Susan Schmidt Bies: A bank supervisor's 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 Enterprise Risk Management Roundtable, North Carolina State University, Raleigh, 28 April 2006.

* * *

Thank you for the invitation to speak today. As you likely know, I am quite interested in the discipline of enterprise risk management (ERM) and believe roundtables such as this are a useful way to share perspectives and approaches to sound ERM. I know that these roundtables cover a wide range of industry sectors, but today I will, naturally, focus on ERM from a banking perspective. I will use some recent cases in which we believe bankers and supervisors have learned some key lessons about ERM and describe how the lessons learned can be more broadly applied to other industries. But before I start discussing particular examples, I want to take a step back and give you my thoughts on ERM more broadly.

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. The Federal Reserve Board, as the primary supervisor of state member banks and the consolidated supervisor of financial holding companies, has been working with other regulators and financial institutions to improve the effectiveness and relevance of regulation and supervision in this changing environment. The Federal Reserve has long emphasized the need for appropriate and strong internal controls in institutions we supervise, and we have taken a continuous-improvement approach to our risk-focused examinations. For many years, enterprise risk management across multiple organizational units within an entity has received increased scrutiny.

In some cases, firms may be practicing good 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. Rapid growth can place considerable pressure on, among other areas, an organization's management information systems, change-management controls, strategic planning, credit concentrations, and asset/liability management. An organization must also understand how its various business components, some of which can be quite sophisticated and complex, dynamically interact. A successful ERM process can help to meet many of these challenges.

Of course, enterprise risk management 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.

Many 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--just what this ERM roundtable is trying to promote.

In the COSO framework, ERM consists of eight interrelated components that are derived from the way management runs an enterprise and that are 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.

- *Internal environment*.The internal environment--the *tone* of an organization--is a reflection of the organization's risk-management philosophy, risk appetite, and ethical values. It determines how risk is viewed and addressed by employees throughout the organization. This tone is established at the very top of the organization.
- *Objective setting*. Objectives must exist before management can identify events that could affect achievement of objectives. The board of directors approves corporate objectives, and management is responsible for achieving them. Enterprise risk management ensures that the board has in place a process for setting appropriate objectives, which support and align with the company's mission and are consistent with its risk appetite.
- *Event identification*. Internal and external events that could affect achievement of a company's objectives must be identified and measured, and a distinction must be made between risks and opportunities. Opportunities are channeled back to management's strategic-planning or objective-setting processes.
- *Risk assessment*. The likelihood and the potential impact of various risks are analyzed, as a basis for determining how the bank should manage risks. Risks are assessed on an inherent and a residual basis.
- *Risk response*. Management selects risk responses--avoiding, accepting, reducing, or sharing risk--and develops a set of actions to align risks with the organization's risk tolerances and risk appetite.
- *Control activities*. Policies and procedures are established and implemented to help ensure that the desired risk responses are effectively carried out.
- *Information and communication*. Relevant information is identified, captured, and communicated in a form and timeframe that enable managers and staff to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing across and up and down the organizational structure. Companies often use key risk indicators and key performance indicators to facilitate this communication.
- *Monitoring*. The organization's entire enterprise risk management process is monitored, and modifications made as necessary. Monitoring is accomplished through ongoing management activities and separate evaluations. It is a continuous process, unlike testing and auditing, which are periodic.

Having laid out some general thoughts about ERM within the COSO framework, I would now like to discuss a few recent examples from banking in which the importance of ERM has been highlighted. With the benefit of hindsight, the financial regulators and the industry have been trying to distill the lessons learned from these recent breakdowns in risk management and internal control in the financial services sector.

Compliance risk

One area in which ERM provides tangible value is the area of compliance risk, which can be defined as the risk of legal or regulatory sanctions, financial loss, or damage to an organization's reputation and franchise value. 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.

To create appropriate compliance-risk controls, organizations should first understand compliance risk across the entire entity. Managers should be expected to evaluate the risks and controls within their scope of authority at least annually. I should also emphasize the need for the board of directors to establish a top-to-bottom compliance culture that is well communicated throughout the organization by senior management so that all staff members understand their compliance responsibilities and their

role in implementing the compliance program. Clear lines of communication and authority help to avoid conflicts of interest.

An enterprise-wide compliance-risk management program should be dynamic and proactive, meaning it constantly assesses evolving risks when new business lines or activities are added or when existing activities and processes are altered. 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. This understanding must be constantly evolving, to keep up with not only the organization's own products and business strategies, but also regulatory changes. To avoid having a program that operates on autopilot, an organization must continuously reassess its risks and controls and communicate with its business lines. Also, if compliance is seen as a one-off project, undertaken only when a new regulation or product is introduced, a banking organization is placing itself at risk that, down the road, the lack of a compliance process will not sustain the effectiveness of the program as the organization changes.

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. On the other hand, regulations that are enacted for broader societal purposes, but that the enterprise sees as of little benefit to its revenue growth, can be viewed as an expensive mandate. For example, the Patriot Act requires significant reporting of transactions to the government, and many in 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 enhanced feedback 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 those of you in nonfinancial organizations, the largest share of your enterprise risk is likely to be operational risk, as opposed to credit and interest-rate risk. Banks have learned much from the practices that you 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 revenue streams that are growing the fastest 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 of activities that pose operational risk, 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) limit employee access to those 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.

Operational risk arising in recent financial restatements

Risks can sometimes quickly appear where they were not traditionally expected. For example, consider the changes we have seen in financial reporting quality of corporations in all industries. In 2005, there were approximately 1,200 restatements of previously filed financial statements by publicly traded companies--twice the rate for 2004. The complexity of GAAP accounting standards and a more stringent, literal interpretation of the application of those standards by auditors and regulatory bodies, primarily the Securities and Exchange Commission, are two major factors that have led to the restatements.

Examples of prominent restatements include FAS 133 hedge accounting and lease accounting issues. In the area of hedge accounting, the restatements generally resulted from the misapplication of the "short-cut" method. The organizations in question did not satisfy all of the criteria for use of the short-cut method but, nonetheless, utilized hedge accounting treatment allowed by this method.

In the area of lease accounting issues, most companies simply failed to apply longstanding accounting standards related to revenue recognition reserves, accruals and contingencies, and equity accounting. Most companies believed they were actually reporting correctly prior to the restatements. Virtually all of these companies were audited by auditing firms that are now registered with the Public Company Accounting Oversight Board (PCAOB). The PCAOB's inspection process, which involves close scrutiny of registered firms, may be a factor in the increased number of restatements.

Section 404 of the Sarbanes-Oxley Act of 2002 requires each annual report of a public company to include a report by management on the company's internal control over financial reporting. Looking only at banking organizations, as a result of restatements, the number of material weaknesses in internal control for the 2004 reporting period has been revised up to 52 from the 37 originally reported. This increase implies a significant amount of operational risk associated with the accounting process.

Generally, examiners review the Sarbanes-Oxley 404 process to determine whether the organization has a clear understanding of the roles of the audit committee, management, internal audit, and the external auditor and whether the organization has implemented an effective plan to achieve the objectives and requirements of Sarbanes-Oxley 404. Examiners also review the Sarbanes-Oxley 404 process to determine whether the organization has an effective follow-up strategy for the remediation of significant deficiencies and material weaknesses. Examiners are encouraged to utilize the results of the Sarbanes-Oxley 404 process, where possible, in their overall assessment of the organization's risk management and control process and in the risk scoping of safety-and-soundness examinations and inspections.

Information security

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. With banking organizations increasingly using the Internet to interact with customers, business partners, and service providers, concerns about the 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 breakdowns in internal control, resulting in 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 logical 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.

Mutual funds

Well-publicized instances of late trading and market timing at mutual fund firms, and the related investigations, have involved many businesses, including banking, securities, and insurance firms. These types of breakdowns in internal control result in sanctions or financial loss and adversely affect a firm's reputation and franchise value.

I would like to highlight a few lessons learned from our experience in investigating control breaches in these mutual fund cases. One of the most obvious is the need to critically evaluate unusual client relationships that require variances from standard procedures. If a high percentage of compensation is derived from a single client, a red flag should immediately go up. Also, organizations should have a formal process for reviewing and approving unique products, customers, and services at the inception of the client relationship. Further, it is always a good idea to shine some light on areas historically labeled "low risk" to validate that assessment. The low occurrence of loss from an activity should not be the only factor considered when assessing risk.

Finally, compensation systems that reward employees for sales without adequately monitoring their internal control breaches can create a conflict between the interest of employees and the interest of the enterprise. As companies move away from straight salaries to more incentive-based systems, it is important that personnel departments be included in an effective enterprise-wide risk-management program to consider how changes in compensation practices affect risks to the enterprise.

Credit derivatives

Finally, I would now like to turn to one more issue that has relevance to ERM, and that is the importance of companies including an ERM perspective as they design and build new lines of business. As many of you might know, last year a dialogue between supervisors and credit derivatives dealers was initiated to support industry efforts to address weaknesses in the operations surrounding credit default swaps (CDS). While we view these new instruments as an effective way to diversify and mitigate risks related to credit exposures from corporations, an industry-led study, the Counterparty Risk Management Policy Group II report, identified significant weaknesses in the infrastructure supporting sales and risk monitoring of these instruments. While the report identified 47 recommendations, regulators in the United States and other countries have focused on two major weaknesses.

One weakness is related to the success of the product. Volume of trades has grown so quickly and reached such a significant volume that broker-dealers are not able to keep up with their paper-based systems to record the trades and document the transactions. As a result, significant backlogs of confirmations of these over-the-counter derivatives have built up. This creates concerns that information feeding risk-management systems--information about the volume, term, and counterparty to the trade--is not complete. This problem would be exacerbated in a stress situation, when positions need to be changed very quickly to mitigate risk.

Another weakness relates to the lack of discipline in enforcing contract terms. Any time an instrument is traded over the counter, it is important to know who you are doing business with. Since an exchange does not stand between the two sides of the trade, parties make payments directly to each other to honor the terms of the contracts. The market practice is to use collateral or pricing to mitigate the risk that the other side of the trade cannot perform per the agreement. The recent industry study also found that competitive pressures were such that brokers did not enforce the standard CDS agreement

and allowed counterparties to assign their side of the trade to another party without notifying the broker. Obviously, this can significantly change the risk profile of a transaction and also make it very difficult to settle payments in a timely manner.

About six weeks ago, fourteen major market participants published a letter reiterating their commitment to improving the infrastructure that supports the credit derivatives markets. The market participants are committed to the development and implementation of a set of industrywide guidelines that include a targeted reduction in each market participant's confirmation backlogs and assurance that agreement terms will be enforced. Additionally, the fourteen participants will work to create a largely electronic marketplace where all trades will be processed through an industry-accepted platform, develop a new set of processing standards for those trades that cannot be confirmed electronically, and establish a new procedure for settlement following a credit event.

We are generally pleased with both the industry's self-identification of the issues and its commitment to making improvements. But for purposes of our discussion of ERM today, the problems surrounding CDS sales highlight the challenges risk managers face when market pressures make the firm's line management reluctant to initiate appropriate controls on their own. It also illustrates that in new lines of business, sometimes ERM must go outside the enterprise and work with competitors to support the growth of shared systems and standards to mitigate risks.

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. Senior management must be involved in ERM, since they are the ones who decide the level and types of risk the organization is comfortable with accepting and what controls and risk mitigants will be employed to ensure that risk exposures stay within the agreed-upon levels.

In addition, it is important for organizations to make sure they do not ignore or accidentally overlook lower-profile activities that still might bear substantial risks. As I noted, such activities can include financial statement reporting, information security, and back-office systems. And operational risk, more broadly, has the potential to create disruptions for the organization that could reduce the value of the organization. Often, the solutions to these problems are basics such as training, developing internal controls, and establishing the appropriate culture across the organization. Therefore, organizations should look at the discipline of enterprise risk management as a way to ensure that they effectively deal with uncertainty and the associated risk and opportunity.

Thank you.