interagency basis, the Federal Reserve will be implementing a process that more quickly validates the BHC Y-9 data so that the data are released faster to the public. You can contact your district Federal Reserve Bank if you would like additional information on this initiative. Information is also available on a Federal Reserve web site (www.reportingandreserves.org/).

Conclusion
I have touched on a number of important topics today. While some of them, such as loan loss reserve accounting, cybersecurity, and corporate ethics, 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 enterprisewide risk management. Successful risk management is 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. The internal audit function can play an important role in reviewing the quality of corporate governance, internal control, and enterprisewide risk management because of its unique, firmwide perspective and its independence.

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; an executive summary is available at http://www.coso.org/publications/executive_summary_integrated_framework.htm. Return to text

2. A copy of the draft can be obtained at the COSO web site at http://www.coso.org/publications.htm. Return to text

3. A copy of the interagency policy statement, which was released on March 17, 2003, can be obtained at http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030317/default.htm. Return to text

4. A copy of the auditing standard can be obtained at the PCAOB web site at http://www.pcaobus.org/pcaob_standards.asp. Return to text

5. The paper can be obtained on the BIS web site at http://www.bis.org/publ. Return to text

6. The Information Security Booklet can be accessed at the FFIEC web site under the Information Technology Examination Handbook InfoBase at http://www.ffiec.gov. Return to text

▲ Return to top

2004 Speeches

Home | News and events
Accessibility | Contact Us
Last update: April 26, 2004