BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM

WASHINGTON, D. C. 20551

DIVISION OF
BANKING
SUPERVISION AND
REGULATION

SR 98-9 (SUP)
April 20, 1998

TO THE OFFICER IN CHARGE OF SUPERVISION AND APPROPRIATE SUPERVISORY AND EXAMINATION STAFF AT EACH FEDERAL RESERVE BANK AND TO EACH DOMESTIC AND FOREIGN BANKING ORGANIZATION SUPERVISED BY THE FEDERAL RESERVE

SUBJECT: Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations

INTRODUCTION

The Federal Reserve recently introduced risk-focused frameworks for the supervision of community banks and large complex banking organizations, including foreign banking organizations. These frameworks incorporate a methodology to assess an organization's risks and business activities and to tailor supervisory activities to its risk profile. These frameworks aim to sharpen the focus of supervisory activities on areas that pose the greatest risk to the safety and soundness of banking organizations and on management processes to identify, measure, monitor, and control risks.[1]

The Federal Reserve has long recognized that the use of information technology can greatly affect a banking organization's financial condition and operating performance.[2] With the increasing dependency of banking organizations on the use of information technology, the Federal Reserve expects an organization's management and board of directors to manage effectively the risks associated with information technology. Accordingly, in implementing the risk-focused supervision framework, examiners must consider the risks associated with information technology in their evaluations of an organization's significant business activities and assess the effectiveness of the risk management process that the organization applies to information technology.

This SR Letter supplements existing guidance on the evaluation of banking organizations' risk management processes. The primary objectives are to:

- Highlight the critical dependence of the financial services industry upon information technology and its potential effect on safety and soundness.
- Reinforce the concept that the risk-focused supervisory process and related products (risk assessments, supervisory plans, and scope memoranda) for an organization must address the risks associated with its use of information technology.[3]
- Provide a basic framework and a common vocabulary to evaluate the effectiveness of processes used to manage the risks associated with information technology.

- Emphasize the Federal Reserve's commitment to continue to provide training to general safety and soundness examiners and information technology specialists that will strengthen their ability to assess the risks associated with information technology.

CHANGING ROLE OF INFORMATION TECHNOLOGY

As the automated processing of information has moved beyond centralized mainframe operations to encompass end-user computer and distributed processing systems, the use of information technology in general has expanded greatly. In the banking industry, information technology was once limited to automation of routine transactions and preparation of financial reports but is now used to automate all levels of a banking organization's operations and information processing. Some decision-making processes such as credit scoring and securities trading have been fully automated. New, complex financial products are possible largely because of valuation models that depend upon technology. Moreover, technological advances in communications and connectivity have served to minimize geographic constraints within the industry.

While information technology enables banking organizations to carry out their activities more efficiently and effectively, information technology also can be a source of risk to the industry, as the Year 2000 problem forcefully illustrates. The operational concerns associated with information processing, traditionally the domain of the "back office," have assumed critical importance during banking mergers and consolidations.

Banking organizations, recognizing the dependency of their operations and decision-making processes on information technology, have placed increased emphasis on the management of this important resource. In large banking organizations, the positions of the chief information officer and chief technology officer have become more visible in the top executive ranks of banking organizations. In addition, managers of activities that rely on end-user computing and distributed processing systems have been assigned more direct responsibility for information technology used in the conduct of their business. As a result, the management of the risks associated with information technology must be evaluated for each significant business activity as well as for the overall organization.

Notwithstanding the move towards decentralized management of information technology, large centralized mainframe computer systems are still an integral part of the information technology on which many large banking organizations rely. This includes systems critical to the global payments system and to the transfer and custody of securities. Similarly, with the continued growth of outsourcing, many third-party information technology service centers also perform a vital role in the banking industry. Therefore, the review of the effectiveness and reliability of the critical mainframe systems and third-party processors will continue to be an important part of the Federal Reserve's supervisory activities.

IMPLICATIONS FOR RISK-FOCUSED SUPERVISION

The risk-focused supervisory process is evolving to adapt to the changing role of information technology, with a greater emphasis being placed on an evaluation of information technology and an assessment of its effect on an organization's safety and soundness. Accordingly, examiners should explicitly consider information technology when developing their risk assessments and supervisory plans. It is expected that examiners will exercise appropriate judgment in determining the level of review given the characteristics, size, and business activities of the organization. Moreover, to determine the scope of supervisory activities close coordination is needed between general safety and soundness examiners and information technology specialists during the risk assessment and planning phase of the examination, as well as during the on-site examination. In general, examiners should:

1. Develop a broad understanding of the organization's approach, strategy, and structure with regard to information technology. This requires a determination of the role and importance of information technology to the organization and any unique characteristics or issues.

2. Incorporate an analysis of information technology systems into risk assessments, supervisory plans, and scope memoranda. The analysis should include identification of critical information technology systems, related management responsibility, and the major technology components.[4] An organization's information technology systems should be considered in relation to the size, activities, and complexity of the organization, as well as the degree of reliance on these systems.
3. Assess the organization's critical systems, that is, those that support its major business activities, and the degree of reliance those activities have on information technology systems. The level of review should be sufficient to determine that the systems are delivering the services necessary for the organization to conduct its business in a safe and sound manner.
4. Determine whether the board of directors and senior management are adequately identifying, measuring, monitoring, and controlling the significant risks associated with information technology for the overall organization and its major business activities.

FRAMEWORK FOR EVALUATING INFORMATION TECHNOLOGY

In order to provide a common terminology and consistent approach for evaluating the adequacy of an organization's information technology, five information technology elements are introduced and defined below. These elements may be used to evaluate the information technology processes at the functional business level or for the organization as a whole. They may also be applied to a variety of information technology management structures: centralized, decentralized, or outsourced.[5]

Although deficiencies in information technology appear to be most directly related to operational risk, information technology also can affect the other business risks (i.e., credit, market, liquidity, legal, and reputational) depending upon the specific circumstances. Examiners should view the information technology elements in an integrated manner with the overall business risks of the organization or business activity as a deficiency in any one of the elements could have a substantive adverse effect on the organization's or activity's business risks. Moreover, these elements do not replace or independently add to the business risks described in SR 95-51. Rather, these elements should be assessed in relation to all business risks.

The elements are intended to be used as a flexible tool to facilitate consideration and discussion of the risks associated with information technology. Where an organization uses different terminology to describe information technology elements, examiners may use that terminology provided that the organization adequately addresses all elements. Regardless of the terminology employed, examiners should focus on those systems and issues that are considered critical to the organization.

The five information technology elements are:

Management Processes[6]: Management processes encompass planning, investment, development, execution, and staffing of information technology from a corporate-wide and business-specific perspective. Management processes over information technology are effective when they are adequately and appropriately aligned with, and supportive of, the organization's mission and business objectives. Management processes include strategic planning, management and reporting hierarchy, management succession, and regular independent review function. Examiners should determine if the information technology strategy for the business activity or organization is consistent with the organization's mission and business objectives and whether the information technology function has effective management processes to execute that strategy.

Architecture[7]: Architecture refers to the underlying design of an automated information system and its individual components. The underlying design encompasses both physical and logical architecture, including operating environments, as well as the organization of data. The individual components refer to network communications, hardware, and software, which includes operating systems, communications software, database management systems, programming languages, and desktop software. Effective architecture meets current and long-

term organizational objectives, addresses capacity requirements to ensure that systems allow users to easily enter data at both normal and peak processing times, and provides satisfactory solutions to problems that arise when information is stored and processed in two or more systems that cannot be connected electronically. In assessing the adequacy of information technology architecture, examiners should consider the hardware's capability to run the software, the compatibility and integration with other systems and sources of data, the ability to upgrade to higher levels of performance and capacity, and the adequacy of controls.

Integrity: Integrity refers to the reliability, accuracy, and completeness of information delivered to the end-user. An information technology system has an effective level of integrity when the resulting information flows are accurate and complete. Insufficient integrity in an organization's systems could adversely affect day-to-day reliability, processing performance, input and output accuracy, and ease of use of critical information. Examiners should review and consider whether the organization relies upon information system audits or independent application reviews to ensure the integrity of its systems. To assess the integrity of an organization's systems, examiners should review the reliability, accuracy, and completeness of information delivered.

Security: Security refers to the safety afforded to information assets and their data processing environments, using both physical and logical controls to achieve a level of protection commensurate with the value of the assets. Information technology has effective security when controls prevent unauthorized access, modification, destruction, or disclosure of information assets during their creation, transmission, processing, maintenance, or storage. Examiners should ensure that operating procedures and controls are commensurate with the potential for and risks associated with security breaches, which may be either physical or electronic, inadvertent or intentional, internal or external.

Availability: Availability refers to the delivery of information to end-users. Information technology has effective availability when information is consistently delivered on a timely basis in support of business and decision-making processes. In assessing the adequacy of availability, examiners should consider the capability of information technology to provide information to the end-users from either primary or secondary sources, as well as the ability of back-up systems, presented in contingency plans, to mitigate business disruption. Contingency plans should set out a process for an organization to restore or replace its information processing resources, reconstruct its information assets, and resume its business activity from disruption caused by human error or intervention, natural disaster, or infrastructure failure (including loss of utilities and communication lines and operational failure of hardware, software, and network communications).

Attachment A provides a table with examples of situations where deficiencies in information technology elements potentially have a negative effect on the business risks of an organization. The table also provides possible action that an organization could take in these situations to mitigate its risks. The examples reflected in this table are representative and should not be viewed as an exhaustive list of the risks associated with information technology.

COORDINATION AND TRAINING FOR EXAMINERS

While mainframe computer systems are still an integral part of the information technology for large organizations, information technology processes have become imbedded in the various business activities of a banking organization with the increased use of local area network and personal computers. In contrast, many community and regional banks continue to rely on third-party information technology service centers. Given this variability of information technology environments, the level of technical expertise needed for a particular examination will vary and should be identified in the planning phase of the examination. For example, a specialist in information technology or the particular business activity may be the most appropriate person to review information technology integrity, while general safety and soundness examiners may be better suited to review management processes related to information technology. Development of the overall supervisory approach for an organization requires continuous collaboration between general safety and soundness examiners and information technology specialists. Accordingly, a discussion of information technology should be integrated into the supervisory process and products. That is, examiners should consider and comment on the risks associated with

information technology in developing an understanding of an organization, assessing an organization's risks, and preparing a scope memorandum.

The increasing role of information technology in the banking industry necessitates a broader understanding of technology on the part of examiners. The Federal Reserve has already developed and implemented a training course to strengthen examiners' ability to identify and to assess the risks associated with information technology from a safety and soundness perspective.[8] Additional training programs will be offered to strengthen the skills of specialists to enable them to better address the evolving information technology environment.

* * * *

Reserve Banks are requested to forward a copy of this SR Letter to the state member banks, bank holding companies, and foreign banking organizations in their districts. A suggested transmittal letter is provided in Attachment B. Any questions on the guidance contained in this letter should be directed to Michael Martinson, Deputy Associate Director, at 202/452-3640 or Blaine Jones, Supervisory EDP Analyst, at 202/452-3759.

Richard Spillenkothen
Director

ATTACHMENTS TRANSMITTED ELECTRONICALLY BELOW

Cross References:

SR 97-25
SR 97-24
SR 95-51
SR 95-45

Footnotes

1. The types of risk may be categorized according to those presented in the guidelines for rating risk management (i.e., credit, market, liquidity, operational, legal, and reputational) or by categories defined by the institution or other supervisory agencies. If the institution uses risk categories that differ from those defined by the supervisory agencies, those categories may be used if all relevant types of risks are captured. Refer to SR 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies."
2. Information technology refers to a business resource that is the combination of computers (hardware and software), telecommunications, and information.
3. The supervisory products are described in SR 97-24 for large complex institutions and SR 97-25 for community banks.
4. These components include mainframe, local area network, and personal computers, as well as software applications.
5. When banking organizations outsource operations, they delegate a certain level of responsibility and authority to an outside party (depending on the contractual arrangements). However, ultimate accountability remains with the banking organization.
6. Also referred to as "organization" or "strategic."
7. Sometimes referred to as "infrastructure."
8. The course is titled "Information Systems and Emerging Technology Risk Management" and will be offered through year-end 1999. Thereafter, elements of the course will be integrated into other examiner training courses.

Attachment A

Examples of Information Technology Elements that Should be Considered
in Assessing Business Risks of Particular Situations

Situation
IT Elements to be Considered
Potential Effect on Business Risks
Risk Mitigants

A bank holding company expands very rapidly via acquisition into new product lines and geographic areas.

Management Processes: Lack of clear, cohesive strategies could result in dependence on different systems that are incompatible and fragmented.

Integrity: Unreliable information could be produced due to incompatible systems.

Availability: Critical information may not be available to management when needed.

Credit Risk: Exposure may increase to less creditworthy borrowers.

Liquidity Risk: Depositors may withdraw funds or close accounts due to unreliable account information.

Operational Risk: Controls may be inadequate to address the increase in manual interventions to correct incompatibility problems between affiliates' systems, leading to a greater potential for fraudulent transactions.

- Develop a well thought-out plan for integrating acquired systems, mapping data-flows and sources, and ensuring reliability of systems.

A bank's consumer loan division inputs erroneous entries into the general ledger system.

Integrity: Billing errors and unwarranted late payment fees could occur due to the inaccurate loan information maintained by the system.

Reputational Risk: Knowledge of errors could become widespread resulting in adverse public opinion.

Operational Risk: Increased expenditures may be required to resolve accounting operations problems.

Legal Risk: Litigation could arise because of errors in customer accounts due to processing deficiencies.

- Improve policies and procedures related to input of accounting entries.
- Ensure internal audit considers system aspects of accounting operations.

Substantial turnover occurs in bank's wire transfer department.

Security: Security procedures could be compromised due to inadequate training and lack of qualified personnel.

Integrity: System may not be able to provided "real time" funds availability.

Operational Risk: Financial losses could occur due to fraud or incorrectly sent wire transfers.

Legal Risk: Litigation could arise as a result of errors in customer accounts and fraudulent wire transfers.

Reputational Risk: Knowledge of fraudulent or erroneous wire operations could result in adverse public opinion.

- Increase and strengthen procedural and access controls for wire operations.

- Implement security measures such as passwords and firewalls.
- Develop and monitor appropriate audit trails.
- Provide for adequate training program and staffing levels.

Attachment B

Suggested Transmittal Letter to
the Chief Executive Officer of Each Domestic and Foreign Banking Organization
Supervised by the Federal Reserve

Subject:
Assessment of a Banking Organization's Information Technology in the Risk-Focused Supervision Framework

The Federal Reserve has long recognized that the use of information technology can greatly affect a banking organization's financial condition and operating performance. Accordingly, Federal Reserve examiners consider the quality of an organization's information technology function in evaluating its management and operations. To assist examiners in their evaluations of this increasingly critical function within banking organizations, the Federal Reserve has developed additional guidance for the assessment of the risks associated with information technology.

The enclosed Supervisory Letter outlines the Federal Reserve's new guidance, which provides a basic framework and common vocabulary to be used by examiners in evaluating the effectiveness of an organization's ability to manage the risks associated with information technology. This guidance is in keeping with the risk-focused frameworks for the supervision of community banks and large complex banking organizations.

Any questions you may have on this guidance should be directed to [insert name and phone number] at this Reserve Bank.

Enclosure