BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM

WASHINGTON, D. C. 20551

DIVISION OF
BANKING
SUPERVISION
AND REGULATION

SR 00-4 (SUP)
February 29,
2000

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: Outsourcing of Information and Transaction Processing

Banking organizations are increasingly relying on services provided by other entities to support a range of banking operations. Outsourcing of information and transaction processing activities, either to affiliated institutions or third-party service providers, may help banking organizations manage data processing and related personnel costs, improve services, and obtain expertise not available internally. At the same time, the reduced operational control over outsourced activities may expose an institution to additional risks.

The federal banking agencies have established procedures to examine and evaluate the adequacy of institutions' controls over service providers.[1] This SR letter reiterates and clarifies the Federal Reserve's expectations regarding the management of risks that may arise from the outsourcing of critical information and transaction processing activities by banking organization. Operations addressed under this supervisory letter include the origination, processing, and settlement of payments and financial transactions, information processing related to customer account creation and maintenance, as well as other information and transaction processing activities that support critical banking functions, such as lending, deposit-taking, fiduciary, or trading activities. While the guidelines outlined in this letter apply to outsourced services, rather than products purchased or licensed from technology vendors (such as systems and software), many of the risk management techniques may also be applicable to the use and maintenance of such products.

Outsourcing Risks

Outsourcing of information and transaction processing involves similar operational risks that arise when these functions are performed internally, such as threats to the availability of systems used to support customer transactions, the integrity or security of customer account information, or the integrity of risk management information systems. Under outsourcing arrangements, however, the risk management measures commonly used to address these risks, such as internal controls and procedures, are generally under the direct

operational control of the service provider, rather than the serviced institution that would bear the associated risk of financial loss, reputational damage, or other adverse consequences.

Some outsourcing arrangements also involve direct financial risks to the serviced institution. For example, for some transaction processing activities, a service provider has the ability to process transactions that result in extensions of credit on behalf of the serviced institution.[2] A service provider may also collect or disburse funds, exposing the institution to liquidity and credit risks should the service provider fail to perform as expected.

Risk Management

The Federal Reserve expects institutions to ensure that controls over outsourced information and transaction processing activities are equivalent to those that would be implemented if the activity were conducted internally. The institution's board of directors and senior management should understand the key risks associated with the use of service providers for its critical operations, commensurate with the scope and risks of the outsourced activity and its importance to the institution's business. They should ensure that an appropriate oversight program is in place to monitor each service provider's controls, condition, and performance. The following areas should be included in this process:

Risk assessment: Before entering into an outsourcing arrangement, the institution should assess the key risks that may arise and options for controlling these risks. Factors influencing the risk assessment could include, for example, the criticality of the function to the institution, the nature of activities to be performed by the service provider, including handling funds or implementing credit decisions, the availability of alternative service providers for the particular function, insurance coverage available for particular risks, and the cost and time required to switch service providers should problems arise.

Selection of service provider: In selecting a service provider for critical information or transaction processing functions, an institution should perform sufficient due diligence to satisfy itself of the service provider's competence and stability, both financially and operationally, to provide the expected services and meet any related commitments.[3]

Contracts: The written contract between the institution and the service provider should clearly specify, at a level of detail commensurate with the scope and risks of the outsourced activity, all relevant terms, conditions, responsibilities, and liabilities of both parties. These

would normally include terms such as:

- Required service levels, performance standards, and penalties.
- Internal controls, insurance, disaster recovery capabilities, and other risk management measures maintained by the service provider.
- Data and system ownership and access.
- Liability for delayed or erroneous transactions and other potential risks.
- Provisions for and access by the institution to internal or external audits or other reviews of the service provider's operations and financial condition.
- Compliance with any applicable regulatory requirements and access to information and operations by the institution's supervisory authorities.
- Provisions for handling disputes, contract changes, and contract termination.

Terms and conditions should be assessed by the institution to ensure that they are appropriate for the particular service being provided and result in an acceptable level of risk to the institution.[4] Contracts for outsourcing of critical functions should be reviewed by the institution's legal counsel.

Policies, procedures, and controls: The service provider should implement internal control policies and procedures, data security and contingency capabilities, and other operational controls analogous to those that the institution would utilize if the activity were performed internally. Appropriate controls should be placed on transactions processed or funds handled by the service provider on behalf of the institution. The service provider's policies and procedures should be reviewed by client institutions.

Ongoing monitoring: The institution should review the operational and financial performance of critical service providers on an ongoing basis to ensure that the service provider is meeting and can continue to meet the terms of the arrangement. The institution's staff should have

sufficient training and expertise to review the service provider's performance and risk controls.

Information access: The institution must ensure that it has complete and immediate access to information critical to its operations that is maintained or processed by a service provider. Records maintained at the institution must be adequate to enable examiners to review its operations fully and effectively even if a function is outsourced.

Audit: The institution's audit function should review the oversight of critical service providers. Audits of the outsourced function should be conducted according to a scope and frequency appropriate for the particular function. Serviced institutions should conduct audits of the service provider or regularly review the service provider's internal or external audit scope and findings. Service providers should have an effective internal audit function or should commission comprehensive, regular audits from a third-party organization.[5] Audit results and management responses must be available to examiners upon request.

Contingency plans: The serviced institution should ensure adequate business resumption planning and testing by the service provider. Where appropriate based on the scope and risks of the outsourced function and the condition and performance of the service provider, the serviced institution's contingency plan may also include plans for the continuance of processing activities, either in-house or with another provider, in the event that the service provider is no longer able to provide the contracted services or the arrangement is otherwise terminated unexpectedly.

International Considerations

In general, arrangements for outsourcing of critical information or transaction processing functions to service providers located outside the United States should be conducted according to the risk management guidelines described above. In addition, the Federal Reserve expects that these arrangements will be established in a manner that does not diminish the ability of U.S. supervisors to review effectively the domestic or foreign operations of U.S. banking organizations and the U.S. operations of foreign banking organizations. In particular, examiners should evaluate the adequacy of outsourcing arrangements in the following areas:

Oversight and compliance: The institution is expected to demonstrate adequate oversight of a foreign service

provider, such as through comprehensive audits conducted by the service provider's internal or external auditors, the institution's own auditors, or foreign bank supervisory authorities. The arrangement must not hinder the ability of the institution to comply with all applicable U.S. laws and regulations, including, for example, requirements for accessibility and retention of records under the Bank Secrecy Act.

Information access: The outsourcing arrangement should be conducted in a manner so as not to hinder the ability of U.S. supervisors to reconstruct the U.S. activities of the organization in a timely manner if necessary. Outsourcing to jurisdictions where full and complete access to information may be impeded by legal or administrative restrictions on information flows will not be acceptable unless copies of records pertaining to U.S. operations are also maintained at the institution's U.S. office.

Audit: Copies of the most recent audits of the outsourcing arrangement must be maintained in English at the institution's U.S. office and must be made available to examiners upon request.

Contingency plan: The institution's contingency plan must include provisions to ensure timely access to critical information and service resumption in the event of unexpected national or geographic restrictions or disruptions affecting a foreign service provider's ability to provide services. Depending on the scope and risks of the outsourced function, this may necessitate back-up arrangements with other U.S. or foreign service providers in other geographic areas.

Foreign banking organizations: With the exception of a U.S. branch or agency of a foreign bank that relies on the parent organization for information or transaction processing services, foreign banking organizations should maintain at the U.S. office documentation of the home office's approval of outsourcing arrangements supporting its U.S. operations, whether to a U.S. or foreign service provider. The organization's U.S. office should also maintain documentation demonstrating appropriate oversight of the service provider's activities, such as written contracts, audit reports, and other monitoring tools. Where appropriate, the Federal Reserve will coordinate with a foreign banking organization's home country supervisor to ensure that it does not object to the outsourcing arrangement.

Foreign branches or subsidiaries of U.S. banks and Edge corporations: Documentation relating to outsourcing arrangements of the foreign operations of U.S. banking organizations with foreign service providers should be made available to examiners upon request.

Examination Implementation

In the development of the examination scope and risk profile, examiners should determine which information and transaction processing activities critical to the institution's core operations are outsourced. During the on-site examination, the adequacy of the institution's risk management for these critical service providers should be assessed and evaluated. The overall assessment should be reflected in the relevant components of the Uniform Information Technology Rating System examination rating, or the Uniform Financial Institution Rating System, if an information systems rating is not assigned.

This supervisory letter should be shared with banking organizations. If you have any questions regarding this letter, please contact Heidi Richards, Manager, Specialized Activities, (202) 452-2598.

Richard Spillenkothen
Director

Cross Reference: SR letter 97-35

Notes:

1. Refer to the Federal Reserve *Commercial Bank Examination Manual* (updated May 1998), Section 4060 Computer Services, and the *FFIEC Information Systems Examination Handbook* (1996 Edition). Other supervisory guidance has addressed outsourcing of business activities, such as internal audit (see SR letter 97-35, "Interagency Guidance on the Internal Audit Function and its Outsourcing.") See also Federal Reserve Bank of New York, "Outsourcing Financial Services Activities: Industry Practices to Mitigate Risks," October, 1999 (available at www.newyorkfed.org/bankinfo/circular/outsource.pdf). Return to text

2. For example, an institution may authorize a service provider to originate payments on behalf of customers for which the institution is required to honor by law or contract, such as ACH credit transfers. Return to text

3. Where the service provider is affiliated with the serviced institution, Sections 23A and 23B of the Federal Reserve Act may apply. In particular, Section 23B provides that the terms of transactions between a bank and its non-

bank affiliate must be comparable to the terms of similar transactions between nonaffiliated parties.

4. Additional information regarding common contract provisions can be found in the Federal Reserve *Commercial Bank Examination Manual* and the *FFIEC Information Systems Examination Handbook*. In addition, FFIEC Supervisory Policy SP-5 requires each serviced institution to evaluate the adequacy of its service provider's contingency plans.

5. AICPA Statement of Auditing Standards No. 70 "Reports on the Processing of Transactions by Service Organizations," commonly known as SAS 70 reports, are one commonly used external audit tool for service providers.