BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM

WASHINGTON, D. C. 20551

DIVISION OF
BANKING
SUPERVISION
AND
REGULATION

**SR 00-3
(SUP)
February 29,
2000**

**TO THE OFFICER IN CHARGE OF SUPERVISION
AT EACH FEDERAL RESERVE BANK**

SUBJECT: Information Technology Examination Frequency

Banking organizations increasingly rely on information technology to conduct their operations and manage risks. As outlined in SR letter 98-9, "Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations," the use of information technology can have important implications for a banking organization's financial condition, risk profile, and operating performance and should be incorporated into the safety and soundness assessment of each organization. In order to facilitate the integration of information technology supervision within the overall risk-focused supervisory process, the separate frequency guidelines for information technology examinations are being eliminated. Instead, all safety and soundness examinations (or examination cycles) of banking organizations conducted by the Federal Reserve should include an assessment and evaluation of information technology risks and risk management.

The scope of the information technology assessment should generally be sufficient to assign a composite rating under the Uniform Rating System for Information Technology (URSIT).[1] URSIT component ratings may be updated at the examiner's discretion based on the scope of the assessment. The scope would normally be based on factors such as:

- Implementation of new systems or technologies since the last examination.
- Significant changes in operations, such as mergers or systems conversions.
- New or modified outsourcing relationships for critical operations.

- Targeted examinations of business lines where internal controls or risk management are heavily dependent on information technology.
- Other potential problems or concerns that may have arisen since the last examination, or the need to follow up on previous examination or audit issues.

Institutions that outsource core processing functions, although not traditionally subject to information technology examinations, are exposed to information technology-related risks. For these institutions, some or all components of the URSIT rating may not be meaningful. In these cases, the assessment of information technology activities may be incorporated directly into the safety and soundness rating for the institution, rather than through the assignment of a URSIT rating. The scope of the information technology assessment for such institutions should include an evaluation of the adequacy of the institution's oversight of service providers for critical processing activities and should incorporate the results of any relevant supervisory reviews of such service providers. The assessment should also include reviews of any significant in-house activities, such as management information systems and local networks, and the implementation of new technologies, such as Internet banking.

The assessment of information technology should be reflected in the overall safety and soundness examination report and in the appropriate components of the safety and soundness examination rating assigned to the institution, as well as associated risk profile analysis. As described in SR letter 98-9, the impact of a positive or negative assessment of information technology may not be limited to the "Management" component of ratings or the "Operational Risk" component of the risk profiles, but in some cases may affect relevant financial risks and ratings as well.

Targeted information technology examinations may be conducted more frequently if deemed necessary by the Reserve Bank. A composite URSIT rating should be assigned in the case of targeted reviews where possible. In addition, institutions for which supervisory concerns have been raised (normally those rated URSIT 3, 4, or 5) should be subject to more frequent information technology reviews, until such time as the Reserve Bank is satisfied that the deficiencies have been corrected.

Examinations of Service Providers

Activities conducted by entities that provide information or transaction processing services to insured depository institutions may be subject to examination by one or more federal banking agencies pursuant to the Bank Service Company Act.[2] Nevertheless, serviced institutions are responsible for maintaining appropriate oversight of their vendors and service providers. Implementation of effective risk management controls by serviced institutions and appropriate review of these controls at the serviced institution by examiners is preferable to separate, on-site examinations at the service provider. Examinations of service providers' operations, where necessary, are conducted solely to support supervision of banking organizations, and should be conducted according to the following guidelines:

- Multiregional Data Processing Servicers (MDPS) and Shared Application Software Review (SASR) entities: As determined by the Information Systems Subcommittee of the Federal Financial Institutions Examination Council (FFIEC), certain large, nationwide service providers and software vendors are subject to interagency examination or review under the MDPS and SASR programs. Federal Reserve examiners lead or assist on these examinations as appropriate.
- Other U.S. service providers: For independent service providers, bank service companies, and nonbank affiliates or subsidiaries of banking organizations that provide services to affiliates or other institutions, Federal Reserve examiners should conduct an on-site examination or assist another federal banking agency with such an examination according to the risk assessment and frequency guidelines described below. Such examinations should be coordinated with other banking agencies as provided under FFIEC SP-1.[3]
- Foreign service providers: Where an U.S. institution outsources operations to its foreign branch or affiliate, the Federal Reserve may arrange to examine the foreign operations, where appropriate, based on the level of risk and the effectiveness of oversight by the U.S. institution. Where the foreign service provider is not affiliated with the serviced U.S. institution, coordination with foreign supervisors may be appropriate to determine whether oversight of the service provider is adequate. The Federal Reserve generally will not conduct on-site examinations of unaffiliated foreign entities that provide information or transaction processing services to U.S. banking organizations or foreign banking organizations operating in the United States, or in cases where U.S. institutions outsource operations to the foreign parent banking organization. All examinations of unaffiliated service providers located outside the United States should be coordinated with Board supervision staff.

Risk Assessments of Service Providers

A risk assessment should be documented annually for each service provider performing critical processing functions for banking organizations subject to Federal Reserve supervision. At a minimum, risk assessments should support examinations of service providers in which Federal Reserve examiners participate. Reserve Banks should coordinate the risk assessment of a service provider located in their districts with other Reserve Banks responsible for supervision of institutions serviced by the service provider, as well as with the current lead bank supervisory agency for the service provider, if applicable. Reserve Banks are encouraged to communicate with service providers and other bank technology vendors located in their districts to maintain

familiarity with the products and services, provide training to examiners, and update risk assessments.

Risk assessments should consider both the inherent risk of the activity or services provided, together with mitigating factors. The risk assessment should focus on material, supervisory risks to serviced institutions supervised by the Federal Reserve, rather than on routine operating risks, which, while potentially leading to some loss of business for institutions, do not threaten their safety and soundness. Mitigating factors, such as the strength of client bank oversight and stability of the service provider's operations, should also be considered. Specific risk factors include:

- Evidence that the outsourced activity gives rise to risk of significant financial losses for institutions subject to Federal Reserve supervision.
- Significant internal control deficiencies, inadequate audit or reporting, or other concerns with the service provider identified during examinations of serviced institutions.
- Evidence of inadequate oversight by the service provider's customers.
- Significant changes in management, staffing, or services at the service provider that may adversely affect risk management.
- Evidence that a service provider that is a nonbank subsidiary of a bank holding company poses significant risk to the holding company.[4]

Service Provider Examination Frequency and Ratings

Service providers considered to pose high risk as a result of a risk assessment should normally be examined at least once during a two-year period. Service providers considered moderate or low risk may be examined at the discretion of the Reserve Bank. These entities may be subject to occasional examinations or periodic targeted reviews, together with off-site monitoring. Reserve Banks may schedule examinations more frequently than indicated in these guidelines as necessary, for example, to follow up on deficiencies noted in an earlier examination.

The examination scope should focus on those operations considered critical to client institutions, rather than on the overall condition, prospects, or business of the service provider itself. Examination findings and URSIT ratings for service providers should likewise reflect the impact of the service provider's operations on the safety and soundness of supervised client institutions. Any significant findings should be provided to examiners responsible for supervising client institutions and should be reflected in the supervisory assessment of those institutions.

By December 31 of each year, Reserve Banks should forward to the Board's Manager, Specialized Activities, a listing of critical service providers in their district, their risk ranking (High, Moderate, or Low), and anticipated examinations scheduled for the ensuing year in which the Reserve Bank's examiners will participate. In addition, examination information for all service provider examinations in which Federal Reserve

examiners participate, including service providers for which the examination is led by another supervisory agency, should be entered into NED.[5]

Effective Date

With the issuance of this SR letter, the portion of SR letter 86-39 addressing the frequency and scope of information technology examinations (previously referred to as Electronic Data Processing examinations) is superseded. Given the need to address activities curtailed or postponed due to century date change activities, however, Reserve Banks may choose to phase in the implementation of this policy over the course of 2000 as resources become available. Questions may be directed to Heidi Richards, Manager, Specialized Activities, (202) 452-2598.

Richard Spillenkothen
Director

Supersedes: SR letter 86-39 (Electronic Data Processing portion)
Cross References:
SR letter 99-17
SR letter 99-8
SR letter 98-9
SR letter 97-24
SR letter 93-19

Notes:

1. Refer to SR letter 99-8 "Uniform Rating System for Information Technology." Assignment of URSIT ratings should be done in accordance with the guidance provided in SR letter 99-17, "Supervisory Ratings for State Member Banks, Bank Holding Companies and Foreign Banking Organizations, and Related Requirements for the National Examination Data System." All URSIT ratings should be entered into the National Examination Data System (NED).
2. 12 U.S.C. 1867.
3. See Federal Financial Institutions Examination Council, *Information Systems Examination Handbook*, Volume 2 (1996 Edition).
4. For further guidance on the frequency of on-site reviews of nonbank subsidiaries of bank holding companies, see SR letter 93-19, "Supplemental Guidance for the Inspection of Nonbank Subsidiaries of Bank Holding Companies," April 13, 1993, and SR letter 97-24 "Risk-Focused Framework for Supervision of Large Complex Institutions," October 27, 1997.
5. Enhancements to NED are being designed to facilitate collection of service provider information.