The Federal Reserve Board

Remarks by Governor Susan Schmidt Bies

At the Financial Managers Society Finance and Accounting Forum for Financial Institutions, Washington, D.C.
June 22, 2004

Trends in Risk Management and Corporate Governance

Thank you for the invitation to participate in the 2004 Finance and Accounting Forum of the Financial Managers Society. The agenda for this year's forum included a significant number of sessions devoted to corporate governance, which is a change from prior years. As senior members of the accounting, auditing, or management functions within your financial institutions, you are probably at the forefront of your institutions' discussion of governance matters. You are also probably spending a considerably greater amount of time and energy implementing revisions to your governance process than you did just three years ago. Even if your institution is not publicly traded, this increased activity is certainly the result of the Sarbanes-Oxley Act of 2002. However, the practice of corporate governance at U.S. financial institutions is not new and did not begin with Sarbanes-Oxley. U.S. financial institutions, both publicly traded and privately held, have a tradition of taking their responsibilities for ensuring effective governance seriously, and those with total assets of $500 million or more have been subject to section 112 of the Federal Deposit Insurance Corporation Improvement Act (FDICIA) for more than ten years.

In my comments today, I will focus primarily on the state of corporate governance at financial institutions. I'll discuss the assessments some of the consultants and public accountants are giving the banking industry, and I'll contrast those assessments with what we are observing through the examination process. I'll also touch on some of the developing best practices in corporate governance, internal controls, and operational risk management. It seems that many of these best practices are being developed by professionals such as yourselves, who are implementing the mandates of Sarbanes-Oxley in a manner that is relevant for your individual businesses and corporate structure. At the Federal Reserve, we tend to favor best-practice approaches for corporate governance rather than a one-size-fits-all approach.

Corporate Governance Perspective of Consultants

Over the past few years, there has been a marked increase in the number of corporate governance surveys at both publicly traded and privately held financial institutions. Recently, several of the major consulting and accounting firms reported on the governance practices at financial services firms, including federally regulated banks. Although the survey questions varied somewhat by consulting or accounting firm, the survey results seem to have a certain amount of commonality. They all begin by recognizing the progress financial services firms have made in the areas of director independence, audit committee oversight, and overall board awareness of governance issues within their organizations. They all cite a growing sensitivity to governance issues among employees and a heightened awareness among senior management and the board. They cite improvements in

governance-type disclosures to shareholders and stakeholders and increased vigilance on the part of the regulatory agencies. However, they almost all conclude by saying that banks and other financial services firms have a long road ahead of them if they are to achieve the goal of effective corporate governance--which sounds as if the firms believe that financial institution governance practices are deficient.

Why is this? According to a global survey of financial institutions conducted by PricewaterhouseCoopers, financial institution governance practices need improvement in part because most institutions equate effective governance with meeting the demands of regulators and legislators. [1] That is, they tend to look at this as another compliance exercise. The study goes on to state that the compliance mentality is limiting these institutions' ability to achieve strategic advantages through governance.

I agree that any institution that views corporate governance as merely a compliance exercise is missing the mark. We all are aware of companies in various industries who have successfully presented their strategic vision to investors but later stumbled because the execution of that strategy did not meet expectations. Although shortfalls can occur for many reasons, one of the more common shortcomings is focusing the strategy itself too much on market and financial results without giving adequate attention to the infrastructure necessary to support and sustain the strategy.

Corporate strategies often focus on the most likely future scenario and the benefits of a strategic initiative. Creation of a sound governance, risk-management, and internal control environment starts by making it part of the strategic-planning exercise. That is, while the strategy is being considered, managers and board members should be asking a number of questions: What are the major risks of this plan? How much risk exposure are we willing to accept? What mitigating controls need to be in place to effectively limit these risks? How will we know if these controls are working effectively? In other words, by considering risks as part of the planning process, controls can be built into the design, the costs of errors and reworking in the initial rollout can be reduced, and the ongoing initiative can be more successful because monitoring can reveal when activities and results are missing their intended goals, so that corrective actions can be initiated more promptly.

Similarly, as these strategies are being implemented, all managers and employees in the organization must have an understanding of the risk exposures and controls in their particular areas of responsibility. Furthermore, management should assign ownership of each control in the various areas to appropriate individuals. From past experience, we know the more common causes of ineffective controls occur when a properly designed control is monitored by an individual who has an incomplete understanding of how the control helps to mitigate risk exposures or fails to assume full responsibility for the operation of the control, or misinterprets the operating effectiveness of the control. In short, controls are only as good as the individuals who operate and monitor their effectiveness.

Many of these surveys note that it is very difficult for outsiders to determine the effectiveness of corporate governance. Unfortunately, it takes significant breaks in internal controls for the public to be aware of weaknesses in the process. The disclosure of deficient business and governance practices can then lead to lower share prices, the likelihood of shareholder lawsuits and enforcement actions, loss of credibility and damage to a bank's reputation, and the payment of higher spreads to access capital markets. The magnitude of the detrimental impact that can result from a serious breach in governance puts the costs of improved governance in perspective.

Several studies reveal that institutions are spending more on corporate governance today than in the past. According to Grant Thornton's *Eleventh Annual Survey of Community Bank Executives*,[2] it isn't just large organizations that are feeling the financial impact of corporate governance. Institutions that are not subject to the Sarbanes-Oxley Act and FDICIA incurred or are expected to incur increases in costs for a number of services and functions related to corporate governance. Seventy-three percent of these banks surveyed expected to incur increases in general audit fees, 62 percent expected to incur increases in director and officer liability insurance premiums, 32 percent expected to incur increases in financial education costs for directors, and 12 percent expected to incur increases in costs associated with attracting and retaining board members.

In response to this survey, a logical question is whether the benefits outweigh the costs. Many of you are reflecting on the first-half 2004 discussion of your operating results, budget estimates, and income projections for the future that were presented at recent board and staff meetings. True, these costs reduced some of your current profitability goals. But corporate managers have demonstrated over the years that focusing on better process management can enhance financial returns and customer satisfaction. They have learned that correcting errors, downtime in critical systems, and lack of training that enables staff to promptly handle their changing tasks, all create higher costs, unhappy customers and lost revenue opportunities. I challenge you to consider the development of a corporate governance structure appropriate to your institution's unique business strategy and scale as an important investment, and consider returns on that investment in terms of avoidance of the costs of poor internal controls.

Corporate Governance Perspective of Regulators

Now I would like to discuss the regulatory community's assessment of corporate governance practices at certain community banks. Regulators typically measure effectiveness by some sort of examination assessment. Using the current CAMELS-type of assessment, a review of recent Federal Reserve examination results indicate that most community banks have effective corporate governance. Eighty-four percent of the banks reviewed were highly rated on their risk-management practices, including corporate governance. This is not to say that we don't see the need for improvement in certain areas. Examination findings routinely cite ways in which risk management, including corporate governance, could be improved. However, it is apparent that the senior management, boards, and audit committees in these highly rated organizations are setting annual agendas that focus attention on the high-risk and emerging-risk areas within their banks while continuing to provide appropriate oversight to the low-risk areas. Internal auditors, or equivalent functions at these banks, are testing to determine whether the risk- management program is effective and are communicating the results to the board and audit committee.

So, the examination results appear to indicate that the vast majority of banks are getting the message on the basics of sound governance. I would like to stop my speech here and conclude by saying, "All is well in the banking industry." However, we also performed a review of the corporate governance at the subset of banks with weak or unsatisfactory ratings. Not surprisingly, the review identified the major challenges facing these banks to be poor asset quality and corporate governance issues, such as policies, planning, management, audits, controls, and systems. Eighty-nine percent of the banks in this group experienced serious asset-quality problems, which was the most significant factor in their low rating. Sixty percent of the banks in this group experienced significant deficiencies in corporate

governance. The corporate governance deficiencies could broadly be described as internal control weaknesses, weak or inadequate internal audit coverage, significant violations of law, accounting system weaknesses, and information technology issues.

Obviously, poor asset quality and ineffective corporate governance are not mutually exclusive. When we find significant asset-quality problems, we usually find corporate governance problems--particularly inadequate internal controls. Similarly, when we find significant control deficiencies, significant asset-quality or financial-reporting problems are generally present. So what is the message we should take away from these statistics?

On the one hand, we could pat ourselves on the back and say that things are generally going very well for most of the industry and we can finally tone down all of the corporate governance rhetoric. Or, we could say that those negative statistics apply only to the boards and senior managers at a small group of poorly rated institutions, which now have to pay the price. Or, yet again, we could say that effective corporate governance is a continuous process that requires ongoing vigilance on the part of the board, audit committee, senior management, and others within your bank. I hope you are thinking along the lines of this last sentiment.

As you know, once an organization gets lax in its approach to corporate governance, problems tend to follow. Many of you can recall the time and attention management devoted to section 112 of FDICIA, which first required management reports and auditor attestations in the early 1990s. Then the process became routine, delegated to lower levels of management, and no longer relevant to the way businesses were being run. That is when the breakdown in internal controls began to occur. Unfortunately, trying to change the culture again is taking an exceptional amount of senior management and directors' time--time taken away from building the business. It is also taking more time from line managers and their staff. The challenge, therefore, is to ensure that banks' corporate governance practices keep pace with the changing risks that you will face in the coming years.

Another consequence of so much public attention on the breakdowns in controls at a few organizations is difficulty in finding good directors. One common theme we have heard during our examinations is the challenge facing banks of all sizes to retain, or attract, board members with the appropriate depth of understanding and commitment to sound corporate governance practices. Many potential directors who have the experience needed are cautious about the potential liability they face. Also, they would rather join a board on which they are able to balance their time among all of the areas of oversight--strategy, marketing, financial performance, human resource development, community involvement, and so on--and not just governance, compliance, audits, and internal controls. This is another result of inconsistent attention over time to good governance practices.

Operational Risk

In addition to corporate governance, the Federal Reserve System is also focusing on operational risk, conducting selected reviews for operational risk at community banks. By operational risk, I mean "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events," which is the definition used by the Basel Committee on Banking Supervision. The Federal Reserve's increasing focus on operational risk is due, in part, to the significant improvements we have seen in the last two decades in the management of interest-rate and credit risk. Thus, operational risks and weaknesses in governance and internal controls become more apparent.

For example, at one of our Reserve Banks we are conducting a pilot program specifically geared toward the operational-risk activities of smaller community banks, those with less than $500 million in assets. One of the objectives of the program is to identify and test the key internal controls used by banks to mitigate operational risk exposures. The reviews focus on specific business processes with high operational risk--for example, the wire transfer and loan administration areas. The bankers involved have responded very favorably to the program and indicated they have received measurable benefits. Moreover, the program has identified some common operational-control weaknesses to which we believe community banks should pay particular attention. Let's use wire transfers and loan administration as examples.

With wires and similar transactions, the bank could suffer a significant financial loss from unauthorized transfers, as well as incur considerable damage to its reputation if operational-risk factors are not properly mitigated. A few recurring recommendations from our reviews are to: (1) establish reasonable approval and authorization requirements for these transactions to ensure that an appropriate level of management is aware of the transaction and to establish better accountability; (2) establish call-back procedures, passwords, funds transfer agreements, and other authentication controls related to customer wire-transfer requests; and (3) pay increased attention to authentication controls, since this area may also be particularly susceptible to external fraud.

Loan administration is an area in which a bank could suffer a significant financial loss from the lack of appropriate segregation of duties or dual controls and could incur considerable damage to its reputation if operational-risk factors are not properly mitigated. A few recommendations that have arisen from our reviews are to (1) ensure that loan officers do not have the ability to book and maintain their own loans; (2) limit employee access to loan system computer applications that are inconsistent with their responsibilities; and (3) provide line staff with consistent guidance in the form of policies and procedures, on how to identify and handle unusual transactions.

Several other recommendations resulted from these reviews, and we have a number of operational-risk initiatives under way. We expect to summarize these findings and provide further updates and guidance to the industry as we move forward. But given the examples of best practice I just mentioned, these are not revolutionary insights. Well-run organizations have these or similar controls in place. We hope these studies serve as reminders to bank managers to keep the focus on continuous improvements in internal controls as part of the normal business process.

Observations on Best Practices

Finally, I want to focus on some best practices for corporate governance at your institutions. Rather than talk broadly about best practices, I'll focus on certain aspects of internal controls and operational-risk management.

Best Practice 1: *Adopt a recognized internal control framework that works for the bank*.

All financial institutions have some framework for internal control. What I'm suggesting as a best practice is to adopt a version of the *Internal Control--Integrated Framework commissioned by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission*.[3] Don't be put off by the title of this framework. It is flexible enough to work effectively at a $25 million bank or a multibillion dollar financial institution and describes

how each internal control element can be tailored to smaller and less-complex organizations. For example, if the COSO framework is used as a best practice, you should modify the five following elements of internal control to meet your organization's needs.

- *Control environment.* Board members and senior managers should identify the bank's key business strategies, objectives, and goals and tailor the COSO framework to influence the bank's management philosophy, culture, and ethics to establish and maintain an appropriate control environment. Line managers and employees should be able to articulate how specific objectives and goals are addressed in their business areas.

- *Risk assessment*. Managers should look at the risks inherent in the businesses and processes they manage, determine the bank's risk appetite, and establish risk-measurement practices that are appropriate for their organization. All employees in the area should have a good sense of acceptable risks and have a process for communicating apparently unacceptable risk taking to appropriate levels of management.

- *Control activities.* Managers should establish and maintain controls and monitoring processes to ensure that they will be effective in achieving the organization's profit and other objectives, based on a designated level of risk. Managers should monitor the organization's business plan to assess how risk exposures are changing and determine whether new controls, or changes in existing controls, are needed to manage that level of risk. Employees should have a detailed understanding of the purpose of each group of controls in their areas of responsibility and a good understanding of how the controls contribute to the institution's ability to achieve its operating objectives and accurate financial reporting.

- *Information and communication.* Information required to achieve the organization's control objectives should typically be accumulated in a management information system and should be communicated through reliable channels to all responsible parties--from tellers to board members. Normal bank communication channels should usually be adequate for this purpose. However, new channels may be necessary if the type of information is too sensitive to communicate over existing channels or if communicating that information poses a risk to the individual making the communication (in other words, if the individual is a whistle blower with knowledge of an incident of identified fraud).

- *Monitoring.* Monitoring should typically be the role of internal audit. A number of small institutions do not have a permanent internal audit department. Each institution must therefore develop a review (audit) function that is appropriate to its size and the nature and scope of its activities.

As you may know, COSO is just about to release a revised framework that will incorporate enterprise risk management (ERM). When this is issued, the best practices in these five elements will need to be re-evaluated to address ERM.

Best Practice 2: *Adopt a program for independently assessing the effectiveness of internal controls at least annually*.

Boards of directors and audit committees are responsible for ensuring that their organizations have effective internal controls that are adequate to the nature and scope of

their businesses and are subject to an effective audit process. Effective internal control is the responsibility of line management. Line managers must determine the acceptable level of risk in their line of business and must assure themselves that they are getting an appropriate return for this risk and that adequate capital is being maintained. Supporting functions such as accounting, internal audit, risk management, credit review, compliance, and legal should independently monitor and test the control processes to ensure that they are effective.

Implementing management reports on internal controls comparable to those required under Sarbanes-Oxley and FDICIA 112 can also help boards of directors and audit committees of institutions that are not subject to these acts obtain a better understanding of the controllable risks within their organizations and the quality of the controls over those risks that are in place. Sarbanes-Oxley and FDCIA 112 require an annual management assessment of internal control effectiveness and an attestation of management's assessment and the effectiveness of controls by the bank's external auditor. Management at institutions that are not subject to Sarbanes-Oxley and FDICIA 112 could perform their own periodic assessment of internal control effectiveness, including a report. Another group of employees within the institution could perform an independent evaluation of management's report.

When I say *independent*, I do not necessarily mean that an external auditor should be engaged to issue a report. In this sense, *independent* may mean that internal audit is brought in to perform something similar to an external auditor's attestation. The details of such an approach need to be worked out. The important point is that the audit committee should have some reasonably independent assessment of management's report. Audit committee members could use these reports to set the audit plan for the next year, to track how risks have changed and are changing within the organization, and to facilitate discussion of which controls should be added.

Best Practice 3: *Adopt a framework for assessing operational risk*.

Over the past few years, the discussion of operational-risk management has increased significantly in banking circles. In 2003, the Basel Committee released a paper, "Sound Practices for the Management and Supervision of Operational Risk."[4] This paper sets forth a set of broad principles that should govern the management of operational risk at banks of all sizes. Although operational risk is nothing new to financial institutions, the prospect of addressing this risk in a structured framework with measurable results is something new.

The broad variety of products and services that institutions provide, the evolution of business processes, and changes in the ethical environment in which we live have all contributed to more observable exposures to this type of risk. Managers and boards are beginning to gather the information necessary to monitor and understand the growing risks inherent in their operations. Supervisors are developing approaches to measuring and evaluating operating risk. At the Federal Reserve, we are studying different approaches and have a project underway to develop guidance on how to address this risk. In the near future, we plan to compare our observations on best practices in the area of internal controls and operational risk management with yours to develop some useful resource materials for good corporate governance at the banks we supervise.

Conclusion

In conclusion, financial institutions are further improving their traditional focus on strong corporate governance. Those institutions leading the way recognize that the culture of

governance, ethics, and controls cannot readily be switched on and off. They build a culture of accountability and ethics to make governance a part of every strategic plan and daily operation. These organizations are also beginning to focus more attention on operational-risk issues, which are an essential part of the overall risk-management plan of the organization. The Federal Reserve has a number of initiatives underway, and we plan to work with banking organizations to continue to identify emerging best practices.

Footnotes

1. PricewaterhouseCoopers and the Economist Intelligence Unit, "Governance: From Compliance to Strategic Advantage,"(436 KB PDF) (April 2004). Return to text

2. Grant Thornton, LLP, *Eleventh Annual Survey of Community Bank Executives* (January 2004). Return to text

3. Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control--Integrated Framework* (American Institute of Certified Public Accountants, 2002). Return to text

4. Basel Committee on Banking Supervision, "Sound Practices for the Management and Supervision of Operational Risk"(99 KB PDF) (February 2003). Return to text

▲ Return to top

2004 Speeches

Home | News and events
Accessibility | Contact Us
Last update: June 22, 2004