Federal Financial Institutions Examination Council

FFIEC

Supervision of Technology Service Providers

TSP

OCTOBER 2012

IT Examination Handbook

Table of Contents

Introduction

The Board of Governors of the Federal Reserve System (FRS), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (each individually, Agency, and collectively, Agencies) have statutory authority to supervise third-party servicers that enter into contractual arrangements with their regulated financial institutions. [1]

The "Supervision of Technology Service Providers" booklet (TSP Booklet), of the FFIEC [2] Information Technology Examination Handbook (IT Handbook), addresses this authority and rescinds the previous version dated March 2003. The TSP booklet outlines the Agencies' risk-based supervisory program and includes the examination ratings used for regulated financial institutions and their Technology Service Providers (TSP). [3]

A financial institution's use of a TSP to provide needed products and services does not diminish the responsibility of the institution's board of directors and management to ensure that the activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations, just as if the institution were to perform the activities in-house.

While the examinations of TSPs generally focus on the underlying information technology (IT) risk, the risk assessment process also considers all business lines in which TSPs engage to ensure that all covered services are effectively included. The Agencies expect financial institutions to have a comprehensive, enterprise risk management process in place that addresses vendor management for their relationships with TSPs. The risk management process should include risk assessments and robust due diligence for the selection of TSPs, contract development, and ongoing monitoring of all TSPs' performance. [4]

The Agencies conduct IT-related examinations of financial institutions and their TSPs based on the guidelines contained in the IT Handbook. The handbook is composed of the following individual booklets that address governance of risks expected of financial institutions and their TSPs as well as detailed examination procedures:

- Audit
- Business Continuity Planning
- Development and Acquisition
- Electronic Banking
- Information Security
- Management
- Operations
- Outsourcing Technology Services
- Retail Payment Systems

- Supervision of Technology Service Providers
- Wholesale Payment Systems

Management of financial institutions and TSPs should be aware of the guidance described in the IT Handbook.

Supervisory Policy

Supervisory policy provides for interagency examinations of TSPs that service insured financial institutions supervised by more than one federal financial institution regulator. The policy is expected to eliminate the need for separate examinations of TSPs by more than one regulator and to result in more efficient use of examiner resources and with less burden to the supervised TSP. Notwithstanding this policy, no federal or state regulatory agency is precluded from conducting an independent examination of any TSP that is servicing an insured financial institution for which the agency is responsible.

Federal and/or state banking agencies participating on interagency TSP examinations are precluded from levying any examination-associated fees against the examined service provider.

Examination Responsibility

Examination responsibility is determined based on the class/type of servicer as well as the class/type of insured financial institution(s) being serviced.

A. Insured Financial Institution

Technology service centers operated by an insured financial institution or its subsidiary are examined by the Agency responsible for the supervision of the financial institution.

B. Insured Financial Institution as TSP

Services provided by an insured financial institution, or by its subsidiary, to one class [5] or more of insured financial institutions are examined by the Agency responsible for supervising the servicing institution. The primary regulatory Agency seeks input from other interested Agencies and performs an IT examination of the entity's operations as they relate to the technology services it provides. The Agency generates a report with supporting information regarding the adequacy of its institution's servicing operations and provides the report to the primary federal regulators of the serviced institution(s). Application of the Risk-Based-Examination Priority Ranking Program (RB-EPRP) to the servicing institution is left to the discretion of its regulatory Agency.

C. Holding Company and Non-Bank Subsidiary of the Holding Company

Services provided by a financial institution holding company, or by its non-bank subsidiary, to one class or more of insured financial institution are examined by the Agency responsible for supervising the servicing entity. The primary regulatory Agency seeks input from other interested Agencies and performs an IT examination of the entity's operations as they relate to the technology services it provides. The Agency generates a report with supporting information regarding the adequacy of the entity's operations and provides the report to the primary federal regulators of the serviced institution(s). Application of the RB-EPRP to the servicing entity is left to the discretion of its regulatory Agency.

D. Bank Service Company as TSP

Responsibility for the examination of bank service companies [6] is based first on the type/class of entity(s) holding controlling ownership [7] in the servicer. Specifically:

- If there is one or more controlling owner, primary examination responsibility falls to the Agency(s) supervising the controlling owner(s).
- Where there is only one controlling owner, or where one controlling owner has claim to materially greater ownership interests relative to the others, the Agency supervising that owner has the discretion to retain primary examination responsibility with regard to any interagency examination work.
- Where controlling ownership is equally distributed, the primary examination responsibilities are rotated as agreed by the interested Agencies.

In all instances, regardless of the number of controlling owners, the Agencies supervising the serviced financial institutions have an interest in participating on interagency examinations.

E. Independent TSPs, Including Those in the Multi-Regional Data Processing Servicers Program

Responsibility for the examination of independent TSPs is based on the class of insured financial institution being serviced. If more than one class of insured institution is serviced, the examination is conducted jointly, and on a rotated basis, as agreed to among the federal financial institution regulators responsible for the classes of serviced institutions.

Examination of companies in the Multi-Regional Data Processing Servicers (MDPS) program is administered by the Agencies. The Agencies determine which TSPs are subject to examination under the MDPS program. Generally, Agency-In-Charge (AIC) responsibilities for an MDPS company are rotated among the Agencies responsible for the class of serviced, insured financial institutions after two consecutive examination cycles, [8] with exceptions subject to the Agencies' review and approval. As indicated in section C on page 3, if an independent MDPS company, through acquisition, becomes a

financial holding company, a bank holding company, a thrift holding company, or a non-financial institution subsidiary or affiliate thereof, the Agency supervising the holding company serves as the AIC unless such Agency chooses to rotate the responsibilities.

Examinations of independent TSPs that are not part of the MDPS program are administered by the Agencies' regional/district management under the guidelines in this booklet.

Supervisory Programs

The Agencies coordinate the interagency programs for the supervision of TSPs through the FFIEC. The programs establish responsibilities and requirements for the collaborative efforts of the Agencies to ensure effective supervision while making efficient use of examiner resources and reducing burden on the TSPs.

MDPS Program

The Agencies are responsible for the administration, coordination, oversight, and implementation of the supervisory program for the largest, systemically important TSPs: the MDPS program. The program represents a cooperative arrangement among the Agencies for the achievement of shared and consistent supervisory goals and objectives.

As a general rule, a TSP is considered for the MDPS program when the TSP processes:

- mission-critical applications [9] for a large number of financial institutions that are regulated by more than one Agency, thereby posing a high degree of systemic risk; or
- from a number of data centers located in different geographic regions.

The companies in the MDPS program can pose a significant risk to the banking system if one or more have operational or financial problems or fail. Because these companies provide services to banks, savings associations, and credit unions, the supervisory program allows for effective use of Agencies' resources, reduced burden to the MDPS, shared knowledge of the company's operations, development of a joint supervisory strategy, and generation of a single Report of Examination (ROE) for the company and its client-regulated financial institutions.

Regional TSP Program

The Agencies' district or regional offices are responsible for the administration, coordination, oversight, and implementation of the supervision of TSPs that are local and smaller in size or complexity. Although these TSPs are not part of the MDPS program, they are supervised in a similar manner and under the guidelines of the Supervisory

Policy previously discussed.

Supervision of Foreign-Based TSP Program

Advances in technology enable financial institutions to provide customers with an array of products, services, and delivery channels. One result of these changes is that financial institutions are entering into contractual obligations with, and outsourcing banking activities to, foreign-based TSPs (FBTSP). Outsourcing or subcontracting (by domestic TSPs) to FBTSPs raises country risk, in addition to other risks presented by the use of domestic TSPs. Country risk is the exposure to social, economic, and political conditions in a foreign country that could adversely affect the ability of a FBTSP to meet its contractual obligations.

The Agencies' supervisory approach to cross-border outsourcing emphasizes the responsibility of the serviced financial institution to conduct adequate due diligence, manage risks appropriately, comply with applicable U.S. and foreign laws and regulations, and ensure access to critical information with respect to the services being provided by the FBTSP. If circumstances warrant, the Agencies arrange, through the appropriate foreign regulatory agencies, to obtain information related to the services provided to U.S. regulated financial institutions. If significant risks and concerns warrant on-site supervision of the FBTSP, the Agencies secure approval of their representatives at the Task Force on Supervision (TFOS) [10] before conducting the examination. For these examinations, the Agencies use the same interagency process defined in this TSP booklet and described throughout the IT Handbook.

Shared Application Software Review Program

The Agencies established the Shared Application Software Review (SASR) program to effectively employ interagency resources in uniform reviews of software packages or systems. Shared application software packages include stand-alone software and integrated (turnkey system) packages. Generally, these are purchased software that involves mission-critical, core, or high-risk applications widely used at financial institutions.

The SASR program is not limited, however, to the review of shared application packages. The Agencies also use SASRs to support interagency safety and soundness initiatives when focusing on higher-risk applications in larger financial institutions. A SASR can evaluate financial institutions' software packages for use in wire transfer, capital markets, derivatives development/record keeping, securities transfer, asset management, Bank Secrecy Act and anti-money laundering, consumer compliance, or other lines of business.

An internal, confidential SASR report is developed strictly for regulatory purposes. The report is not provided to the company that developed the software application or to the user financial institutions. The information in the SASR report is intended to augment and expedite the Agencies' supervisory process by identifying potential systemic risks and presenting information, suggestions, and instructions to aid in completing the examinations of financial institutions that use the various applications and software products covered by this program.

Roles and Responsibilities

Agency-In-Charge

Based on an annual schedule approved by either the Agencies or the Agencies' district/ regional offices, the Agencies select an AIC for each examined TSP.

Central Point of Contact

Each Agency assigns a qualified IT examiner to serve as its Central Point of Contact (CPC) for each company in the MDPS program, and where appropriate, for regional TSPs. [11] The selected CPCs form the CPC team, which serves as the primary group for all interagency examination-related activities, including developing supervisory strategies, performing examination activities, and pursuing the resolution of any significant findings. The CPC for the AIC is designated as the Lead CPC.

For TSPs that do not have designated CPC teams, the examiners assigned by the AICs are responsible for the supervision and oversight of the TSPs. These examiners carry out their responsibilities in collaboration with examiners from participating Agencies.

Examiner-In-Charge of Site or Activity

Some examinations of sites or specific supervisory activities of a TSP may have an examiner, who is not a member of the CPC team, assigned as Examiner-In-Charge (EIC). In these situations, the EIC conducts the assignment under the direction of the CPC team and is responsible to the Lead CPC for the administration and overall performance of the supervisory activity. The EIC keeps the CPC team informed of examination progress and findings.

Risk-Based Supervision

The Agencies' IT examination process is based on the concept of ongoing, risk-based supervision. This includes the identification and selection of TSPs warranting interagency supervision and the development of a risk-based supervisory strategy for each of these entities. This approach provides for examination coverage of selected TSPs, including core application processors, electronic funds transfer switches, Internet banking providers, item processors, managed security servicers, and data storage servicers. [12]

The examinations of TSPs focus on the following underlying risk issues that affect the client financial institutions or the institutions' customers:

- **Management of technology.** The planning and oversight of technology resources and

services, ensuring they support the strategic goals and objectives of the TSP and its serviced financial institutions.

- **Integrity of data.** The accuracy and reliability of automated information processes and associated management information systems.

- **Confidentiality of information.** The protection of information from intentional or inadvertent disclosure to unauthorized individuals.

- **Availability of services.** The resilience of the TSP, including effective disaster recovery, business continuity plans, and adherence to service-level agreements.

- **Compliance.** TSPs are expected to provide services to client financial institutions to help them comply with applicable laws, rules, regulations, and policies.

- **Financial stability.** The maintenance of sufficient capital and liquidity to support ongoing operations and the ability to generate profit to ensure future viability. Financial difficulties at the TSP can negatively affect the safe and sound operations of serviced financial institutions through deteriorating quality of service, reliability of service, or adequacy of controls.

Risk-Based-Examination Priority Ranking

The Agencies use the Risk-Based-Examination Priority Ranking Program (RB-EBR) in determining the overall level of risk a TSP presents to its client financial institutions. The Agencies also use the RB-EPRP to prioritize and establish the frequency of TSP examinations. The RB-EPRP ranks TSPs based on the risk their business lines, controls, and risk management processes present to their client financial institutions.

Uniform Rating System for Information Technology

The Agencies use the Uniform Rating System for Information Technology (URSIT) to uniformly assess and rate IT-related risks of financial institutions and their TSPs. The primary purpose of this rating system is to evaluate the examined institution's overall risk exposure and risk management performance and determine the degree of supervisory attention necessary to ensure that weaknesses are addressed and risks are properly managed. The assigned rating determines the degree of supervisory attention necessary.

The URSIT is based on a risk evaluation of four critical components: Audit, Management, Development and Acquisition, and Support and Delivery. The ratings assigned to these

individual components are used to quantify the overall effectiveness of the institution's IT risk management practices and condition. Examiners evaluate the functions identified within each component to assess the institution's ability to identify, measure, monitor, and control IT risks. The overall performance of IT within a financial institution or TSP is reflected by a composite rating. Please refer to Appendix A for additional information on composite and component URSIT ratings.

Frequency of Examinations

All TSPs that the Agencies supervise receive an examination sufficient in scope to assign or update the URSIT during each examination cycle. The number and frequency of supervisory activities conducted during the examination cycle varies depending on the risk profile of the TSP as established by the RB-EPRP and the URSIT. TSPs with a higher risk ranking are subject to more frequent and extensive examinations. The examination cycles, based on the assigned URSIT and Examination Priority Ranking (EPR), are as follows:

- **"A" ranking**: 24-month examination cycle
- **"B" ranking**: 36-month examination cycle
- **"C" ranking**: 48-month examination cycle

As part of the supervision of a TSP, examiners can conduct interim supervisory reviews or unscheduled site or service examinations for areas of evolving supervisory interest or concern. The number and frequency of interim supervisory reviews conducted during an examination cycle are based on the level of risk identified by the CPC team. All examined TSPs must receive at least one interim supervisory review during each examination cycle.

Examinations are conducted jointly according to schedules agreed upon by the participating Agencies. When joint examinations cannot be scheduled, one or more Agencies may be designated to perform the examination on behalf of all interested Agencies. If, however, the TSP's overall condition is determined to be less than satisfactory, the Agencies make a special effort to ensure subsequent examinations are conducted on a joint basis until the TSP's overall condition is satisfactory.

Risks Associated With TSPs

Operational risk is the primary risk associated with TSP processing. Operational risk may arise from inadequate or failed internal processes or systems, the misconduct or errors of people, and adverse external events. Operational risk also may affect other risks, such as credit, interest rate, liquidity, price, compliance, strategic or reputation. Other risks associated with TSPs include:

- **Reputation risk.** Errors, delays, or omissions in IT that become public knowledge or directly affect customers can significantly affect the reputation of the serviced financial institutions. For example, a TSP's failure to maintain adequate business resumption plans and facilities for key processes may impair the ability of serviced financial institutions to provide critical services to their customers.
- **Strategic risk.** Inaccurate information from TSPs can cause the management of serviced financial institutions to make poor strategic decisions.
- **Compliance (legal) risk.** Inaccurate or untimely data related to consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose financial institutions to civil money penalties or litigation. For example, TSPs often agree to keep disclosures or calculations in compliance with banking regulations, and their failure to track regulatory changes could increase compliance risk for their serviced financial institutions.
- **Credit, interest rate, liquidity, and price (market) risks.** Processing errors related to investment income or repayment assumptions could increase these risks of serviced financial institutions.

The quantity of operational risk at a TSP is the level or volume of risk that exists. The quality of operational risk management is an assessment of how well risks are identified, measured, controlled, and monitored.

Risk Management

The Agencies recognize that management practices, particularly as they relate to risk management, vary considerably among financial institutions and TSPs, depending on their size and sophistication, the nature and complexity of their business activities, and their risk profile. Accordingly, the Agencies also recognize that for less complex information systems environments, detailed or highly formalized systems and controls may not be required.

Financial institutions should oversee their TSPs and perform due diligence in selecting their third-party servicers, including a review of the risk management systems used by the TSPs. Such reviews should include measures taken by the TSPs to protect information about financial institutions' customers. Financial institutions also should monitor their TSPs to confirm the TSPs implement adequate security measures. As part of their monitoring activities, financial institutions should review such information as TSP service-level reports, audits, third-party reviews, internal control testing results, and other equivalent evaluations of their TSPs.

If a TSP has weak risk management controls requiring corrective action, the TSP's serviced institutions may also have to take remedial actions because the institutions have the ultimate responsibility to properly manage their risks. Management of TSPs and financial institutions should monitor changes in laws, regulations, and guidance that affects the services provided to financial institutions.

Audit and Internal Controls

Well-planned, properly structured audit programs are essential to strong risk management and effective internal control systems. Effective internal and external audit programs are also a critical defense against fraud and provide vital information to the board of directors about the effectiveness of internal controls systems. The Agencies encourage the use of well-supported risk-based auditing. Through this process, the board, management, and auditors can focus their resources on areas of greatest risk.

TSPs with effective risk-based auditing programs typically require less examination work by the Agencies. Additional guidance on what examiners review in information systems, audit, and internal control functions can be found in the "Audit" and "Management" booklets of the IT Handbook.

Report of Examination

The Agencies have a uniform Report of Examination (ROE) format for IT examinations of financial institutions and their TSPs. The ROE includes an "Open Section," which contains all significant findings and conclusions, and a "Confidential Section," which includes information solely for the Agencies' internal use.

ROE Distribution

The ROE is generally distributed to three primary groups: the Agencies, the supervised TSP, and the serviced financial institutions. [13]

All ROEs of a TSP, including those of stand-alone, subsidiary data centers, are directed to the board of directors, a committee thereof, or senior management of the TSP. The ROE is accompanied by a letter to the board, which includes the assigned URSIT and a reminder to recipients of the confidential nature of the letter and ROE.

The Agencies distribute to serviced financial institutions, either automatically or upon request, the Open section of a TSP ROE. Reports are automatically distributed when the TSP receives a composite URSIT rating of 4 or 5. A serviced financial institution can request a copy of the ROE from the institution's primary regulator and must demonstrate that it had a valid and current contract with the TSP as of the date of the examination.

The ROE is the joint property of the Agencies and is provided to the TSP and its client regulated financial institutions for their internal, confidential use. Under no circumstances shall any recipient of the ROE disclose or make public the ROE or any portion thereof. Unauthorized disclosure of any of the contents of the ROE is subject to the penalties in 18 USC 641.

Customer List

As part of the supervisory process, the Lead CPC obtains from the TSPs a list of

regulated financial institutions with which the servicer has entered into a contractual arrangement. The customer list, which is to be provided upon request (generally, during examinations, or, at a minimum, once each examination cycle), must be accurate, complete, and in a specified format that identifies the services being provided to each client financial institution.

The customer lists allow the Agencies to identify and validate regulated financial institutions that are entitled to copies of the ROEs produced on the TSPs. Additionally, the customer lists give the Agencies information to determine the scope of regulated financial institutions that may be affected by the operations of a TSP.

Endnotes

[1]	12 USC 1464(d)(7), 1867(c)(1). The Consumer Financial Protection Bureau (CFPB) has authority as described in 12 USC 5514(e), 5515(d), and 5516(e). See CFPB Bulletin 2012-03 (Apr. 13, 2012), available at http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf. The National Credit Union Administration (NCUA) does not have independent regulatory authority over TSPs. The Agencies coordinate the interagency programs to supervise third-party servicers through the Federal Financial Institutions Examination Council (FFIEC).
[2]	The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. The FFIEC members include the FRS, the FDIC, the NCUA, the OCC, the State Liaison Committee (SLC), and the CFPB.
[3]	The term TSP generally includes independent third parties, joint venture/limited liability corporations, and bank and credit union service corporations that provide processing services to financial institutions supervised by the FFIEC member Agencies.
[4]	Additional information on appropriate due diligence and oversight of outsourced technology services and third-party relationships can be found in the FFIEC Information Technology Examination Handbook, (IT Handbook), "Outsourcing Technology Services" booklet.
[5]	For example, national banks, state member banks, state non-member banks.
[6]	As defined in 12 U.S.C. 1861(b)(2).
[7]	12 U.S.C. 1861(b)(8).
[8]	The examination cycle is based on the assigned Examination Priority Ranking derived through the RB-EPRP. Examination cycles are 24, 36, or 48 months.
[9]	An application or system is mission-critical if it is vital to the successful continuance of a core business activity. An application also may be mission-critical if it interfaces with a designated mission-critical system. Products of software vendors also may be mission-critical.
[10]	The FFIEC TFOS coordinates and oversees matters relating to safety and soundness supervision and examination of depository institutions. It provides a forum for the member agencies that supervise banks, thrifts, and credit unions to promote quality, consistency, and effectiveness in examination and supervisory practices and to reduce unnecessary regulatory burden on those institutions. The TFOS has one standing subcommittee, the Information Technology (IT) Subcommittee.
[11]	Agencies that do not have sufficient regulatory interest in a TSP may choose not to have a designated CPC.

[12]	This list is representative of some types of service providers that may be examined and is not intended to be all-inclusive.
[13]	The Agencies also provide CFPB with access to service provider examination reports in accordance with the provisions of section 1022(c)(6)(B)(i) of the Dodd-Frank Wall Street Reform and Consumer Protection Act. See 12 USC 5512(c)(6)(B)(i)

Appendix A: URSIT

Introduction

Use of Composite Ratings

Each TSP examined for IT is assigned a summary or composite rating based on the overall results of the evaluation. The IT composite rating and each component rating are based on a scale of 1 through 5 in ascending order of supervisory concern, with 1 representing the highest rating and least degree of concern; and 5, the lowest rating and highest degree of concern.

The first step in developing an IT composite rating for an organization is the assignment of a performance rating to the individual Audit, Management, Development and Acquisition, and Support and Delivery (AMDS) components. The evaluation of each of these components, their interrelationships, and relative importance is the basis for the composite rating. A direct relationship exists between the composite rating and the individual AMDS component performance ratings. However, the composite rating is not an arithmetic average of the individual components. An arithmetic approach does not reflect the actual condition of IT when using a risk-focused approach. A poor rating in one component may heavily influence the overall composite rating for an institution.

A principal purpose of the composite rating is to identify those financial institutions and TSPs that pose an inordinate amount of information technology risk and merit special supervisory attention. Thus, individual risk exposures that more explicitly affect the viability of the organization or its customers should be given more weight in the composite rating.

The AIC of the TSP examination should notify other FFIEC Agencies' supervisory offices prior to issuing URSIT composite ratings of 3, 4, or 5 or engaging in informal or formal enforcement actions.

Use of Component Ratings

Each performance or component rating also ranges from 1 through 5, with 1 representing the highest or best, and 5, the lowest rating or worst. Each functional area of activity (audit, management, development and acquisition, and support and delivery) must be evaluated to determine its individual performance rating.

Composite Ratings Definitions

Composite - 1

Financial institutions and service providers rated composite 1 exhibit strong performance in every respect and generally have components rated 1 or 2. Weaknesses in IT are minor in nature and are easily corrected during the normal course of business. Risk management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are well defined and fully integrated throughout the organization. This allows management to quickly adapt to changing market, business, and technology needs of the entity. Management identifies weaknesses promptly and takes appropriate corrective action to resolve audit and regulatory concerns. The financial condition of the service provider is strong and overall performance shows no cause for supervisory concern.

Composite - 2

Financial institutions and service providers rated composite 2 exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination, or improved communication throughout the organization. As a result, management anticipates, but responds less quickly, to changes in market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. However, greater reliance is placed on audit and regulatory intervention to identify and resolve concerns. The financial condition of the service provider is acceptable and while internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is informal and limited.

Composite - 3

Financial institutions and service providers rated composite 3 exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution or service provider is likely. Risk management processes may not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the entity. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. As a result, management often has difficulty responding to changes in business, market, and technological needs of the entity. Self-assessment practices are weak and are generally reactive to audit and regulatory exceptions. Repeat concerns may exist indicating that management may lack the ability or willingness to resolve concerns. The financial condition of the service provider may be weak and/or negative trends may be evident. While financial or operational failure is unlikely, increased supervision is necessary. Formal or informal supervisory action may be necessary to secure corrective action.

Composite - 4

Financial institutions and service providers rated composite 4 operate in an unsafe and unsound environment that may impair the future viability of the entity. Operating weaknesses are indicative of serious managerial deficiencies. Risk management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Strategic plans are poorly defined and not coordinated or communicated throughout the organization. As a result, management and the board are not committed to, or may be incapable of ensuring, that technological needs are met. Management does not perform self-assessments and demonstrates an inability or unwillingness to correct audit and regulatory concerns. The financial condition of the service provider is severely impaired or deteriorating. Failure of the financial institution or service provider may be likely unless IT problems are remedied. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.

Composite - 5

Financial institutions and service providers rated composite 5 exhibit critically deficient operating performances and are in need of immediate remedial action. Operational problems and serious weaknesses may exist throughout the organization. Risk management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Strategic plans do not exist or are ineffective, and management and the board provide little or no direction for IT initiatives. As a result, management is unaware of, or inattentive to, technological needs of the entity. Management is unwilling or incapable of correcting audit and regulatory concerns. The financial condition of the service provider is poor and failure is highly probable due to poor operating performance or financial instability. Ongoing supervisory attention is necessary.

Component Ratings Definitions

Each performance or component rating also ranges from 1 through 5, with 1 representing the highest and 5 the lowest rating. Each functional area of activity (audit, management, development and acquisition, and support and delivery) must be evaluated to determine its individual performance rating.

Each performance or component rating is described as follows:

Component 1-Strong performance: Performance that is significantly higher than average.

Component 2- Satisfactory performance: Performance that is average or slightly above and that provides adequately for the safe and sound operation of the data center.

Component 3-Less than satisfactory: Performance that exhibits some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe.

Component 4-Deficient: Performance that is in an unsafe and unsound environment that may impair the future viability of the entity.

Component 5-Critically deficient: Performance that is critically deficient and in need of immediate remedial attention. The financial condition of the service provider is poor and failure is highly probable due to poor operating performance or financial instability.

Component Rating Areas of Coverage

Audit

Financial institutions and service providers are expected to provide independent assessments of their exposure to risks and the quality of internal controls associated with the acquisition, implementation, and use of information technology. Audit practices should address the IT risk exposures throughout the institution and its service provider(s) in the areas of user and data center operations, client/server architecture, local and wide-area networks, telecommunications, information security, electronic data interchange, systems development, and contingency planning. This rating should reflect the adequacy of the organization's overall IT audit program, including the internal and external audit's abilities to detect and report significant risks to management and the board of directors on a timely basis. It should also reflect the internal and external auditor's capability to promote a safe, sound and effective operation.

The performance of audit is rated based upon an assessment of factors, such as:

- The level of independence maintained by audit and the quality of the oversight and support provided by the board of directors and management;
- The adequacy of audit's risk analysis methodology used to prioritize the allocation of audit resources and to formulate the audit schedule;
- The scope, frequency, accuracy, and timeliness of internal and external audit reports;
- The extent of audit participation in application development, acquisition, and testing, to ensure the effectiveness of internal controls and audit trails;
- The adequacy of the overall audit plan in providing appropriate coverage of IT risks;
- The auditor's adherence to codes of ethics and professional audit standards;
- The qualifications of the auditor, staff succession, and continued development through training;
- The existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses; and
- The quality and effectiveness of internal and external audit activity as it relates to IT controls.

Ratings

- **A rating of 1** indicates strong audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or its audit committee in a thorough and timely manner. Outstanding audit issues are monitored until resolved. Risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities with appropriate scope and frequency. Audit work is performed in accordance with professional auditing standards and report content is timely, constructive, accurate, and complete. Because audit is strong, examiners may place substantial reliance on audit results.

- **A rating of 2** indicates satisfactory audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or audit committee, but reports may be less timely. Significant outstanding audit issues are monitored until resolved. Risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities; however, minor concerns may be noted with the scope or frequency. Audit work is performed in accordance with professional auditing standards; however, minor or infrequent problems may arise with the timeliness, completeness, and accuracy of reports. Because audit is satisfactory, examiners may rely on audit results but because minor concerns exist, examiners may need to expand verification procedures in certain situations.

- **A rating of 3** indicates less than satisfactory audit performance. Audit identifies and reports weaknesses and risks; however, independence may be compromised and reports presented to the board or audit committee may be less than satisfactory in content and timeliness. Outstanding audit issues may not be adequately monitored. Risk analysis is less than satisfactory. As a result, the audit plan may not provide sufficient audit scope or frequency for IT operations, procurement, and development activities. Audit work is generally performed in accordance with professional auditing standards; however, occasional problems may be noted with the timeliness, completeness, or accuracy of reports. Because audit is less than satisfactory, examiners must use caution if they rely on the audit results.

- **A rating of 4** indicates deficient audit performance. Audit may identify weaknesses and risks but it may not independently report to the board or audit committee and report content may be inadequate. Outstanding audit issues may not be adequately monitored and resolved. Risk analysis is deficient. As a result, the audit plan does not provide adequate audit scope or frequency for IT operations, procurement, and development activities. Audit work is often inconsistent with professional auditing standards and the timeliness, accuracy, and completeness of reports is unacceptable. Because audit is deficient, examiners cannot rely on audit results.

- **A rating of 5** indicates critically deficient audit performance. If an audit function exists, it lacks sufficient independence and, as a result, does not identify and report

weaknesses or risks to the board or audit committee. Outstanding audit issues are not tracked and no follow-up is performed to monitor their resolution. Risk analysis is critically deficient. As a result, the audit plan is ineffective and provides inappropriate audit scope and frequency for IT operations, procurement, and development activities. Audit work is not performed in accordance with professional auditing standards and major deficiencies are noted regarding the timeliness, accuracy, and completeness of audit reports. Because audit is critically deficient, examiners cannot rely on audit results.

Management

This rating reflects the abilities of the board and management as they apply to all aspects of IT acquisition, development, and operations. Management practices may need to address some or all of the following IT-related risks: strategic planning, quality assurance, project management, risk assessment, infrastructure and architecture, end-user computing, contract administration of third-party service providers, organization and human resources, and regulatory and legal compliance. Generally, directors need not be actively involved in day-to-day operations; however, they must provide clear guidance regarding acceptable risk exposure levels and ensure that appropriate policies, procedures, and practices have been established. Sound management practices are demonstrated through active oversight by the board of directors and management, competent personnel, sound IT plans, adequate policies and standards, an effective control environment, and risk monitoring. This rating should reflect the ability of the board and management as it applies to all aspects of IT operations. The performance of management and the quality of risk management are rated based upon an assessment of factors such as:

- The level and quality of oversight and support of the IT activities by the board of directors and management;
- The ability of management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions;
- The ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner;
- The adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
- The effectiveness of risk monitoring systems;
- The timeliness of corrective action for reported and known problems;
- The level of awareness of and compliance with laws and regulations;
- The level of planning for management succession;
- The ability of management to monitor the services delivered and to measure the organization's progress toward identified goals in an effective and efficient manner;

- The adequacy of contracts and management's ability to monitor relationships with third-party servicers;
- The adequacy of strategic planning and risk management practices to identify, measure, monitor, and control risks, including management's ability to perform self-assessments; and
- The ability of management to identify, measure, monitor, and control risks and to address emerging information technology needs and solutions.
- In addition to the above, factors such as the following are included in the assessment of management at servicer providers:
- The financial condition and ongoing viability of the entity;
- The impact of external and internal trends and other factors on the ability of the entity to support continued servicing of client financial institutions; and
- The propriety of contractual terms and plans.

Ratings

- **A rating of 1** indicates strong performance by management and the board. Effective risk management practices are in place to guide IT activities, and risks are consistently and effectively identified, measured, controlled, and monitored. Management immediately resolves audit and regulatory concerns to ensure sound operations. Written technology plans, policies and procedures, and standards are thorough and properly reflect the complexity of the IT environment. They have been formally adopted, communicated, and enforced throughout the organization. IT systems provide accurate, timely reports to management. These reports serve as the basis of major decisions and as an effective performance-monitoring tool. Outsourcing arrangements are based on comprehensive planning; routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided. Management and the board have demonstrated the ability to promptly and successfully address existing IT problems and potential risks.

- **A rating of 2** indicates satisfactory performance by management and the board. Adequate risk management practices are in place and guide IT activities. Significant IT risks are identified, measured, monitored, and controlled; however, risk management processes may be less structured or inconsistently applied and modest weaknesses exist. Management routinely resolves audit and regulatory concerns to ensure effective and sound operations; however, corrective actions may not always be implemented in a timely manner. Technology plans, policies, procedures, and standards are adequate and are formally adopted. However, minor weaknesses may exist in management's ability to communicate and enforce them throughout the organization. IT systems provide quality reports to management that serve as a

basis for major decisions and a tool for performance planning and monitoring. Isolated or temporary problems with timeliness, accuracy, or consistency of reports may exist. Outsourcing arrangements are adequately planned and controlled by management, and provide for a general understanding of vendor contracts, performance standards, and services provided. Management and the board have demonstrated the ability to address existing IT problems and risks successfully.

- **A rating of 3** indicates less than satisfactory performance by management and the board. Risk management practices may be weak and offer limited guidance for IT activities. Most IT risks are generally identified; however, processes to measure and monitor risk may be flawed. As a result, management's ability to control risk is less than satisfactory. Regulatory and audit concerns may be addressed, but time frames are often excessive and the corrective action taken may be inappropriate. Management may be unwilling or incapable of addressing deficiencies. Technology plans, policies, procedures, and standards exist, but may be incomplete. They may not be formally adopted, effectively communicated, or enforced throughout the organization. IT systems provide requested reports to management, but periodic problems with accuracy, consistency, and timeliness lessen the reliability and usefulness of reports and may adversely affect decision making and performance monitoring. Outsourcing arrangements may be entered into without thorough planning. Management may provide only cursory supervision that limits its understanding of vendor contracts, performance standards, and services provided. Management and the board may not be capable of addressing existing IT problems and risks, as evidenced by untimely corrective actions for outstanding IT problems.

- **A rating of 4** indicates deficient performance by management and the board. Risk management practices are inadequate and do not provide sufficient guidance for IT activities. Critical IT risks are not properly identified, and processes to measure and monitor risks are not properly identified, and processes to measure and monitor risks are deficient. As a result, management may not be aware of and is unable to control risks. Management may be unwilling or incapable of addressing audit and regulatory deficiencies in an effective and timely manner. Technology plans, policies and procedures, and standards are inadequate, have not been formally adopted or effectively communicated throughout the organization, and management does not effectively enforce them. IT systems do not routinely provide management with accurate, consistent, and reliable reports, thus contributing to ineffective performance monitoring or flawed decision-making. Outstanding arrangements may be entered into without planning or analysis, and management may provide little or no supervision of vendor contracts, performance standards, or services provided. Management and the board are unable to address existing IT problems and risks, as evidenced by ineffective actions and longstanding IT weaknesses. Strengthening of management and its processes is necessary. The financial condition of the service provider may threaten its viability.

- **A rating of 5** indicates critically deficient performance by management and the board. Risk management practices are severely flawed and provide inadequate guidance for IT activities. Critical IT risks are not identified, and processes to measure and monitor risks do not exist, or are not effective. Management's inability to control risk may threaten the continued viability of the institution or service provider.

Management is unable or unwilling to correct audit and regulatory identified deficiencies and immediate action by the board is required to preserve the viability of the institution or service provider. If they exist, technology plans, policies, procedures, and standards are critically deficient. Because of systemic problems, IT systems do not produce management reports that are accurate, timely, or relevant. Outsourcing arrangements may have been entered into without management planning or analysis, resulting in significant losses to the financial institution or ineffective vendor services. The financial condition of the service provider presents an imminent threat to its viability.

Development and Acquisition

This rating reflects an organization's ability to identify, acquire, install, and maintain appropriate information technology solutions. Management practices may need to address all or parts of the business process for implementing any kind of change to the hardware or software used. These business processes include an institution's or service provider's purchase of hardware or software, development and programming performed by the institution or service provider, purchase of services from independent vendors or affiliated data centers, or a combination of these activities. The business process is defined as all phases taken to implement a change including researching alternatives available, choosing an appropriate option for the organization as a whole, converting to the new system, or integrating the new system with existing systems. This rating reflects the adequacy of the institution's systems development methodology and related risk technology. This rating also reflects the board's and management's ability to enhance and replace information technology prudently in a controlled environment. The performance of systems development and acquisition and related risk management practice is rated based upon an assessment of factors such as:

- The level and quality of oversight and support of systems development and acquisition activities by senior management and the board of directors;
- The adequacy of the organizational and management structures to establish accountability and responsibility for IT systems and technology initiatives;
- The volume, nature, and extent of risk exposure to the financial institution in the area of systems development and acquisition;
- The adequacy of the institution's system development life cycle (SDLC) and programming standards;
- The quality of project management programs and practices which are followed by developers, operators, executive management/owners, independent vendors or affiliated servicers, and end users;
- The independence of the quality assurance function and the adequacy of controls over program changes;
- The quality and thoroughness of system documentation;

- The integrity and security of the network, system, and application software;
- The development of information technology solutions that meet the needs of end users; and
- The extent of end user involvement in the system development process.
- In addition to the above, factors such as the following are included in the assessment of development and acquisition at service providers:
    - The quality of software releases and documentation; and
    - The adequacy of training provided to clients.

Ratings

- **A rating of 1** indicates strong systems development, acquisition, implementation, and change management performance. Management and the board routinely demonstrate successfully the ability to identify and implement appropriate IT solutions while effectively managing risk. Project management techniques and the SDLC are fully effective and supported by written policies, procedures, and project controls that consistently result in timely and efficient project completion. An independent quality assurance function provides strong controls over testing and program change management. Technology solutions consistently meet end-user needs. No significant weaknesses or problems exist.

- **A rating of 2** indicates satisfactory systems development, acquisition, implementation, and change management performance. Management and the board frequently demonstrate the ability to identify and implement appropriate IT solutions while managing risk. Project management and the SDLC are generally effective; however, weaknesses may exist that result in minor project delays or cost overruns. An independent quality assurance function provides adequate supervision of testing and program change management, but minor weaknesses may exist. Technology solutions meet end-user needs. However, minor enhancements may be necessary to meet original user expectations. Weaknesses may exist; however, they are not significant and they are easily corrected in the normal course of business.

- **A rating of 3** indicates less than satisfactory systems development, acquisition, implementation, and change management performance. Management and the board may often be unsuccessful in identifying and implementing appropriate IT solutions; therefore, unwarranted risk exposure may exist. Project management techniques and the SDLC are weak and may result in frequent project delays, backlogs or significant cost overruns. The quality assurance function may not be independent of the programming function, which may adversely impact the integrity of testing, and program change management. Technology solutions generally meet end-user

needs, but often require an inordinate level of change after implementation. Because of weaknesses, significant problems may arise that could result in disruption to operations or significant losses.

- **A rating of 4** indicates deficient systems development, acquisition, implementation, and change management performance. Management and the board may be unable to identify and implement appropriate IT solutions and do not effectively manage risk. Project management techniques and the SDLC are ineffective and may result in severe project delays and cost overruns. The quality assurance function is not fully effective and may not provide independent or comprehensive review of testing controls or program change management. Technology solutions may not meet the critical needs of the organization. Problems and significant risks exist that require immediate action by the board and management to preserve the soundness of the institution.

- **A rating of 5** indicates critically deficient systems development, acquisition, implementation, and change-management performance. Management and the board appear to be incapable of identifying and implementing appropriate information technology solutions. If they exist, project management techniques and the SDLC are critically deficient and provide little or no direction for development of systems or technology projects. The quality assurance function is severely deficient or not present and unidentified problems in testing and program change management have caused significant IT risks. Technology solutions do not meet the needs of the organization. Serious problems and significant risks exist that raise concern for the financial institution or service provider's ongoing viability.

Support and Delivery

This rating reflects an organization's ability to provide technology services in a secure environment. It reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information delivery system. The factors include customer support and training, and the ability to manage problems and incidents, operations, system performance, capacity planning, and facility and data management. Risk management practices should promote effective, safe, and sound IT operations that ensure the continuity of operations and the reliability and availability of data. The scope of this component rating includes operational risks throughout the organization and service providers.

The rating of IT support and delivery is based on a review and assessment of requirements such as:

- The ability to provide a level of service that meets the requirements of the business;
- The adequacy of security policies, procedures, and practices in all units and at all levels of the financial institution and service providers;

- The adequacy of data controls over preparation, input, processing, and output;
- The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers and business units;
- The quality of processes or programs that monitor capacity and performance;
- The adequacy of controls and the ability to monitor controls at service providers;
- The quality of assistance provided to users, including the ability to handle problems;
- The adequacy of operating policies, procedures, and manuals;
- The quality of physical and logical security, including the privacy of data;
- The adequacy of firewall architectures and the security of connections with public networks.
- In addition to the above, factors such as the following are included in the assessment of support and delivery at service providers:
  - The adequacy of customer service provided to clients; and
  - The ability of the entity to provide and maintain service level performance that meets the requirements of the client.

Ratings

- **A rating of 1** indicates strong IT support and delivery performance. The organization provides technology services that are reliable and consistent. Service levels adhere to well-defined service-level agreements and routinely meet or exceed business requirements. A comprehensive corporate contingency and business resumption plan is in place. Annual contingency plan testing and updating is performed; and, critical systems and applications are recovered within acceptable time frames. A formal written data security policy and awareness program is communicated and enforced throughout the organization. The logical and physical security for all IT platforms is closely monitored, and security incidents and weaknesses are identified and quickly corrected. Relationships with third-party service providers are closely monitored. IT operations are highly reliable, and risk exposure is successfully identified and controlled.

- **A rating of 2** indicates satisfactory IT support and delivery performance. The organization provides technology services that are generally reliable and consistent; however, minor discrepancies in service levels may occur. Service performance adheres to service agreements and meets business requirements. A corporate contingency and business resumption plan is in place, but minor enhancements may be necessary. Annual plan testing and updating is performed and minor problems may occur when recovering systems or applications. A written data security policy is

in place but may require improvement to ensure its adequacy. The policy is generally enforced and communicated throughout the organization, e.g., through a security awareness program. The logical and physical security for critical IT platforms is satisfactory. Systems are monitored, and security incidents and weaknesses are identified and resolved within reasonable time frames. Relationships with third-party service providers are monitored. Critical IT operations are reliable and risk exposure is reasonably identified and controlled.

- **A rating of 3** indicates that the performance of IT support and delivery is less than satisfactory and needs improvement. The organization provides technology services that may not be reliable or consistent. As a result, service levels periodically do not adhere to service-level agreements or meet business requirements. A corporate contingency and business resumption plan is in place but may not be considered comprehensive. The plan is periodically tested; however, the recovery of critical systems and applications is frequently unsuccessful. A data security policy exists; however, it may not be strictly enforced or communicated throughout the organization. The logical and physical security for critical IT platforms is less that satisfactory. Systems are monitored; however, security incidents and weaknesses may not be resolved in a timely manner. Relationships with third-party service providers may not be adequately monitored. IT operations are not acceptable and unwarranted risk exposures exist. If not corrected, weaknesses could cause performance degradation or disruption to operations.

- **A rating of 4** indicates deficient IT support and delivery performance. The organization provides technology services that are unreliable and inconsistent. Service-level agreements are poorly defined and service performance usually fails to meet business requirements. A corporate contingency and business resumption plan may exist, but its content is critically deficient. If contingency testing is performed, management is typically unable to recover critical systems and applications. A data security policy may not exist. As a result, serious supervisory concerns over security and the integrity of data exist. The logical and physical security for critical IT platforms is deficient. Systems may be monitored, but security incidents and weaknesses are not successfully identified or resolved. Relationships with third-party service providers are not monitored. IT operations are not reliable and significant risk exposure exists. Degradation in performance is evident and frequent disruption in operations has occurred.

- **A rating of 5** indicates critically deficient IT support and delivery performance. The organization provides technology services that are not reliable or consistent. Service-level agreements do not exist and service performance does not meet business requirements. A corporate contingency and business resumption plan does not exist. Contingency testing is not performed and management has not demonstrated the ability to recover critical systems and applications. A data security policy does not exist, and a serious threat to the organization's security and data integrity exists. The logical and physical security for critical IT platforms is inadequate, and management does not monitor systems for security incidents and weaknesses. Relationships with third-party service providers are not monitored, and the viability of a service provider may be in jeopardy. IT operations are severely deficient, and the seriousness of weaknesses could cause failure of the financial institution or service provider if not

addressed.