# Susan S Bies: Managing business risks

Speech by Ms Susan S Bies, Member of the Board of Governors of the US Federal Reserve System, before the Oregon Bankers Association, Independent Community Banks of Oregon, and Idaho Bankers Association; Sunriver, Oregon, 16 June 2003.

* * *

Thank you for inviting me to participate in the joint annual convention of the Oregon Bankers Association, the Independent Community Banks of Oregon and the Idaho Bankers Association. 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 bankers and supervisors, and to think about how we can better manage the risks inherent in banks.

First I'll focus on some of issues arising from events at public companies and banks in the past eighteen months that have shown weaknesses in risk management practices. And then I'll talk about how operational risk management is evolving into a discipline that can strengthen the corporate governance process at banks.

## Bank earnings and performance

Banks in the United States have experienced two consecutive years of record earnings, despite the recession and slow recovery, losses due to exposures to bankruptcies arising from corporate fraud, and record low interest rates. In 2002, the return on assets rose 16 basis points, to 1.33 percent, the highest level in three decades. The improvements in earnings and ROA are even more remarkable in that they occurred while banks were strengthening their capital ratios. Thus, banks' performance was driven by increased net interest margins, lower relative costs and comparatively constant loan loss provisions.

The ability of bankers to achieve record earnings during a recession and the early part of the recovery reflects the improvement in risk management that occurred in the 1990s. This is especially true in relation to credit and asset/liability risks. Operational risks are a different matter: Banks have had to deal with losses arising from operational issues, as a few well-publicized events have shown.

## Operational risk

"Operational risk" is a relatively new term that has no unique definition. In the mid-1990s the concept began to receive attention at banks and nonfinancial firms as enterprise-risk management began to evolve. 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.

Operational risk has always been part of banking. But the greater variety of products and services that banks 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. An example of this is the growing use of automated loan underwriting systems.

When individual loan officers are responsible for making lending decisions within established credit guidelines, unexpected losses tend to be concentrated. That is, if a particular loan officer is a weak underwriter, only the portion of the loan portfolio generated by that individual shows higher delinquencies and charge-offs. Management could address this risk in many ways, including by providing additional training for that loan officer and by increasing loan-review activities.

Today, many lending decisions are made by automated systems. If the model used for underwriting has a weakness, a systemic asset-quality problem can arise. That is, higher delinquencies are no

longer isolated in a small portion of the portfolio managed by one loan officer. Instead, significant losses can occur simultaneously across the bank's loan portfolio. Avoiding the problems of "model risk" requires more-rigorous oversight of internal controls. The model should be back-tested to verify that the factors it uses deliver the level of losses that was assumed when the loans were made and priced. Avoiding model risk also requires greater data integrity in loan application and underwriting systems, as data errors can also contribute to unintended results.

Many banks today use credit-scoring models to help in mortgage and consumer credit originations. Although most of these models have been shown to be effective in the past few years they have been in use, they have not been tested through a serious consumer-led recession. In the last recession, the weaknesses in asset quality were - and have been since - on the commercial loan side rather than the consumer side. During the period, consumer disposable income continued to grow. The test of the models will come when we hit a period of significantly higher unemployment or falling incomes. Then we'll be able to see if the credit models have reliably predicted the credit losses.

**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. Many of these events reflect operational risk breakdowns. 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 identify the range of the bank's services, 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.

**Accounting**

Over the past year and a half, some organizations have had to restate financial results because of inappropriate accounting. Both corporate financial officers and outside auditors failed to effectively evaluate the sophisticated nature of the underlying transactions and arrive at the appropriate accounting policy. At a few banks, the evaluations were ineffective for special-purpose entities and derivatives. You have all read accounts of these incidents, and I will not dwell on them.

Rather, I want to illustrate operational risk in relation to a basic accounting concept by discussing another area of weakness that bank regulators determined needed attention - accounting for subprime credit card activity. The accounting concept is not new or esoteric. Rather, the nature of the subprime credit card business, compared with that of the prime card business, is to rely much more on fee income than on interest income for revenue. For subprime accounts, rapid growth of the account base can mask underlying revenue trends. Some financial institutions did not have management information that allowed them to track the percentage of delinquent accounts that were not paying late fees and other charges that had been billed.

In such situations, the accounting is very straightforward. Even if you have billed a customer for services, if you do not think you are going to collect the fee, you should not recognize the revenue and should set up a reserve for bad debt. Some financial institutions with a large subprime client base did not have adequate accounting systems to disclose that a significant amount in fees was not being collected. By recording revenue on the basis of billed fees, these institutions were overstating income. New guidance issued jointly by the bank regulators clarifies these accounting standards.

Further, at some subprime banks, management information did not reflect the level of charge-offs of fees and advances as accounts aged. By relying on charge-off reports for the portfolio as a whole, portfolio growth was masking the increasing amount of loan losses. This is a good example of how changes in the customer mix and profit drivers of an existing 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.

**FDICIA: Internal controls**

Other areas of operational risk have come to light as a result of the events and debate surrounding the Sarbanes-Oxley Act. I want to talk about a couple of these areas - internal control assessments and the role of outside auditors.

Since 1991, the Federal Deposit Insurance Corporation Improvement Act (FDICIA) has required that the chief executive officer (CEO) and the chief financial officer (CFO) of all Securities and Exchange Commission (SEC) registrants report on the quality of internal controls. One of the observations that regulators made this past year was that at some banks that had breaks 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. The related lesson is that compliance with a similar requirement in Sarbanes-Oxley will require monitoring by bank regulators to make certain the goal of strengthening accountability and governance is achieved.

Recently, the Federal Reserve and the other bank regulators made known our expectations about the application of Sarbanes-Oxley to small, non-SEC registrant banks. Although we are not requiring that these banks report on internal controls for either FDICIA or Sarbanes-Oxley purposes, recent losses at banks and notable corporate scandals demonstrate that sound governance and internal control practices are important for all banks. Depending on the size, riskiness, and complexity of any bank's business mix, elements of the internal control framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) can provide a process to help identify and monitor areas in which controls should be strengthened. I will describe some ways in which aspects of these processes can assist corporate governance at some community banks.

FDICIA came after the savings and loan failures and a series of corporate governance scandals in the 1980s. In the late 1980s, the COSO issued guidance on best practice in the area of internal controls, and FDICIA adopted this framework. The management report on internal controls that banks issue should be prepared in a manner similar to the COSO framework. FDICIA requires that once a year, managers step back and look at the risks inherent in the businesses and processes they manage, and then 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.

As each manager completes their report on internal controls, the report should go up the chain of command to their boss, who then repeats the process for all of their managed areas. When the report

gets to the top of the organization, the CEO and CFO issue the final management report on internal controls to bank regulators. Further, the external auditor is to review the report and attest to its validity.

At the Fed, we have been looking at the 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 basic 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. In some of these cases, the external auditor did not identify the known failure in the attestations. We are working with banks to make sure this basic control process has substance in the future.

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 bring to their attention recurring concerns - control weaknesses that managers continue to fail to address in a timely manner.

Having seen weaknesses in the quality of external auditors' review of financial reporting and internal controls, the bank regulators have issued an exposure draft to define a policy under which an auditor can be debarred from serving as an auditor of a bank. Bank regulators have had this authority since FDICIA but have not chosen to use it in the past. Regulators have relied on the quality assurance process of public accounting firms and the peer review process of the American Institute of Certified Public Accountants' (AICPA) to monitor the quality of auditors.

But as you all are aware, the events of the past year have clearly shown that these self-regulatory controls have not always been effective. The Sarbanes-Oxley Act established the Public Company Accounting Oversight Board, which will be the regulator charged with monitoring the quality of audit work. Since bank regulators rely heavily on the work of external auditors, we are proposing that bank regulators also lay out the expectations for the quality of audit work and the conditions under which an individual or firm would be debarred from audit work at a bank. We expect to work closely with the Oversight Board, as it gets fully up and running, to improve the quality assurance for audit services.

As bankers, 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 regularly works for another financial institution or is part of a larger organization that 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.

## 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 you make risk management part of your 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.

With the improvements in credit and asset/liability management, failures in operational controls and corporate governance will continue to be a larger source of losses for banks in the future. Thus, all bankers need to formally add the evaluation and mitigation of operational risk to their corporate governance processes.