Susan Schmidt Bies: A supervisory perspective on enterprise risk management

Remarks by Ms Susan Schmidt Bies, Member of the Board of Governors of the US Federal Reserve System, at the American Bankers Association Annual Convention, Phoenix, Arizona, 17 October 2006.

* * *

Good morning. It is always an honor to address the American Bankers Association. Having been a banker, I find it particularly interesting to address this group in my current role as supervisor and central banker. I hope my past private sector experience helps provide a useful perspective on our current regulatory and supervisory policies.

Today I would like to focus on the topic of enterprise risk management. I am quite pleased to see more and more sessions at conferences devoted to risk management, analyzing its different facets and exploring ways to tailor it to specific institutions and situations. Indeed, there is a growing understanding that good risk management should be an integral part of running any type of business. A key theme I would like to highlight today is that all banking institutions should seek ways to improve risk management, but that the methods to improve risk management should depend on the size and sophistication of the institution.

In my remarks I will look at some recent cases in which we believe bankers and supervisors have learned some key lessons about enterprise risk management, or ERM. These lessons demonstrate how good risk management increases business efficiency and profitability. But before I start discussing particular examples, I want to take a step back and give you my thoughts on ERM generally.

General thoughts on enterprise risk management

The financial services industry continues to evolve to meet the challenges posed by emerging technologies and business processes, new financial instruments, the growing scale and scope of financial institutions, and changing regulatory frameworks. A successful ERM process can help an organization meet many of these challenges by providing a framework for managers to explicitly consider how risk exposures are changing, determine the amount of risk they are willing to accept, and ensure they have the appropriate risk mitigants and controls in place to limit risk to targeted levels.

Of course, ERM is a fairly broad topic that can mean different things to different people. For our purposes here today, I will define ERM as a process that enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build stakeholder value. Borrowing from ERM literature, I would say that ERM includes

- aligning the entity's risk appetite and strategies,
- enhancing the rigor of the entity's risk-response decisions,
- reducing the frequency and severity of operational surprises and losses,
- identifying and managing multiple and cross-enterprise risks,
- proactively seizing on the opportunities presented to the entity, and
- improving the effectiveness of the entity's capital deployment.

Some of you are probably familiar with the ERM framework published over a year ago by the Committee of Sponsoring Organizations of the Treadway Commission, or COSO. The COSO framework provides a useful way to look at ERM and helps generate further discussion. In the COSO framework, ERM consists of eight interrelated components derived from the way management runs an enterprise and integrated with the management process: (1) internal environment, (2) objective setting, (3) event identification, (4) risk assessment, (5) risk response, (6) control activities, (7) information and communication, and (8) monitoring. Each of these is described in more detail in the COSO literature.

Notably, the COSO framework states explicitly that, while its components will not function identically within every entity, its principles should apply to all sizes of institutions. Small and mid-size entities, for example, may choose to apply the framework in a less formal and less structured way and scale it to

their own needs - as long as quality is maintained. This underscores the message from bank supervisors that good risk management is expected of every institution, regardless of size or sophistication. Naturally, there will still be some tension between what supervisors expect and what bankers do, but we hope that supervisory expectations for risk management are becoming more and more aligned with the way that bankers run their businesses.

And as most of you know, running a smaller or less complex bank presents different types of challenges and requires a risk management framework appropriately tailored to the institution. For example, smaller organizations often face a challenge of ensuring independent review of processes and decisions since officers and staff members often have multiple responsibilities that can present conflicts of interest.

Having made some general points, I would now like to discuss a few recent examples from banking that highlight the importance of ERM. With the benefit of hindsight, the financial regulators and the industry have been trying to distill the lessons learned from these recently identified weaknesses in risk management and internal control in the financial services sector.

Compliance risk

One area in which ERM provides tangible value is compliance risk. This type of risk may arise when an organization fails to comply with the laws, regulations, or codes of conduct that are applicable to its business activities and functions. The Federal Reserve expects banking organizations to have in place an infrastructure that can identify, monitor, and effectively control the compliance risks that they face. Needless to say, the infrastructure should be commensurate with the nature of the organization's compliance risk. For a large complex banking organization, dealing with compliance risk can be particularly challenging unless it has a well-developed risk management program. On the other hand, smaller organizations with limited staffs face a challenge in keeping up to date with changing regulations.

To create appropriate compliance-risk controls, organizations should first understand compliance risk across the entire entity. Understandably, this can be a daunting task, but I think most would agree that an effective risk assessment is critical. Managers should be expected to evaluate the risks and controls within their scope of authority at least annually. An enterprise-wide compliance-risk management program should be dynamic and proactive. It should assess evolving risks when new business lines or activities are added, when existing activities and processes are altered, or when there are regulatory changes. The process should include an assessment of how those changes may affect the level and nature of risk exposures, and whether mitigating controls are effective in limiting exposures to targeted levels. To avoid having a program that operates on autopilot, an organization must continuously reassess its risks and controls and communicate with all employees who are part of the compliance process. If compliance is seen as a one-off project, an organization faces the risk that its compliance program will not keep up with the changes in its services or customer mix. The board of directors needs to ensure the organization has a top-to-bottom compliance culture that is well communicated by senior management so that all staff members understand their compliance responsibilities. Clear lines of communication and authority help to avoid conflicts of interest.

Compliance-risk management can be more difficult for management to integrate into an organization's regular business processes because it often reflects mandates set out by legislation or regulation that the organization itself does not view as key to its success. For example, bankers understand how vital credit-risk management and interest-rate risk management are to their organizations, because they reduce the volatility of earnings and limit losses. However, regulations enacted for broader societal purposes can be viewed as an expensive mandate. For example, the Patriot Act requires significant reporting of transactions to the government, and many in the banking industry have expressed frustration about the burden associated with such reporting. I can assure you, we recognize banking organizations' investment in and commitment to compliance with regulatory requirements, including those imposed by anti-money-laundering and counter-terrorism regulations. The Federal Reserve will continue to work with our counterparts in the federal government to encourage feedback to the industry on how reporting is contributing to our common fight against money laundering and terrorism.

Operational risk

Over the past few years, the Federal Reserve has been increasing its focus on operational risk. For many nonfinancial organizations, the largest share of enterprise risk is likely to be operational risk, as opposed to credit and interest-rate risk. Banks have learned much from the practices that nonfinancial firms have developed over the years. Operational risk has more relevance today for bankers largely because they are able to shed much of their interest-rate and credit risk through sales of loans, use of financial derivatives and sound models to manage the risks that are retained. Further, the fastest-growing revenue streams are increasingly related to transaction processing, servicing accounts, and selling sophisticated financial products. To be successful, organizations must have complex systems to execute these activities. Banks are also utilizing advanced models to estimate and manage credit risk and market risk exposures. Growing use of sophisticated models requires stronger risk management practices since weaknesses in the models' operational design and data integrity can lead to significant losses. Thus, effective risk management requires financial institutions to have more-knowledgeable employees to identify system requirements, monitor their effectiveness, and interpret model results appropriately.

We have learned quite a bit about operational risk from our examinations of banking organizations. For example, during routine examinations we look at the adequacy of banks' procedures, processes, and internal controls. Such reviews include transaction testing of control routines in higher-risk activities. For example, a bank's wire transfer activities and loan administration functions are often targeted for review, and our experiences have identified some common weaknesses in operational control that are worthy of attention.

With wire transfers and similar transactions, a banking organization could suffer a significant financial loss from unauthorized transfers and incur considerable damage to its reputation if operational risks are not properly mitigated. A few recurring recommendations from our reviews are to (1) establish reasonable approval and authorization requirements for wire 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 customers' 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 another area where banking organizations could suffer significant financial losses from inappropriate segregation of duties or lack of dual controls. An institution could also incur considerable damage to its reputation if operational risk factors are not properly mitigated. A few recurring recommendations from these types of reviews that may be applied to corporations more generally are to (1) ensure that loan officers do not have the ability to book and maintain their own loans; (2) confine employee access to only those loan system computer applications that are consistent 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.

Mortgage lending

Effectively managing the risk of a mortgage portfolio involves much more than prudent underwriting. Experienced risk managers should understand the need to temper their enthusiasm during boom times by considering carefully the accompanying risks. These risks include the possibility that expectations for future income growth for marginal borrowers may be optimistic. In addition, there could be an accumulation of outsized portfolio concentrations that leave the institution exposed to a downturn in that sector. And the need to consider these risks is most pronounced when competition among lenders for market share is most intense.

During the recent housing boom, faced with soaring home prices and rising interest rates, many borrowers have sought to lower their debt service obligations by turning to mortgages with nonstandard payment and amortization schedules. Much of the new loans extended in the past two years have been nontraditional mortgages, including adjustable-rate mortgages with teaser rates and negative amortization features. At the same time, some banks have weakened proof of income and appraisal standards, and did not fully assess borrowers' ability to pay when interest rates rise and full amortization begins. In addition, a fair share of the recent lending with nontraditional products has been in the subprime market.

Net housing wealth (as a multiple of income) also jumped over the same period. To some extent this increase is a source of comfort, providing larger collateral cushions to lenders. And a solid base of

household housing wealth has been important to household confidence and influenced their appetite for consumption spending. But we know from experience the risks of extending credit with too much emphasis on collateral values. A borrower's equity in his or her home matters most when a property is foreclosed, something that both lenders and borrowers would prefer to avoid. Having equity in a home can provide an added incentive for borrowers to stay current on their loans, of course, especially for second homes and investment properties. Most important, borrowers want their home mortgage payments to remain current, and that requires cash flow that is adequate to comfortably service the loan.

At present, mortgage delinquencies remain low, although delinquencies on subprime mortgages have risen in recent months. The recent rise in subprime mortgage delinquencies has been concentrated among adjustable-rate subprime loans, which is probably related to interest rates resetting - as the first reset tends to occur much earlier for subprime ARMs than prime ARMs. The outlook for mortgage credit quality remains favorable, but modestly cautionary signs are on the horizon. We have had clear initial signals in recent months that housing prices are no longer rising as they had been and are declining modestly in some key markets. Growth in housing wealth may slow or stagnate while the debt service obligation continues to rise, as teaser rates expire and fully-indexed loan rates eventually catch up with increases in market rates. While we continue to expect that mortgage delinquencies will remain manageable, lenders should closely monitor future developments.

Information security

Issues involving information security and identity theft have received quite a bit of attention from the federal government over the past several years. Not too long ago, President Bush signed an executive order that created an Identity Theft Task Force for the purpose of strengthening federal efforts to protect against identity theft. The heads of the federal bank regulatory agencies are designated members of this task force; and as supervisors of financial institutions, I believe we can offer a valuable perspective on this issue.

As you have probably noticed, cyber attacks and security breaches involving nonpublic customer information appear in the headlines almost every week. These events have cost the financial services industry millions of dollars in direct losses and have done considerable reputational damage. The cost of identity theft to affected consumers is also significant. Banking organizations' increased use of the Internet as a communication and delivery channel have resulted in the need for and use of more-sophisticated control mechanisms, such as enterprise-wide firewall protections, multifactor authentication schemes, and virtual private-network connections.

While many of the widely publicized information security breaches have involved parties outside the affected banking organization accessing the organization's customer information, organizations also remain at risk for breaches or misuses of information by an insider. During our examination activities, we have seen operating losses that were traced back to weak controls over insiders' access to information technology systems interfacing with electronic funds transfer networks. Further investigation into these situations suggests that the duration and magnitude of the fraud and resulting losses is a direct function of the internal party's access to accounting and related systems.

Several lessons have emerged. First, institutions should tightly control access to funds transfer systems and ensure that access settings enforce separation of duties, dual controls, and management sign-offs. Second, an institution's senior management should be restricted from regular access to business-line functional systems, especially funds transfer systems. When such restriction is impractical, additional controls must be in place and functioning effectively. Finally, effective management of information security risk, even when focused on a specific function, requires an enterprise-wide approach to yield a true and complete evaluation of the associated risks.

Portfolio credit risk

Portfolio credit risk also should be recognized and managed across the entire organization. In some cases, firms may be practicing good credit risk management on an exposure-by-exposure basis, but they may not be paying close enough attention to aggregation of exposures across the entire organization.

Practicing good portfolio credit risk management is not easy. Institutions often encounter challenges in aggregating exposures and identifying and measuring credit concentrations within the entire portfolio.

Naturally, supervisors from time to time have concerns about growing credit risk concentrations at banks and bankers' ability to manage them. A current example is commercial real estate (CRE). Recently, the U.S. banking agencies issued proposed supervisory guidance on managing CRE concentrations.

While banks' underwriting standards are generally stronger than they were in the 1980s, the agencies are proposing the CRE guidance now to reinforce sound portfolio management principles that a bank should have in place when pursuing a CRE lending strategy. A bank should be monitoring performance both on an individual loan basis as well as on a collective basis for loans collateralized by similar property types or in the same markets. In addition, while lending to different geographic areas can provide diversification, bankers should be mindful of potential problems when they begin to lend outside their market or "footprint," where they normally have better market intelligence. In recent years, supervisors have observed banks lending outside their established footprint - to maintain a customer relationship - into real estate markets with which they have less experience.

One misconception about our draft CRE guidance relates to the proposed explicit thresholds. Contrary to what many think, these thresholds are not intended as hard limits. Rather, the thresholds should be viewed as supervisory screens that examiners should use to identify banks with potential CRE concentration risk. Examiners would expect organizations to strengthen their portfolio risk management as CRE concentrations grow. This would include effective monitoring of emerging conditions in the real estate market segments where a bank is lending. Institutions are expected to conduct their own analyses of CRE concentration risk and establish their own concentration limits. Institutions, after all, are in the best position to identify and understand their concentration risk and it is the job of supervisors to confirm that institutions are indeed doing so.

Conclusion

At the Federal Reserve, we believe that all banking organizations need good risk management. An enterprise-wide approach is appropriate for setting objectives across the organization, instilling an enterprise-wide culture, and ensuring that key activities and risks are being monitored regularly. Clearly, there is always an opportunity to improve upon ERM strategies and maintain the proper discipline to implement them effectively. In addition, bankers should be mindful that problems can sometimes quickly arise in a business line or unit that has presented no past difficulties. Accordingly, it is always helpful to evaluate the "what if" scenarios even for the most pristine of business units.

But the manner in which risk management challenges are addressed can - and should - vary across institutions, based on their size, complexity, and individual risk profile. In many cases, it simply does not make sense for small organizations to adopt the most sophisticated risk management practices - but that does not absolve such smaller institutions of their responsibility to improve risk management. Additionally, as supervisors, we want to ensure that institutions are not only identifying, measuring, and managing their risks but also developing and maintaining appropriate corporate governance structures to keep up with their business activities and risk taking. Our hope is that the guidance we offer to bankers on these various topics is becoming more consistent with their own risk management practices.