The Federal Reserve Board

Remarks by Governor Susan Schmidt Bies

At the Community Bank Directors Conference of the Federal Reserve Bank of Chicago, Des Moines, Iowa
August 7, 2003

The Role of Community Bank Directors in Strengthening Corporate Governance

I want to thank you for inviting me to participate in this Community Bank Directors Conference. As I travel and speak to bank directors and management, I frequently am asked questions about corporate governance. While some of the questions have been prompted by the corporate scandals of the last two years, many go beyond the details of specific cases to focus on best practices in the area of corporate governance. While the Sarbanes-Oxley Act and new Securities and Exchange Commission regulations are directed to public companies, the message I hope to convey today is that aspects of these reforms can provide benchmarks for private and community banks who wish to strengthen internal controls.

One of my responsibilities as a governor on the Federal Reserve Board is to chair the Board's Committee on Supervisory and Regulatory Affairs. In that role I apply my knowledge of banking to the continuing task of adapting the Federal Reserve's supervision process to meet the needs of the evolving financial services industry. Today I want to explore some issues of joint interest to us, as directors and supervisors, to think about how we can improve corporate governance in banking organizations.

First, I will discuss the basic framework of good corporate governance and internal control. Then I will talk about the role of the board of directors in the control process and how directors can become more informed about the nature of changing risks in their banks. I will give examples of types of risks that can occur at community banks without effective governance. And finally, I'll discuss why it is important for bank directors and managers to be fully aware of the implications of operational risk and reputational risk.

Internal Control Framework

Over the past two years, we all 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 exemplify breakdowns in fundamental systems of internal control. These companies lost track of the basics of effective corporate governance--internal controls and a strong ethical compass. While most companies have effective governance processes in place, these events remind all of us of the importance of doing the basics well.

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 types of frauds. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission issued a report titled *Internal Control--Integrated Framework*[1] that has become the most-referenced standard on internal control.

If one re-reads that report, the need to return to focusing 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 (FDICIA) was enacted in 1991. FDICIA came after the savings and loan failures, the series of corporate governance scandals in the 1980s, and the work of the Treadway Commission were well known. Section 112 of FDICIA requires bank management to report annually on the quality of internal controls and outside auditors to attest to that control evaluation. The internal control framework of COSO became the standard by which the FDICIA and, now, the Sarbanes-Oxley reports are modeled.

While banks with assets less than $500 million do not have to file FDICIA reports with regulators, a modified form of the process can be very effective for smaller organizations. In fact, the COSO framework is versatile enough that it recognizes that the size and complexity of an organization are important determinants of an effective system of internal controls. Each chapter of the report discusses how small and mid-sized entities can incorporate the aspects of effective internal controls relevant to their organization. I would encourage those of you who are interested to read a copy, and I have included a reference to the source of this publication in the copy of my remarks.

Control Assessments

COSO requires all managers to, at least once a year, step back from their other duties and evaluate risks and controls. Managers should look at the risks inherent in the businesses and processes they manage, and determine what level of risk exposure is appropriate given the profit and strategic goals of the organization. Once the risk limit is set, managers should evaluate the mitigating controls and monitoring processes to see if they are effective in achieving the designated level of risk. Managers should also look at the organization's business plan to see how risk exposures are expected to change and to determine whether new controls, or changes in existing controls, are needed to manage that level of risk. Finally, managers should prepare action plans for building or modifying existing controls to effectively manage risk.

Managers then 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 broader areas of responsibility. The results of this process are ultimately to be reported to the audit committee of the board of directors. In the case of FDICIA 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 are also useful in assessing the risks and controls 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 the Institute of Internal Auditors and the National Association of Corporate Directors showed that directors were not focusing on risk management. I was surprised to learn that 45 percent of directors surveyed said their organization did not have a formal enterprise risk management process--or any other formal method of identifying risk. An additional 19 percent said they were not sure whether their company had a formal process for identifying risks. These percentages indicate that there are companies out there that have directors who don't understand their responsibilities. I trust that none of the directors who participated in the survey were on the board of a financial services company.

At the Fed, we have been looking at the FDICIA reports produced by banks at which internal control breakdowns led to significant losses. We have found instances in which failures of internal controls that were known to management were not mentioned in the management report. These failures include various types of internal control breakdowns, such as failure to reconcile accounts in a timely fashion or failure to segregate duties in critical transaction-processing or accounting functions. Our review also identified more serious internal control deficiencies. In some of these cases, the external auditor did not identify the known failure in the attestations. We are working with banks and independent auditors to make sure this basic control process has substance in the future.

Examiners also observed that at some banks with breakdowns in internal controls the process of reporting on internal controls had become a "paper pushing" exercise rather than a robust part of the corporate governance process. FDICIA is now twelve years old, and the results of these regulatory reviews again show how important the tone at the top is to reinforcing the importance of good governance and effective internal controls. Banks which try to delegate the update of annual control assessments to junior auditors, rather than "wasting the time" of management, lose an opportunity to remind managers that they have the responsibility for maintaining effective internal control--a responsibility that cannot really be delegated. These banks also demonstrated how challenging it can be to keep focused on doing the basics well, year after year, when the excitement and rewards of management are focused on developing and implementing strategies for the future.

Communicating Internal Control Assessments to Boards of Directors

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 executives who have integrity, 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.

Management reports on internal controls can also help bank boards of directors and audit committees gain a better understanding of the nature of the risks and the quality of the controls in place. Audit committees should not just hear that the outside auditors have "signed off" on the FDICIA report. Rather, the report itself can be the basis for an effective

discussion of internal controls among managers, internal auditors, external auditors, and the audit committee. Audit committee members can use these reports to discuss how risks are changing and what the priorities for strengthening controls should be. Audit committees can also use the reports to focus on recurring concerns, such as control weaknesses that managers fail to address in a timely manner.

The COSO framework and management's process for developing the FDICIA annual report can be an effective tool for the internal auditor to communicate risks and control processes to the audit committee. Members of that committee should use the reports to ensure business strategy, changing business processes, management reorganizations, and positioning for future growth are conducted 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. In fact, the issues highlighted in the COSO internal control report can provide a basis for setting the audit committee calendar for the year--areas where internal controls need to be reviewed and strengthened, and to monitor progress in achieving those results.

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?" Directors 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.

Finally, but to regulators surely not least important, bank examiners can provide information to boards to benchmark the level of risks and effectiveness of internal controls at their organizations. Board members have an opportunity to talk with examiners when they report the results of the exams at Board meetings. This will occur every twelve to eighteen months, depending on your bank's exam frequency. The examiners should be using the Board's time effectively, by highlighting the key issues arising from the exam. They should make the board aware of how new products or processes are changing the risk exposure of the bank. They also should prioritize the areas where internal controls, compliance, risk management, capital, management and governance need to be strengthened. Further, they should give the board a "heads up" about emerging issues that regulators are seeing at similar organizations that boards may want to monitor.

Your examiners are part of an organization that is constantly observing best practices and changing risks and profitability at other financial institutions. Examiners will be glad to respond to any issues you may raise; indeed they provide an independent objective perspective that is not available to non-regulated companies.

Internal Controls

The basics of internal controls for directors and management are simple. Directors do not serve full time, so it is important that senior management 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 internal auditor should test and evaluate the effectiveness of management's program and communicate the results to the board and audit committee. The challenge of the audit committee is to ensure that the internal audit approach is well designed and the

internal audit staff has the expertise, ongoing training, and other resources to meet the specific and changing risks of the organization.

Before a company moves into new and higher-risk areas, the board of directors, management, and the auditors need assurances that they have the tools to ensure adherence to the basics of sound governance. 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.

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. A strong internal audit function can help management fulfill its responsibility to validate the strength of internal controls.

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 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.

Internal Audit

Earlier this year, the Federal Reserve, along with the other federal banking agencies, 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, and I want to use that document to comment on some other aspects of corporate governance that should be considered by directors.

First, the internal audit function must be independent from day-to-day operations. It says, "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.

Second, we take the position that the 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.

Third, 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.

As directors, you should make certain that you are receiving value for audit services. As you hire your independent accountant, or if you outsource internal auditing, look for an auditor who is a partner in a firm with other financial institutions as clients and who is aware of and concerned about emerging risks and best-practice controls. Such a firm will provide resources to ensure that corporate governance and controls are appropriate for your organization and that internal controls evolve to keep pace with changing business practices.

Operational Risk

"Operational risk" is a relatively new concept that began to receive attention at banks and nonfinancial firms as enterprise-risk management began to evolve in the mid-1990s. For purposes of my talk today, I am going to refer to operational risk as any risk that arises from inadequate or failed internal processes, people, or systems or from external events. Examples of operational risk include employee fraud, customer lawsuits, failed information system conversions, and mis-sent wires.

Earlier this year, the Basel Committee on Banking Supervision released a paper titled *Sound Practices for the Management and Supervision of Operational Risk*.[2] This paper sets forth a set of broad principles that should govern the management of operational risk at banks of all sizes. These principles will likely play a key role in shaping our ongoing supervisory efforts in the U.S. with regard to operational risk management. As with the COSO framework, I encourage you to read the sound practices paper, and have included a reference to the source of this publication in the copy of my remarks.

Operational risk has always been part of banking. But the greater variety of products and services that banks 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 operational risks. In a few cases, dominant chief executives perpetrated frauds 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 did not have the information necessary to monitor and understand the growing risks inherent in what appeared to be profitable strategies.

Let me further illustrate operational risks by referring to some guidance that bank regulators issued earlier this year--accounting for subprime credit card activity. For subprime accounts, rapid growth of the account base can mask underlying revenue trends. As new accounts begin to age, the level of charge-offs of fees, finance charges, purchases and advances generally increase. By relying on reports for the portfolio as a whole, rather than by vintage of the account, portfolio growth can mask the increasing amount of losses. Charge-offs of

fees, finance charges, purchases and advances in seasoned accounts at some banks ran higher than 30 percent, rather than the lower level reported when losses were measured by the size of the entire portfolio, including new accounts. Thus, when growth slows, losses catch up. While losses in these portfolios ultimately manifest themselves as credit losses, a major underlying contributor to the losses is the operational risk of inadequate monitoring and reporting. This is a good example of how changes in the customer mix and profit drivers of a traditional banking product can lead to unintended loss exposures if management information and accounting do not reflect the economics and risks of the product when it is altered.

Another example of how controls should change as products are modified is bounced-check protection. Banks have always paid occasional overdrafts for good customers, but recently vendors have been selling programs to banks to market these services to customers. Banks are recognizing the increase in fees for these services, but not all banks are monitoring the changing risk profile and losses that may be inherent in their increased exposures. These marketing campaigns may be changing the traditional prudence of customers to remedy their overdraft positions promptly.

Reputational Risk

Another area of risk that has received attention because of recent events is reputational risk. Bankers know that a critical element of success is customer and investor perceptions of the organization's integrity. When customers select an organization to manage their wealth and financial transactions, they have a few essential expectations--that their privacy will be protected, their transactions will be conducted in a timely manner, the advice they are given will be reliable, and their assets will be invested appropriately and consistently with their financial goals and appetite for risk.

Events of the past eighteen months have shown that customers and investors react quickly when a reputation is tainted. The case of Arthur Andersen has several lessons for bankers, and I want to focus on the reputational risk aspects.

A key component of many banks' strategies is the use of relationship managers. Bankers believe that a single point of contact will help a customer understand the range of the bank's services that are available, will provide a consistent level of service quality, and will increase the cross-selling of services. As a result, customer retention will increase and profitability will improve.

Arthur Andersen had a similar relationship-management strategy. The breakdown occurred because engagement partners who served as relationship managers had the final word on signing-off on accounting policy. Because the engagement partner was compensated on the basis of total revenues paid by the client, the partner had a natural conflict between trying to increase his or her compensation and holding firmly to recognized accounting standards. Further, it appears that Andersen did not have an effective quality-assurance process so that executive management would know when a particular partner was compromising accounting standards to meet his or her own compensation goals. Since the reputation of an independent auditing firm rests on its perceived integrity in ensuring that all its clients meet generally accepted accounting standards, the core value of the enterprise was compromised.

As bankers offer more products via a relationship-management model, they should heed the lessons of the Arthur Andersen incident: Make sure operational controls are in place to monitor the conflicts that the account officer is facing. Controls are especially necessary in the area of credit oversight. Rarely can enough fee income be generated to offset credit

losses. An effective risk-management process can help identify areas of conflict that emerge as new products and management processes are adopted. Risk assessments initiated early in the planning process can give the bank time to get mitigating controls and monitors in place and conduct an internal audit validation of the quality of those controls, before product launch. Thus, risk management functions can be effective tools for bankers to help limit surprises that affect their reputation in the marketplace.

Conclusion

Banks are becoming more differentiated as they choose to serve different customer mixes, focus on specialized activities, or rely on new delivery channels. Thus, it is important that directors make governance and internal control assessments a part of the strategic planning process.

Corporate governance and audit failures over recent months demonstrate how quickly trust can be lost. Reputation and integrity are vital to building and maintaining good relations with bank customers, employees, investors and communities. Good governance and continued attention to internal controls are responsibilities that boards of directors and management cannot afford to neglect.

Many failures of community banks are due to breakdowns in internal controls, thus increasing operational risk. In smaller banks, it is more difficult to segregate duties and hire expertise for specialized areas. Thus it is more important that community banks 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.

Footnotes

1. "Internal Control--Integrated Framework," available from the American Institute of Certified Public Accountants, Order Department, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881; www.coso.org; (phone 1-888-777-7077). Return to text

2. *Sound Practices for the Management and Supervision of Operational Risk*, Basel Committee on Banking Supervision, February 2003, available on the public web site of the Bank for International Settlements: (http://www.bis.org/publ/bcbs96.htm). Return to text

▲ Return to top

2003 Speeches

Home | News and events
Accessibility | Contact Us
Last update: August 7, 2003