FEDERAL RESERVE BANK *of* NEW YORK *Serving the Second District and the Nation*

SPEECH

Operational Risk Management - Current Issues and Supervisory Concerns

March 22, 2004

William L. Rutledge, Executive Vice President

Remarks by William L. Rutledge before the ABA/Foreward Financial Operations Conference in Orlando, FL

Introduction

Thank you Jim. Let me also thank Mike ter Maat for inviting me to speak and, more broadly, the ABA for organizing this conference. From my perspective as a bank supervisor, conferences that promote greater awareness of operational risk issues, and management approaches for them, are most timely and important. Without question, operational risk management has become a major element of our supervisory assessment process in the past several years. And our concerns have been further intensified by the spate of recent events that demonstrate the costs of operational risk shortcomings.

As one of the first speakers at the conference, I thought I would begin by offering a broad supervisory perspective on operational risk management, and then do a quick run-down of a few of the more specific operational risk management issues before us today—highlighting, for each, various supervisory concerns, expectations, and challenges.

One of the obvious first steps in describing operational risk management is to define what we mean by operational risk. Operational risk has of course always existed in banking, as well as in other industries, but the perception of what it constituted was typically very narrow. If you had asked bankers even just a handful of years ago to describe the operational risks of their firms, you would have likely gotten a limited response referring to processing operations, or maybe some generalized references to "back office" risk.

Today, the concept of operational risk is recognized as being much broader than that. A definition of operational risk that has been used by the Basel Committee for regulatory capital purposes is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Clearly, that definition was designed for the specific purpose of framing a regulatory capital requirement. As such it covers quite a bit of ground. But in my view, having a similar broad starting point to identify the range of operational risk concerns also makes a great deal of sense. I say that because I see a number of common elements relevant to overseeing the broad range of operational risk concerns, even if the specific method of managing or measuring a particular subset of the risks varies from one to another.

Let us look at that broad range of kinds of operational risk exposures. It is very easy to make a list of the numerous ways in which operational risk can manifest itself, just by culling from the events of the last few years. For example, the events of September 11th and the Northeast blackout of last summer, directly impacted the back offices of financial institutions, and in that one sense they fit the narrow view of an externally-driven operational incident. Another example—the very large foreign exchange trading loss at Allfirst Bank—resulted from the breakdown of fundamental internal control processes, specifically, a lack of appropriate segregation of duties. While this latter example reflects internally driven shortcomings cutting across various business processes of the firm, it too comports with a traditional view of operational problems.

Going even further away from classic back office concerns, the more expansive definition of operational risk would encompass many of the situations that have dominated financial news in the past year or two—including corporate failures such as Enron and Parmalat. As you know, in addition to incurring direct credit losses from Enron, some banks that engaged in complex, structured financings with the company reached settlements with various government agencies totaling hundreds of millions of dollars. And they have additional exposure in the form of civil litigation. Clearly, potential and realized losses such as these are captured in the broader concept of operational risk. The same can be said for the costs and penalties arising from the investigations of mutual fund practices.

The question I would pose is whether there are some broad elements an institution should ensure are in place, so that it will have its arms around this diverse a range of concerns. Whether our focus is on processing problems, breakdowns in basic internal controls, or various new ways in which operational risk may manifest itself, several principles essential to managing operational risk apply. Let me briefly highlight them.

First is the need for those at the very top of the organization to focus on operational risks and their management. The board of directors and senior management must establish, and then periodically review, an operational risk framework for the firm. That framework should make clear the range of risks to be covered by the program and outline how they are to be identified, assessed, monitored and controlled across the various lines of business within the firm.

Second, beyond whatever is spelled out in a framework's formal policies and procedures, senior management must instill a strong control culture. This, of course, is much easier said than done given all the various factors, tangible and intangible, that must come together to create a culture. There are some immediate questions that come to mind—answers to which should provide some helpful insights into how a firm is run.

- For example, what are the bank's incentive structures? Are the people responsible for specific business lines held accountable, in ways that really matter, for all aspects of the business, including the quality of control of the operations? Are managers rewarded financially solely, or virtually solely, on the basis of the earnings of their units? Or does the performance of their units, as reflected in audits and compliance reviews, directly and materially affect their compensation?

- Another example. How are decisions made on shifting business strategy or introducing new products? Are those decisions made solely by the business area and corporate strategists or are appropriate control personnel—such as those in the risk management, accounting, and legal functions involved in the decision-making process?

- Lastly, what is the role of internal audit—do auditors have unfettered access to information and to people, and how seriously are their findings

taken?

- Answers to these questions will go a long way to determining whether a bank has a sound control culture.

A third principle, essential to sound operational risk management, is the need for effective internal analysis, reporting and information sharing. We have observed that banks with more proactive approaches to operational risk management employ a range of tools, including key risk indicators (or KRIs), self-assessments and, the collection of operational risk loss data. Having sound metrics through the design of good KRIs and through the collection of loss data are very important, but I would particularly single out self-assessments as a key part of the process. From a supervisory perspective, we view well-designed and well-executed control self-assessment programs—where the onus is on individual business units to identify control weaknesses or gaps—as critical for large, complex firms.

Now, let us move from a conceptual discussion of supervisory principles to seeing how those principles apply in setting our expectations for several, high profile issues drawn from your conference agenda: outsourcing, business continuity, and operational risk capital. I will spend my remaining time focusing on these three issues, beginning with outsourcing.

Outsourcing

I know this audience is keenly aware of the degree to which financial institutions rely on outsourcing. Within the area of IT, outsourcing has expanded beyond mainframes to encompass mid-range and distributed computing, as well as data and voice networks. Today, it is also typical for various business processes—such as customer call centers, back office processing and, more recently, accounting and finance functions to be outsourced.

Another broad trend that you are aware of concerns firms moving some of their operations out of the United States. This activity may take the form of outsourcing to a third party located abroad, or having a subsidiary or affiliate (as opposed to a third party) provide services from an offshore location.

Outsourcing arrangements may give rise to significant risk management and supervisory issues. The over-arching principle we emphasize is that transferring some of the day-to-day decision making to someone else does not in any way diminish the responsibility the banking organization has to itself, and to its supervisors, to ensure that risks of those operations are being well addressed. But in addition, the organization has to recognize that it is exposed to new risks from the relationship with the service provider and must take steps to ensure that such risks are addressed.

- This should begin with extensive due diligence and careful contract negotiations. Not only is it critical that expectations pertaining to the level of service be carefully spelled out, but provisions establishing termination arrangements, should they become necessary, must also be very clear.

- The bank's responsibilities extend to monitoring that the service provider is performing as agreed, including ensuring that the service provider's own operational controls are working well.

- Its responsibility also extends to ensuring that the service provider is in sound financial condition—effective short-term performance means little if the long-term viability of the service provider is in question.

One of our key starting points in the supervision of banking organizations is that we must be able to obtain a complete picture of the risks they face. In this vein, outsourcing arrangements cannot be allowed to impair our ability to assess the risks of, and to effectively supervise, financial institutions. Therefor, in our discussions with banks, and our evaluations of their systems, we will continue to include fully the operations that have been outsourced. Our starting point is the same—we expect you to understand the full set of your risks and to demonstrate to us that those risks are being effectively managed. And we need to be able to validate those matters—which could pose a problem if key operations are outsourced overseas.

Information security and business continuity top the list in terms of potential supervisory concerns with outsourcing. Among our information security concerns is the question of how well the organization complies with consumer privacy laws. Another is how strong the process is for safeguarding data and computer networks. This is much on our minds today given the increasing public focus on computer hacking, viruses and worms.

These issues are especially important when systems are made available to vendors as part of an outsourcing arrangement. Banks must have mechanisms to ensure that these major information security issues are being well handled throughout their outsourced functions.

With respect to business continuity, outsourcing arrangements require banks to not only look inward, but also to the state of preparedness of its service providers should a disruption occur. I recognize the challenges involved in doing this, particularly when a financial institution has relationships with multiple service providers, but these challenges must be faced very directly by the banking organization. At the same time, banking organizations are also key service providers—their responsibilities in this regard must be carefully considered when developing and implementing contingency arrangements.

The potential risks associated with IT security and business continuity are further amplified in cross-border arrangements. As such, when contemplating such arrangements, bank management should take into account the full range of potential risks associated with doing business overseas. Such issues as differences in legal requirements—and potential shifts in such requirements—have to be focused on by both the bank and its supervisor.

There also is a range of more subtle risks associated with outsourcing. Are decisions regarding such arrangements made in a truly strategic manner? Or, are the decisions being driven by individual business lines in a potentially uncoordinated fashion? In other words, is senior management taking a systematic look across the firm to identify the full range of activities that might be outsourced, based on a set of well-defined parameters? As more critical functions are designated for outsourcing (whether within the U.S. or abroad) I see the need for a more strategic approach to ensure that senior management is fully cognizant of the risks and trade-offs the institution as a whole is assuming. This expectation ties back to one of the key principles I highlighted earlier in my remarks, namely that it is the responsibility of a firm’s board and senior management to set clear strategies and oversee their execution.

Business Continuity

Let me take a few moments to elaborate on the risks associated with business continuity arrangements more broadly. As business processes become

more globally connected, the magnitude and speed with which problems may be transmitted to others could have real implications for systemic risk. Further, there are new threats to address. While natural disasters historically have been a focus of business continuity planning, the events of September 11th have brought terrorism squarely into the portfolio of risks facing us all.

Of course, the U.S. supervisory agencies have long had in place guidance pertaining to business continuity. We have periodically updated such guidance—for example, recently by building in more explicitly the need for a stronger risk management orientation to the business continuity planning process.

Moreover, in the aftermath of September 11th, we also focused particularly intensively on ways of mitigating risk in systemically important business areas, such as clearance and settlement within various critical markets. As many of you know, in April 2003, the Federal Reserve, the OCC and the SEC published a sound practices paper on strengthening resilience in such activities.

The paper points to the need for institutions to identify the activities within their firms that support clearing and settlement within critical financial markets and then to identify recovery and resumption objectives. Clear guidance is provided in the paper on the amount of time those processes should take. The sound practice that received the most attention concerned the need for banks to achieve sufficient geographic separation between primary and back-up sites while maintaining these recovery objectives.

That guidance is now quite firmly entrenched in our supervisory framework, and I think there is good support for its principles among industry participants. However, there will clearly be some challenges in ensuring the full and effective implementation of the principles.

One of the challenges is to make sure that all of the parties involved—the whole set of supervisors and the industry—continue to have a strong dialogue to ensure that the principles are applied in a consistent and appropriate manner. I think that the development of the principles was greatly enhanced by the interaction among the U.S. supervisory agencies, and between the supervisors and the firms involved. Implementation of these principles will benefit from a continuation of such structured discussions.

Another challenge to effective business continuity relates to the extent of the financial industry's reliance on telecommunications. In the aftermath of September 11th, significant risks within the telecommunication infrastructure were identified. We expect organizations to actively manage the resilience of their telecommunication links for both voice and data, with such efforts encompassing both the design and the maintenance of their communication networks. In particular, it is critical that firms work with their vendors to periodically conduct an inventory of their telecommunication circuits to identify points of commonality to find potential single points of failure.

While there is much an individual firm can do to address the reliability of its telecommunication connections, we recognize that these efforts need to be coordinated with others. This is why it is important for all interested parties—financial institutions, telecommunication service providers and governmental agencies—to work together to ensure telecommunications diversity and resiliency.

Another challenge stems from the ability of firms to test continuity arrangements across firms or industry segments. Testing is of course an essential element to ensure satisfactory contingency planning. Designing and carrying out effective tests within critical financial markets is no easy task, given that such markets typically have many interdependent parts. Ensuring that tests are meaningful, practical and affordable is therefor a challenge for the industry and supervisory authorities.

A final thought on contingency arrangements. Intuitively, I think we would all agree there are some clear benefits to having strong contingency arrangements, but how much value to attach to them may be less clear. From a supervisory perspective I see a need for financial institutions to be able to better quantify those benefits. It seems to me that further work in this dimension would have tremendous value not only in understanding the need overall for strong investments for business continuity, but by allowing firms to allocate resources more effectively.

Operational Risk Capital

Alluding to this kind of quantitative analysis provides a neat segue to my final topic of operational risk capital. As I have mentioned earlier in my remarks, the concept of operational risk has evolved from a fairly narrow focus on back office operations to one that is much broader in scope, in significant part because of the prospect of a change in capital regime. The Basel Committee, of which I am pleased to be a member, views operational risk as a significant risk, necessitating the holding of capital to protect against losses. Accordingly, it has been explicitly captured within the Pillar I minimum capital requirements of Basel II.

The need for an explicit operational risk capital charge also became clearer as we sought to build a more sophisticated capital regime for capturing credit as well as market risk, and recognized that operational risk may arise in part as a result of techniques aimed at mitigating or transferring credit or market risk. For example, one might focus on the potential for the netting and collateralization of OTC derivative trades to reduce measured credit exposure. However, it is also important to emphasize that those very same techniques—which require legally enforceable netting contacts, effective collateral management systems and timely margining—also create operational risk exposure. The same can be said of securitization activities where the transfer of credit risk introduces elements of operational risk. Accordingly, if increased focus were placed solely on refining the measurement and management of credit risk and market risk, there was a very real potential for banks and supervisors to overlook operational risk as a significant and potentially increasing source of possible losses.

By design, the Basel II approach to operational risk builds upon banks' rapidly developing internal assessment techniques. It also seeks to provide incentives for banks to improve upon them, and more broadly to improve their management of operational risk over time. This is particularly true of the Advanced Measurement Approaches to operational risk (or AMA), which are the focus of my remaining remarks.

Now, I view the principal goal of regulating and supervising banking organizations as to promote and to enforce sound practices while allowing and encouraging banks to innovate and to compete. In other words, the aim is to create an environment that promotes healthy, disciplined risk-taking by banks. We do this partly by laying out a broad framework of requirements through regulation, and partly through exercising supervisory judgment in assessing the performance of individual firms. The complementary roles of regulation and supervision are well illustrated by the issuance of an Advance Notice of Proposed Rulemaking (or ANPR) on Basel II—which was accompanied by draft supervisory guidance.

As you know, the ANPR indicates that the U.S. agencies intend that the AMA approach to operational risk will be adopted by the large, internationally-active U.S. banks. The AMA is particularly attractive to me as a supervisor because it is grounded in the need for banks to have a strong risk management and control framework. I anticipate that as those techniques are further refined there will be benefits not only for the banks subject to the AMA, but for banks of all sizes as the enhancements spread across the industry. The further improvement in operational risk management techniques by banks generally—including banks that will not be subject to the new operational risk capital charge—is a development that I would view very positively.

In any event, issuing the draft supervisory guidance was important in order to provide a detailed explanation of our current thinking on what we would specifically expect of the AMA banks, but doing this work was also important in order to flesh out in our own minds what we as supervisors need to do to prepare. Let me turn now to the implications for first, the banks that would be subject to the AMA, and then their supervisors, of introducing a regulatory capital framework for operational risk with the flexibility of AMA.

Implications for AMA Banks

For banks subject to AMA, a key, as I have suggested, is that the supervisory guidance establishes a very close link between risk measurement and risk management. Operational risk capital assessments must be one component—although of course a very important one—of a sound risk management and control framework. As I have emphasized throughout my remarks today, we expect all firms to demonstrate a clear understanding of their potential exposure to losses from a range of operational risk failures relevant to their specific business mix. Further, we expect them to establish an effective decision-making and control framework for those risks. Having a sound risk management and control environment is a prerequisite for the AMA approach, but once achieved, the draft supervisory guidance gives banks considerable flexibility in deriving their operational risk capital charge.

Our discussions with the AMA banks indicate that they are in various stages of putting into place the necessary management and measurement elements. Most already have an independent operational risk management function, along with corporate policies for managing and assessing this risk. An increasing number of such banks have also been heavily engaged in developing or enhancing an analytical framework to quantify operational risk.

I should note that the AMA supervisory guidance does not prescribe a particular measurement approach for quantifying operational risk. Rather, the guidance requires a firm to combine four elements in a manner that is most appropriate to its business model. These four elements are: internal loss data; relevant external loss data; scenario analysis; and business environment and internal control factor assessments. The relative weight attached to these four elements varies by institution—most AMA banks currently emphasize statistical approaches based on loss data, but there are others, which place greater weight on scenario analysis derived from expert opinion.

In any event, it is clear that an important step is collecting internal loss data in a consistent manner across the firm—a challenge given that operational risk, as I have discussed, does not derive from a neat well-defined set of exposures, as do, for the most part, credit and market risk.

A few leading institutions have made real progress in pulling all the qualitative and quantitative elements of a sound operational risk capital framework together. Those elements include sound operational risk governance, accurate measurement inputs, and, as I just described, a rigorous methodology, for the quantification of capital requirements. We see it as critical that larger banks' risk management systems comprise all of these elements, and strongly encourage further progress as implementation of Basel II draws near.

Implications for Bank Supervisors

I have focused on the challenges large, complex U.S. banks will confront in implementing the AMA. Let me now spend a few moments in discussing how our supervisory approach is also likely to evolve over time. The draft supervisory guidance for the AMA places emphasis on the need for examiners to not only evaluate the risk management and control environment of the firm—which we do today—but to also consider the methods banks use to quantify their operational risk exposures.

I think you will agree that the pace of innovation in operational risk management is rapid. Accordingly, our examiners will have to become well versed in the changing technical aspects of those methods. Further, they will have to understand, and be able to critically evaluate to a much greater degree than is currently the case, how banks combine qualitative and quantitative techniques needed for regulatory capital, and economic capital, requirements.

In addition, since operational risk measures do not lend themselves to the type of quantitative back testing techniques available on the market risk side, examiners will have to rely on other more flexible methods for validating and approving the models developed by banks. Here, an ability to assess the reasonableness of key assumptions made by AMA banks will be important. Further, I see benchmarking—where examiners evaluate a bank's practice relative to peers—as critical. A good deal of informed judgement will be necessary in order to determine whether a bank's given approach makes sense in light of its own control environment.

Of course, to meet these responsibilities, we will need to ensure that our examiners are well trained, and are well-supported by clear supervisory guidance and examination procedures.

Conclusion

I hope that I have been able to give you a sense of the importance we place on operational risk management. I recognize the seriousness with which the industry is addressing this topic, including in the areas I have discussed today—outsourcing arrangements, business continuity and operational risk capital. As I have illustrated, close cooperation between industry participants and supervisory authorities has played an important role in our thinking in such areas as business continuity and operational risk capital. And, given recent trends in outsourcing, I anticipate greater dialogue in this area going forward.

With the supervisors and the industry working together—each meeting our responsibilities and reinforcing the other—I am confident we will be able to successfully address the challenges in measuring and managing operational risk in all of its forms. While perspectives may differ from time to time, our objective is the same—to maintain a strong and vibrant financial system over the long term.

Thank you very much.