Federal Financial Institutions Examination Council

FFIEC

Supervision of Technology Service Providers

TSP

MARCH 2003

IT EXAMINATION

HANDBOOK

TABLE OF CONTENTS

INTRODUCTION 1

RISK-BASED SUPERVISION 3

Risk Assessment 4
Uniform Rating System for Information Technology 5
Risk Management 6
Audit and Internal Control 7
Supervisory Strategies 7
- Objectives 7
- Work plans 7
- Activities 8

SUPERVISORY PROCESS 9

FFIEC Work Products 9
Frequency of IT Examinations 9
Examination Responsibilities 10
Examination Planning 11
Examination Scope 11
Request Information 12
Entrance Meeting 12
Work Papers 12
Exit Conference 13
Board Meeting 13
FFIEC IT Report of Examination 13
Report Distribution 14

MULTI-REGIONAL DATA PROCESSING SERVICER PROGRAM. 15

Responsibilities of Agency-In-Charge (AIC) 15
Risk Ranking OF MDPS Examinations 16
General Procedures 16
- Pre-Examination Procedures 16
- MDPS Examiner-in-Charge Responsibilities 16
- Scope of Examination 17

Supervisory Timeline 17
Presentation of Findings and Recommendations 17
Work Papers and Workprograms 17
Regular Off-site Reviews 18
Report Preparation and Distribution 18
Report Preparation 18
Rating 18
Recommendations 19
Distribution 19

SHARED APPLICATION SOFTWARE REVIEWS 20
Purpose of the SASR Program 20
Objectives of the SASR Program 20
Responsibility 21
Program Administration 21

APPENDIX A: EXAMINATION PLANNING PROCEDURES A-1

APPENDIX B: EXAMINATION PRIORITY RANKING SHEET B-1

APPENDIX C: REPORT OF EXAMINATION C-1

APPENDIX D: UNIFORM RATING SYSTEM FOR INFORMATION TECHNOLOGY D-1

INTRODUCTION

The "Supervision of Technology Service Providers" booklet is one of a series of updates to the 1996 *FFIEC Information Systems Examination Handbook* and rescinds chapters 2–7 of that handbook. This booklet primarily governs the supervision of technology service providers (TSPs)[1] and briefly summarizes the Federal Financial Institutions Examination Council (FFIEC) member agencies' (agencies) expectations of financial institutions in the oversight and management of their TSP relationships. This booklet outlines the agencies' risk-based supervision approach, the supervisory process, and the examination ratings used for information technology (IT) service providers[2]. In addition, this booklet discusses two special IT-related programs administered by the FFIEC agencies: the Multi-Regional Data Processing Servicer (MDPS) Program, geared towards examining large TSPs, and the Shared Application Software Review (SASR) Program aimed at reviewing mission-critical software packages.

Many financial institutions outsource IT processing to a TSP. 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 these activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations. Financial institutions should have a comprehensive outsourcing risk management process to govern their TSP relationships. Such processes should include risk assessment, selection of service providers, contract review, and monitoring of service providers[3]. Many TSP relationships should be subject to the same risk management, security, privacy, and other internal controls and policies that would be expected if the financial institution were conducting the activities directly. This handbook primarily focuses on how the agencies review TSPs based upon risk. For more details on how to assess institutional risk, refer to the other booklets in this series.

To help ensure that the client financial institutions operate in a safe and sound manner, the services performed by TSPs are subject to regulation and examination.[4] The federal

---

[1] The term TSP generally includes independent data centers including Multi-Regional Data Processing Servicers, joint venture/limited liability corporations, and bank service corporations.

[2] NCUA follows the outlined supervision approach, supervisory process, and examination rating methodology for TSP reviews that it conducts or participates under the auspices of the FFIEC. NCUA utilizes its established supervision approach, supervisory process, and examination rating methodology for the voluntary reviews of TSPs that it independently conducts.

[3] Additional information on appropriate due diligence and oversight of outsourced technology services and third-party vendor relationships can be found in FFIEC Bulletin "Risk Management of Outsourced Technology Services" (November 28, 2000) and in other sections of the *FFIEC IT Handbook.*

financial regulators have the statutory authority to supervise all of the activities and records of the financial institution whether performed by the institution or by a third party on or off of the premises of the financial institution. Accordingly, the examination and supervision of a financial institution is not hindered by a transfer of the institution's records to another organization or by having another organization carry out all or part of the financial institution's functions.[5]

[4] See 12 USC 1867 (c)(1) and 12 USC 1464 (d)(7). The NCUA does not currently have independent regulatory authority over TSPs.

[5] S. Rep. No. 2105, 87th Cong. 2d Sess. 3 (1962) reprinted in 1962 U.S. Code Cong. & Ad. News 3878, 3880.

RISK-BASED SUPERVISION

The FFIEC agencies base their IT examination process on the concept of on-going, risk-based supervision. Risk-based supervision of TSPs is designed to

- Identify existing or potential risks associated with the TSP that could adversely affect serviced financial institutions;
- Evaluate the overall integrity and effectiveness of the TSP's risk management systems and controls;
- Determine compliance with any applicable laws or regulations that affect the services provided to financial institutions;
- Communicate findings, recommendations, and any required corrective actions in a clear and timely manner to TSP management, and as appropriate, to client financial institutions and supervisory personnel;
- Obtain commitments to correct significant deficiencies and verify the effectiveness of corrective actions; and
- Monitor any significant changes in a TSP's products, services, or risk management practices that would adversely affect its risk profile or those of its client financial institutions.

The FFIEC agencies' risk-based supervision consists of the identification and selection of TSPs warranting examination by IT examiners, followed by the development of a risk-based supervisory strategy for each entity including any necessary follow-up reviews. This approach provides for examination coverage of selected TSPs including core application processors, electronic funds transfer switches, Internet banking providers, item processors, etc.

To assist in the scheduling and prioritization of TSP examinations, the FFIEC agencies use an "Examination Priority Ranking Sheet" (Appendix B). This worksheet groups TSPs into various supervisory priorities, based on the relative risk of their business lines, their client base, and their overall controls and risk management oversight. Higher-risk TSPs are subject to more frequent and extensive examinations and reviews.

Examiners develop an initial risk profile for a TSP from information gathered during examinations, from supervisory activities, and from reports prepared by independent third parties, for example, external audits.

When conducting IT examinations, examiners should focus on the underlying risk issues that are common to all IT activities:

- *Management of Technology*—The planning and overseeing of technological resources and services and ensuring they support the strategic goals and objectives of the financial institution or TSP.

- *Integrity of Data*—The accuracy and reliability of automated information and associated management information systems.
- *Confidentiality of Information*—The protection of information from intentional or inadvertent disclosure to unauthorized individuals.
- *Availability of Services*—The effectiveness of business continuity programs and adherence to service-level agreements.
- *Financial Stability*—The maintenance of capital to support ongoing operations and the ability to generate a profit to support capital levels and the adequacy of liquidity due to potentially overvalued technology assets or cash shortages during times of rapid growth. Financial difficulties at the TSP can negatively affect the serviced financial institution through deteriorating quality of service, reliability of service, or adequacy of controls.

RISK ASSESSMENT

Transaction risk (also referred to as operational risk) is the primary risk associated with TSP processing. Transaction risk may arise from fraud, error, or the inability to deliver products or services, maintain a competitive position, or manage information. It exists in each process involved in the delivery of TSPs' products or services. Transaction risk not only includes operations and transaction processing, but also areas such as customer service, systems development and support, internal control processes, and capacity planning. Transaction risk also may affect other risks such as credit, interest rate, compliance, liquidity, price, strategic or reputation. Some other TSP risks include

- *Reputation risk*—Errors, delays, or omissions in information technology 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.

- *Interest rate, liquidity, and price (market) risk*—Processing errors related to investment income or repayment assumptions could increase interest rate risks of serviced financial institutions.

Examiners should determine the degree of risk and the quality of risk management of the TSP at each examination. Their assessments of a TSP's degree and quality of risk management should be discussed with TSP management and factored into the TSP's "Examination Priority Ranking Sheet" and its supervisory ratings. Examiners also should explain how the TSP's deficiencies increase the risk to the serviced institutions. For example, inadequate business resumption plans at the TSP may increase the transaction and reputation risks at serviced institutions.

The quantity of transaction/operational risk at a TSP is the level or volume of risk that exists. Examiners should consider the following factors in evaluating the quantity of transaction/operational risk:

- Financial condition of the TSP
- Number of client institutions serviced
- Volume (both dollar value and quantity) of transactions processed for serviced financial institutions
- Aggregate size (both dollar value and quantity) of all regulated financial institutions serviced
- Number and type of product lines provided
- Reliability of the technology used
- Adequacy of business continuity planning

The quality of transaction/operational risk management is an assessment of how well risks are identified, measured, controlled, and monitored. Examiners should consider the following factors in evaluating the quality of transaction/operational risk:

- The quality of the TSP's policies;
- The adequacy of the TSP's control and operational processes;
- The extent of the TSP's technical and managerial expertise;
- Directorate oversight; and
- The timeliness and completeness of management information systems that are used to measure performance, make decisions about risk, and assess the effectiveness of processes

UNIFORM RATING SYSTEM FOR INFORMATION TECHNOLOGY

The FFIEC agencies use the Uniform Rating System for Information Technology (URSIT) to assess and rate IT-related risks of financial institutions and TSPs. The primary purpose of the rating system is to identify those entities whose condition or performance of information technology functions requires special supervisory attention.

This rating system assists examiners in making an assessment of risk and compiling examination findings. Examiners should use the rating system to help evaluate the entity's overall risk exposure and risk management performance, and determine the degree of supervisory attention necessary to ensure that weaknesses are addressed and that risk is properly managed. The FFIEC agencies require the use of URSIT for all nonbank TSPs selected for examination.

The URSIT is based on a risk evaluation of four critical components: audit; management; development and acquisition; and support and delivery (AMDS). These components are used to assess the overall performance of IT within an organization (e.g., the composite rating). Examiners evaluate the functions identified within each component to assess the institution's ability to identify, measure, monitor and control information technology risks. Please refer to Appendix D for additional information on composite and component URSIT ratings.

RISK MANAGEMENT

The FFIEC 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 FFIEC 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 vendors, including a review of the risk management systems used by the TSP. Such reviews should include measures taken by the TSPs to protect information about financial institutions' customers. Financial institutions should monitor their TSPs to confirm that they implement adequate security measures. As part of this monitoring, financial institutions should review information such as TSP service-level reports, audits, internal control testing results, and other equivalent evaluations of their TSPs.

Examiners may identify situations where a TSP has weak risk management controls requiring corrective action. In such situations, the TSP's serviced institutions may also have to take remedial actions since they have the ultimate responsibility to properly manage their risks.

TSPs and financial institutions should monitor changes in laws, regulations, and guidance that affect the services provided to financial institutions.

AUDIT AND INTERNAL CONTROL

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 control systems. The FFIEC agencies encourage the use of well-supported risk-based auditing. Through this process, the board, management, and auditors can focus their resources on the areas of greatest risk.

Examiners' assessments of the adequacy of audit and internal control assist in effectively using supervisory resources, establishing the scope of current and future supervisory activities, and assessing the quality of risk management. TSPs with an effective risk-based auditing program typically require less examination work by regulatory agencies.

Additional guidance on what examiners review in information system audit and internal control functions can be found in the "Audit" and "Management" booklets of the FFIEC IT Handbook.

SUPERVISORY STRATEGIES

A supervisory strategy is a plan to provide effective, efficient examinations for each organization. The supervisory strategy should address the supervisory objectives, specific work plans, and the planned supervisory activities. The examiner-in-charge (EIC) prepares the supervisory strategy that directs the examination activities and reflects

- Statutory and policy-based examination requirements
- Knowledge of the institution including
  - Risk profile and risk management system;
  - Strengths and weaknesses, including areas where examiners have noted exceptions in the past;
  - Supervisory history; and
  - Market factors.

OBJECTIVES

The EIC should base supervisory objectives for a TSP examination on the TSP's risk profile and appropriate statutory or agency standards. The supervisory objectives are the foundation for all activities and work plans. Well-defined objectives provide for focused and efficient activities and ensure consistent and appropriate application of supervisory policy. Supervisory objectives must be clear, attainable, specific, and action oriented.

WORK PLANS

Examination work plans provide the documented methodology for achieving the TSP supervisory strategies. Work plans detail the scope, timing, and resources needed to meet supervisory objectives and strategies.

ACTIVITIES

Supervisory activities detail the steps that will achieve supervisory objectives. Each activity should link directly to one or more of the supervisory objectives. They should be focused on ensuring that risk management systems operate effectively. Activities should include a plan for communicating with the TSP (e.g., reports of examination, meeting with the board of directors).

SUPERVISORY PROCESS

This section reviews the process for examining a TSP. It explains the different types of FFIEC work products and details the responsibilities of IT examiners for TSP examinations.

FFIEC WORK PRODUCTS

- *Technology Service Provider (TSP) Examinations*—TSPs include independent data centers, joint venture/limited liability corporations, and bank service corporations. The FFIEC agencies examine these entities to identify existing or potential risks that could adversely affect serviced financial institutions.
- *Multi-Regional Data Processing Servicer (MDPS) Examinations*—MDPS companies may be regional or national in scope and service more than one class of financial institution. The FFIEC IT subcommittee selects TSPs for the MDPS program based upon their systemic risk to the banking industry. For MDPS companies, the FFIEC agencies supplement on-site examination coverage with the Enhanced Supervisory Program (ESP). The ESP provides for interim reviews of material changes in the company's activities or condition. The ESP allows each agency to more promptly recognize and supervise risks associated with systemically significant service providers. An ESP visitation usually results in a letter to the board of directors communicating any findings or concerns.
- *Shared Application Software Review (SASR)*—An SASR is typically an interagency review of software programs or systems in use at financial institutions. The primary objective of these reviews is to identify potential systemic risks posed by such programs or systems. SASRs can help reduce the time and resources needed to examine software systems at individual financial institutions.
- *Follow-Up Review*—The purpose of these reviews is to maintain communications with TSPs between on-site examinations; to identify significant changes in management, products, services, or risk management practices affecting serviced financial institutions; to follow up on any issues or concerns previously identified; and to confirm business-line and service provider risk designations and the resulting examination priority, and to update supervisory strategies.

FREQUENCY OF IT EXAMINATIONS

The frequency of IT examinations varies based on the risk profile of the TSP (i.e., the lower the risk, the less often examinations need to be done). Examiners determine risk based upon the TSP's risk factors noted on the FFIEC "Examination Priority Ranking Sheet" in Appendix B. The ranking sheet contains the business line risk rankings, TSPs'

risk categories, and recommended examination priority. Having established the examination priority, examiners use the "Summary of Supervisory Approach", contained in Appendix B, to determine the required frequency for supervisory activities. Occasionally, examiners will need to perform an unscheduled examination for areas of evolving supervisory interest or concern. In all cases, the IT examinations of TSPs that service more than one type of financial institution must be coordinated among the regulatory agencies during scheduling meetings held at the district/region or subcommittee levels, depending on the TSP involved.

EXAMINATION RESPONSIBILITIES

The EIC is responsible for the administration and overall performance of the IT examination. These responsibilities include, but are not limited to

- Developing and maintaining an effective risk-based strategy and examination scope;
- Communicating and coordinating all supervisory activities including examination planning, meetings, and written communication with the appropriate supervisory office, agency-in-charge, and participating agencies;
- Assisting in scheduling interagency examinations;
- Communicating examination plans with the TSP to coordinate on-site activity before the examination begins;
- Supervising the examination team to ensure the ratings, examination conclusions, procedures, work papers, and workdays are consistent with, and completed in accordance with, the approved supervisory strategy;
- Holding exit conferences with management and the board of directors, as appropriate, to review examination findings and recommendations for follow-up; and
- Writing the report of examination.

The supervisory office for the agency-in-charge (AIC) will assist the examiners by

- Coordinating interagency reviews;
- Ensuring that TSPs within its areas of responsibility receive IT examinations consistent with FFIEC policy outlined in Appendix B;
- Enforcing compliance with interagency agreements relating to TSP supervision;
- Ensuring appropriate staffing for examinations;
- Attending exit meetings, as appropriate;
- Reviewing and distributing the report of examination (ROE) to the TSP and the appropriate FFIEC agency offices; and

- Overseeing the potential distribution of ROEs to its regulated, serviced financial institutions. Each FFIEC agency is responsible for distributing ROEs to the serviced financial institutions it regulates.

EXAMINATION PLANNING

Examination planning is essential to effective supervision. Planning helps examiners develop risk-based strategies to effectively and efficiently examine each TSP. Planning begins with an examiner's assessment of current and anticipated risks. Examiners should give special attention to mergers and acquisitions, new products or services offered, and management changes. The EIC must gather, organize, and analyze available information prior to beginning an on-site IT examination. The extent of advance preparation depends on the complexity of the TSP's structure and on the type of services provided. Sources of information include, but are not limited to

- Approved supervisory strategy;
- Prior examination reports, work papers, and recommendations;
- Supervisory actions and correspondence;
- Internal and external audit reports, when available;
- Internal risk assessments or other reviews including security testing;
- Interim correspondence and memoranda related to the TSP;
- Financial statements and stock research reports;
- News reports;
- The TSP's Web site, as applicable; and
- SEC filings for public companies.

A work program to assist with planning is located in Appendix A.

EXAMINATION SCOPE

The EIC should determine the scope of examination work and estimate the workdays required for completion. For examinations of TSPs that have more than one data processing center, the EIC should evaluate the subsidiary data centers for risk. The scope should cover the headquarters location and any data center chosen in the planning stage. The EIC should prepare a scope memorandum that identifies the risks highlighted in the last examination, areas for further review, and examination schedule information. The scope memorandum also should outline the objectives of the examination, assignments, workday budget, and other relevant information.

During the task of setting the scope and throughout an examination, EICs should maintain regular communications with their supervisor and other agencies, if appropriate. EICs should promptly communicate any significant anticipated changes in scope, projected staffing, or completion dates to the supervisory office and their examination team.

REQUEST INFORMATION

At least four weeks prior to the start of the examination, the EIC should communicate with the TSP, notifying it of the upcoming examination. The communication should request items the TSP should have ready when the examiners arrive.

ENTRANCE MEETING

The EIC should schedule an entrance meeting with key TSP staff members to introduce the examination team and to identify primary points of contact for specific areas of review. The agenda of the entrance meeting should, at a minimum, include the following:

- Significant management or audit concerns;
- Significant planned or anticipated changes and developments in IT hardware or software;
- Effects of new developments since the last examination (e.g., changes in control or management);
- Actions taken to correct issues discussed in prior examination and audit reports;
- Financial performance;
- Significant changes in operations, strategies, services offered or client base;
- Economic and competitive conditions in market area;
- Plans for meetings with management or audit to update them on examination status; and
- Standard contract provisions between the TSP and its customers.

The EIC should also plan to meet frequently with TSP management to inform them of the progress of the review.

WORK PAPERS

Work papers are used to document IT examination procedures and support conclusions. Work papers should be prepared for every area reviewed during the examination. They must provide sufficient documentation for a reviewer to understand what was done, why it was done, and how conclusions were reached. The work papers for each area should contain only essential information that supports conclusions, violations of law or regulations, or any applicable corrective actions. The work papers should also clarify what needs to be done about the conclusions, either by the TSP or the AIC.

All conclusions must be properly documented and maintained in the examination's work papers. Examiners may obtain documentation by inspection, observation, inquiry, confirmation, or analytical tests. The EIC has the responsibility for reviewing all examination-related work papers prior to leaving the examination. The review should ensure that the overall quality of work papers is consistent with member agency standards.

Work papers are the joint property of the FFIEC agencies noted in the ROE. Examiners must secure work papers at all times. The IT examiner may not release examination work papers or ROEs outside of the FFIEC agencies without proper authorization.

Examiners and FFIEC agencies' staff must maintain control over all sensitive examination-related information on their portable computers. Following the completion of the examination, examiners and staff should promptly remove examination-related information from their portable computers. If work papers are kept in an electronic format, agency personnel should protect the confidentiality of work papers by sharing them only through secure communications that protect the documents from unauthorized access.

EXIT CONFERENCE

The objective of the exit conference is to communicate clearly the examiner's findings, conclusions, and recommendations, and to obtain/confirm management's commitment to any recommended corrective action. The EIC arranges the exit conference and prepares an agenda. The agenda should include the main issues contained in the draft examination report. All potential attendees should be informed of the meeting time and location several business days before the meeting date.

Before the meeting, the EIC should review all conclusions and recommendations with lower and mid-level management of the TSP. The EIC should research any disagreements before the exit conference to both validate the examination concern and to build additional support where needed.

BOARD MEETING

The EIC has the responsibility for presenting the ROE findings and conclusions at board meetings for composite 3-, 4-, and 5-rated TSPs. The AIC of the TSP examination should notify other FFIEC member agencies' supervisory office prior to issuing URSIT composite ratings of 3, 4 or 5 or engaging in informal or formal enforcement actions. A representative from the AIC should attend the meetings.

Examiners have the discretion to schedule board meetings for TSPs rated 1 or 2 when justified by the issues or other factors.

FFIEC IT REPORT OF EXAMINATION

The FFIEC has a uniform ROE format for IT examinations at TSPs. The ROE and preparation instructions are contained in Appendix C. The ROE contains an "Open Section," which is distributed to the TSP, and an "Administrative Section" that contains information for FFIEC agencies use only. All significant findings and conclusions, including management comments, should be presented in the open section (i.e., unsafe and unsound practices, noncompliance with statutes and regulations, and deficiencies noted). Matters of a proprietary nature and administrative information for agency use should be reported in the administrative section of the report.

The report should be completed by the EIC within 45 days of leaving the TSP or MDPS site. The supervisory office has an additional 15 days to review, revise, approve, and issue the report.

REPORT DISTRIBUTION

The ROE is generally distributed to three primary groups: the TSP, FFIEC agencies and serviced financial institutions. The ROE is distributed according to the following table:

ROE Components	Service Provider	FFIEC Agencies	Serviced Financial Institutions
Transmittal Letter[6]	X	X	
Open Section[7]	X	X	X[8]
Administrative Section[9]		X	

Each FFIEC agency distributes TSP examination reports to serviced financial institutions either automatically or upon request. Reports are automatically distributed to serviced financial institutions when the TSP receives a composite IT rating of 4 or 5. In addition, all serviced financial institutions can receive a copy of the ROE from their primary regulator if the financial institution is on the customer list of the respective ROE or the institution can provide documentation reflecting that it contracted with the TSP subsequent to the examination.

[6] A transmittal letter accompanies the ROE to remind recipients of the confidential disclosure requirements. It also includes the TSP rating.

[7] Includes examiners' conclusions and supporting comments.

[8] Only comments relevant to the services for which the financial institution contracted are transmitted.

[9] Confidential and for regulatory use only. It includes information of administrative use to the agencies.

MULTI-REGIONAL DATA PROCESSING SERVICER PROGRAM

An organization is considered for the Multi-Regional Data Processing Servicer (MDPS) Program when it processes:

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

The FFIEC agencies examine MDPS organizations because these entities pose a systemic risk to the banking system should one or more have operational or financial problems or fail. Since these companies service banks, thrifts, and credit unions, the FFIEC conducts interagency IT examinations of these large TSPs. Interagency IT examinations provide a single examination report for the TSP management and the board of directors.

The MDPS program represents a cooperative arrangement among FFIEC agencies for the achievement of shared common supervisory goals and objectives. All FFIEC agencies participate in key decisions on MDPS examinations through the FFIEC IT Subcommittee. Prior to September 30th of each year, the FFIEC IT Subcommittee of the Task Force on Supervision determines a schedule of MDPS examinations designating the servicer, the date of the examination, and the agency-in-charge (AIC) for the following cycle. The IT subcommittee agency representatives distribute the schedule to their respective regional/district offices.

The following MDPS examination guidelines supplement the policies and procedures contained in FFIEC SP-1: "Interagency IT Examination, Scheduling and Distribution Policy" and SP-11: "Enhanced Supervision Program for MDPS."

RESPONSIBILITIES OF AGENCY-IN-CHARGE (AIC)

The FFIEC IT subcommittee selects one AIC for the supervision of each MDPS company. The AIC administers the MDPS examination on behalf of all participant FFIEC agencies during the rotating cycle.

The AIC assigns the EIC for the MDPS examination. The EIC is responsible for including the requirements of participating agencies in the supervisory strategy and scope of supervisory activities, leading the on-site examination, assigning the ratings, writing the ROE, communicating the status of the examination to participating agencies, and conducting follow-up activities. The EIC will also conduct periodic reviews as required by agency policy. As overall lead of the examination, the EIC must work closely and com-

municate frequently with appropriate representatives of participating agencies including headquarters, district/region, and field personnel.

It is the responsibility of the upcoming AIC to ensure that the examiner who will be responsible for the supervision of the TSP/MDPS in the future participates in the current examination to facilitate and ensure a smooth transition. Participation in the current examination ensures that the EIC for the next cycle is familiar with the entire MDPS operation.

RISK RANKING OF MDPS EXAMINATIONS

Examiners will use the "Examination Priority Ranking Sheet" contained in Appendix B to risk-rank each MDPS organization. Occasionally, examiners will need to perform an unscheduled examination for areas of evolving supervisory interest or concern. Examiners should monitor the ongoing condition of MDPSs between examinations through regular off-site or informal reviews. This information should be coordinated with the FFIEC IT Subcommittee.

GENERAL PROCEDURES

PRE-EXAMINATION PROCEDURES

The pre-examination review is conducted by the EIC of the AIC to determine the scope of the overall examination, identify resource requirements, schedule events, and determine which data centers, based on their level of risk, should be examined. Based on this review, the EIC should prepare a document providing details on the organization's corporate history, corporate and organizational structure, scope of the upcoming examination, data centers included in the examination, data centers excluded from examination and the reason why they are excluded, schedule of examinations, and examiner resource requirements. The pre-examination review may include meetings with MDPS management to discuss changes that have taken place since the prior examination, or that may occur in the near future.

MDPS EXAMINER-IN-CHARGE RESPONSIBILITIES

In addition to the duties previously assigned to the IT examiner-in-charge in the supervisory process section of this booklet, the MDPS EIC is also responsible for the following:

- Scheduling and setting the scopes of MDPS examinations of corporate headquarters and remote data centers, based on input from all affected agencies;
- Coordinating resources to conduct examinations;
- Reviewing individual MDPS data center ROEs and resolving examination issues with the other agencies and MDPS management;

- Preparing the MDPS ROE, assigning ratings, signing the ROE and sending the ROE to the appropriate supervisory office for review and approval;
- Reviewing MDPS responses to ROE findings and recommending the appropriate response; and
- Adhering to the current FFIEC policies in place throughout the supervisory cycle.

SCOPE OF EXAMINATION

The EIC for the MDPS company develops the scope of the examination during the pre-examination review and selects the data centers to be examined. The AIC's headquarters presents the scope document to the FFIEC IT subcommittee for review and approval.

The EIC should complete the scope document and forward it to the AIC's Washington office for review by the IT subcommittee at least 150 days before the target date for the first on-site activity. The subcommittee should have 30 days to review and approve the scope document. The agency's headquarters office will distribute the examination scope document to the other regulatory agencies.

SUPERVISORY TIMELINE

The EIC sets the time frames for examining the data centers and for the submission of reports. Examinations of subsidiary data centers should generally not begin more than 30 days prior to the target date of the headquarters examination. The completed reports on these data centers should be submitted to the EIC for consolidation prior to the start of the headquarters examination. These reports should be sent within 30 days of completion of the on-site activity.

PRESENTATION OF FINDINGS AND RECOMMENDATIONS

The EIC will notify agency headquarters' staff of the date, time, and location of the presentation of examination findings and recommendations to management of the MDPS company. Each participating agency will have the opportunity to review the examination findings and be represented at the presentation. Normally, MDPS examination findings are presented first to senior management and then to the board of directors.

WORK PAPERS AND WORKPROGRAMS

The lead examiner for each subsidiary data center must review work papers to ensure that the examination findings are accurate and well documented. The AIC should retain work papers and workprograms in its Washington, regional, district, or field office as deemed appropriate by the AIC. If work papers are electronic, the AIC will store them in a manner consistent with its existing internal policies. If the AIC duties rotate, the current AIC will provide an index of electronically stored work papers and copy specific work paper documents at the request of the upcoming AIC.

REGULAR OFF-SITE REVIEWS

The MDPS AIC is responsible for completion of regular off-site and any interim ESP reviews. These reviews are used to assist in assessing controls, confirm the URSIT ratings and assigned examination priority, and maintain ongoing communications with the MDPS organization. These reviews should focus on identifying significant changes in management and risk management, new products and services, and mergers and acquisitions; determining inherent risk to supervised financial institutions; and following up on any issues or concerns. These reviews will generally be completed at least once between regularly scheduled examinations. Reviews may be conducted through correspondence, telephone interviews, or any other means determined to be appropriate by the AIC.

REPORT PREPARATION AND DISTRIBUTION

REPORT PREPARATION

The AIC is responsible for preparing a consolidated ROE. The ROE should give an overall view of the organization and include an evaluation of each data center examined. The ROE should contain an assessment of the major risks to the financial institutions serviced by the MDPS organization, recommendations for reducing or managing those risks, and management's responses to the findings and recommendations. The ROE should be prepared following the guidelines in this handbook.

The reports for any subsidiary data centers examined should be summarized and consolidated in the corresponding sections of the final ROE. To facilitate distribution of the ROE to the serviced financial institutions, the examiner should document findings for each subsidiary data center on a separate page of the report. Or, as an alternative, a separate subsidiary data center report may be issued with the approval of the MDPS EIC, AIC, and other regulatory agencies. Deviations from the consolidated report format should be approved by the AIC's headquarters office and by the other participating FFIEC agencies.

RATING

Each on-site MDPS examination will include one set of component ratings and one composite rating, based upon the overall condition of its entire operation. The MDPS ratings will follow URSIT (see Appendix D**).** Each MDPS subsidiary data center examined requires a separate rating. The ratings are disclosed to the subsidiary data center in a transmittal letter that accompanies the report of examination to the TSP. Ratings are *not* reported in the open section of the MDPS ROE; however, they are included in the administrative section, which is not provided to serviced financial institutions.

The AIC of the MDPS 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.

RECOMMENDATIONS

At the end of the examination, the MDPS EIC will provide recommendations to the AIC's supervisory office on resource requirements and the scope of subsequent examinations. These recommendations will assist in planning future MDPS examinations.

DISTRIBUTION

The AIC's headquarters office is responsible for distributing the final MDPS ROE to the TSP. The EIC will send the MDPS consolidated ROE to the appropriate supervisory office within his/her agency for review and approval before its distribution, as defined by his/her agency's procedures. The MDPS board of directors receives the open section of the final ROE. The ROE is also routed to the FFIEC IT subcommittee members for their distribution to their respective regulated, serviced financial institutions. Serviced institutions should only receive those portions of the report applicable to the services they receive. Some agencies' policies also call for further distribution to appropriate state supervisory agencies.

SHARED APPLICATION SOFTWARE REVIEWS

The FFIEC established the Shared Application Software Review (SASR) Program to employ interagency resources in uniform reviews of major software packages. These packages include stand-alone software and integrated (turnkey system) packages. Criteria for selection include, but are not limited to, purchased software that involves mission-critical applications used by a large number of financial institutions or high-risk applications. These applications include, but are not limited to, wire transfer, capital markets, securities transfer, loans, deposits, and general ledger. SASRs are for use by FFIEC agencies only. Their contents are not shared with the software vendor or the user financial institutions because FFIEC agencies do not have the authority to share SASRs with these respective entities.

PURPOSE OF THE SASR PROGRAM

The SASR program was designed to provide reviews of major software systems while conserving examiner resources. Only experienced IT examiners should prepare SASRs. Because of the continuing demand by all agencies for senior IT examiner resources, the performance of SASR reviews must be clearly beneficial when compared to costs. The FFIEC IT subcommittee has the responsibility for the selection of turnkey software packages included in the SASR reviews, and the scheduling of these reviews. The benefits of the program include

- Ensuring a cost effective use of agency/interagency IT examiner resources; and
- Equipping examiners with information and tools to assist in doing more comprehensive and accurate reviews of institutions using these systems and applications.

The use of SASR procedures is not limited to the review of community financial institution turnkey systems. The agencies can also use SASRs to support interagency safety and soundness initiatives when focusing on higher-risk applications in larger financial institutions. A SASR could evaluate financial institution software packages for use in wire transfer, capital markets, derivatives development/record keeping, securities transfer, asset management, or other lines of business.

OBJECTIVES OF THE SASR PROGRAM

The objectives of the SASR program are to

- Augment the IT examination work in community financial institutions;

- Provide examiners with information that can reduce time and resources needed to examine turnkey software systems;
- Reach conclusions on the adequacy of the software product and identify where compensating controls are needed to ensure financial institutions operate in a safe and sound manner;
- Identify potential systemic risks by reviewing software packages used by a large number of financial institutions; and
- Maintain a continuing knowledge of software upgrades and changes.

RESPONSIBILITY

The IT subcommittee has the ultimate responsibility for oversight of the national SASR program. The selection of packages for review should be made by September 30 of each year. In some cases, FFIEC regional offices will oversee SASRs conducted on software products that are not a part of the national SASR program. Annually, the IT subcommittee will

- Select the agency-in-charge (AIC) for each vendor/software product;
- Identify vendors and software packages for SASR review; and
- Establish and monitor schedules. The supervisory strategy of MDPS companies that have products subject to review should include the SASR activity, if applicable.

PROGRAM ADMINISTRATION

The designated AIC conducts the review in an institution that it supervises, and, with authorization from the vendor, at the vendor's location. The part of the review done at an institution should be part of the regular IT examination. The AIC also performs the following steps:

- Examiner-in-Charge Selection—The AIC should select an experienced IT examiner to supervise the review.
- Notification—The AIC must provide other agencies with at least six months' prior notice of the upcoming review to assure the availability of specialized IT examiners.
- Research—The AIC should perform preliminary research of the selected software product before beginning the review. The research information should include background data and a description of the organizational structure of the firm and any user group activity. Information collected before the review aids in setting its scope.
- Location Selection—The AIC has the responsibility for selecting the best location to conduct the software review and for notifying the participating agencies of the target review date.
- Scope document—A scope document for the review must be prepared in a manner similar to that of a MDPS. If a software review is

part of the MDPS examination, the AIC may include in the scope document for the MDPS examination the information discussed under "Research" and "Location Selection" bullets.

- Vendor Notification—The AIC should notify the vendor of the upcoming software review and request the designation of a contact person. The vendor may provide information and suggestions that enhance the review. The AIC should inform the vendor that the final product of the review is a confidential report for regulatory agencies' purposes only. The AIC should caution the vendor that it should not publicize his or her participation in the SASR program and no one should construe the review as an endorsement of the software program.
- Report—An internal confidential report, summarizing the review findings, must be completed and be strictly for regulatory purposes only.
- Exit Meeting—The AIC must conduct an exit meeting at the mutual convenience of the vendor and the participating examiners, unless the vendor refuses to meet. Ideally, the EIC will make a draft report available for this meeting with the vendor. The EIC may discuss the draft report with the vendor representative to ensure the accuracy of the information. However, the vendor cannot copy the draft and must return the draft to the examiners after the meeting. In addition, the EIC may request comments on planned enhancements to the software program. During the exit meeting, examiners should discuss significant areas of concern identified in the review. With the approval of the IT subcommittee or regional FFIEC contacts, the EIC may document significant concerns in a follow-up letter to the vendor.
- Review Submission—The EIC should complete and forward the SASR report for approval to the supervisory office of the AIC within 30 days from the completion of the on-site review.
- Document Review and Distribution—The AIC will review, approve, and distribute the final SASR report to the FFIEC agencies for internal agency use only. Each agency will distribute the final document to its respective regional office or district.
- Follow-up—The vendor should be requested to keep the AIC apprised of major software changes and enhancements.
- Scheduled Updates—Feedback from field examiners and other events can trigger a subsequent review. These events may include changes of ownership, significant software changes, or other developments.

APPENDIX A: EXAMINATION PLANNING PROCEDURES

This section assists examiners in planning the examination of a TSP. The examiner should consider the following steps when planning an examination.

1. Coordinate with appropriate agency personnel any preliminary materials, procedures, or other documentation that need review or development for the examination. Develop and mail examination request/first day letter and review any material received.
2. Review the following matters relevant to the current examination:
    - The previous report of examination and any other reports used to monitor the condition of the TSP;
    - The correspondence file, including any memoranda relevant to the current examination; and
    - Audit reports and third party reviews of outside servicers.
3. During planning, discuss with appropriate management and obtain current information on significant planned developments or important developments since the last examination. This may include relocations, mergers, acquisitions, major system conversions, changes in hardware and software, new products/services, changes in major contract services, staff or management changes and changes in internal audit operations. Consider:
    - Significant planned developments;
    - Important changes in IT policies;
    - Additions or deletions to customer service; and
    - Level of IT support the provider receives from outside servicers, if any.
4. Request information about the financial condition of any major servicer(s) who provide IT servicing to the TSP, if applicable.
5. Determine if the TSP offers Internet banking services. Indicate the vendor and functions performed.
6. Begin the process for obtaining data on serviced customers. This must include institution name, type of institution, city and state. Sort by regulatory agency first, followed by state.

CONCLUSIONS

1. From the materials reviewed, determine if significant changes occurred in operations that may affect the timing, staffing, and extent of testing necessary in the examination.
2. Assign assisting examiners to the applicable areas.
3. Provide any additional information that will facilitate future examinations.

APPENDIX B: EXAMINATION PRIORITY RANKING SHEET

I. Agency-In-Charge: **FDIC**_____ **FRB**_____ **NCUA**_____ **OCC**_____ **OTS**_____

Agency Representative _____ **Phone** _____

Location (Office) _____ **Email** _____

II. Technology Service Provider Name: _____

Corporate Address: _____

III. Business Line Risk Ranking **Higher** _____ **Average**_____ **Lower** _____

Business Lines: (Check ALL that apply)

Higher Risk:

_____ Asset Management Processing
_____ Clearing and Settlement
_____ Core Bank Processing
_____ Corporate Electronic Banking/Cash Management
_____ Disaster Recovery Services
_____ Wholesale Payments

Lower Risk:

_____ Bill Payment Services
_____ Check Processing
_____ Credit Card Issuance
_____ Imaging and Electronic Safekeeping
_____ Web Site Hosting (informational)

Average Risk:

_____ ACH Processing
_____ Aggregation & Other Emerging Technologies
_____ ATM/POS Processing and Switching
_____ Asset/Liability Management
_____ Credit Card Merchant Processing
_____ Credit Card Network/Switching
_____ Credit Scoring
_____ Employee Benefit Account Processing
_____ Loan and Mortgage Processing
_____ Investment Processing
_____ Retail Electronic Banking/Transactional Web Site Hosting

---

IV. TSP Risk Category: _____ **Higher** _____**Average**_____ **Lower**

Risk Factors: (Select only ONE, Higher, Average, or Lower for each Factor)

Factor	Higher Risk:	Average Risk:	Lower Risk:	NA*
1	☐ Large client base (250 or more supervised financial institutions, or based on other measures, e.g., aggregate client assets affected, transaction volume)	☐ Moderate-sized client base (at least 25 but not more than 249 supervised financial institutions, or based on other measures, e.g., aggregate assets affected; transaction volume).	☐ Small client base (less than 25 supervised financial institutions, or based on other measures, e.g., aggregate client assets affected; transaction volume).	☐
2	☐ Company rated URSIT 3, 4, or 5 at last examination.	☐ Company rated URSIT 2 at last examination.	☐ Company rated URSIT 1 at last examination.	☐
3	☐ Client institutions do not provide effective oversight; SAS 70 reports and other audit reviews are not comprehensive.	☐ Client institutions provide limited oversight; SAS 70 reports and audits cover most areas.	☐ Client institutions provide effective oversight; SAS 70 reports and other audit reviews are comprehensive.	☐
4	☐ Company is using new or untested technology or products. Company is undergoing significant organizational change.	☐ Company is using stable technology and products but implements significant upgrades. Company has minimal organization changes.	☐ Company is using stable technology and products. Company has stable organizational structure.	☐
5	☐ Client institutions or their examiners have reported problems or concerns that require supervisory follow-up.	☐ Client institutions or their examiners have reported minimal problems or concerns that require supervisory follow-up.	☐ Client institutions or their examiners have reported no problems or concerns that require supervisory follow-up.	☐

** If NA briefly explain in comment section below*

4/25/02

V. AIC's Recommended Examination Priority: **A**_____ **B**_____ **C**_____ **NA***_____

	Business Line Risk **Higher**	Business Line Risk **Average**	Business Line Risk **Lower**
Service Provider Risk **Higher**	Examination Priority A	Examination Priority A	Examination Priority B
Service Provider Risk **Average**	Examination Priority A	Examination Priority B	Examination Priority C
Service Provider Risk **Lower**	Examination Priority B	Examination Priority C	Examination Priority C

**Not Applicable ranking refers to a service provider not warranting interagency examination - Not all service providers have to be ranked A, B, or C.*

Recommend for MDPS Program: **Yes** ____ **No** ____ *(If yes, provide support for recommendation in comment section below)*

VI. Agency Agreement on Examination Priority: **Yes**_____ **No***_____

** If NO, explain in comment section below.*

Agency: Include name and phone # of agency representative		**Ranking**
FDIC:		
FRB:		
OCC:		
OTS:		
NCUA:		

VII. Comments:

SUMMARY OF SUPERVISORY APPROACH

Exam Priority	On-Site Examinations	Off-Site/ Informal Monitoring	Other
A	Interagency on-site examinations should be conducted at least every 24 months sufficient to establish or confirm URSIT ratings and determine appropriate off-site monitoring strategy.	Regular off-site or informal reviews (generally at least once between examinations) to confirm the risk ratings and assigned examination priority and maintain ongoing communication with the service provider. Reviews should focus on identifying significant changes in management and risk management, in the quantity of inherent risk to supervised financial institutions, or in products or services affecting financial institutions, and following up on any issues or concerns.	Regular review of monitoring and oversight by client institutions and user groups. A concise product/service review document will be provided (or updated) annually for internal use by regulatory examiners in assessing controls in place at client institutions.
B	Interagency on-site examinations should be conducted at least every 36 months sufficient to establish or confirm URSIT ratings and determine appropriate off-site monitoring strategy. Discussions with company management, limited scope visits, reviews of significant product and service issues, or other alternative supervisory strategies can satisfy the on-site supervision requirement.	Same as above for Priority A.	Same as above for Priority A.
C	Infrequent on-site examinations. For example, the supervisory strategy may call for an initial on-site visitation or limited scope examination.	Periodic (generally at least every 18 months) off-site or informal reviews to confirm the risk ratings and assigned examination priority and obtain information for product/service review documents. Reviews should focus on identifying significant changes in management and risk management, in the quantity of inherent risk to financial institutions, or in products or services affecting financial institutions, and following up on any issues or concerns.	Same as above for Priority A. Product/service review document may be combined with off-site/informal review documentation.

GENERAL INSTRUCTIONS FOR COMPLETING EXAMINATION PRIORITY RANKING SHEETS:

Only one "Examination Priority Ranking Sheet" (EPR) should be completed for each TSP, regardless of the fact that the TSP may have multiple processing sites. Although risk levels at individual processing sites may vary, the EPR should reflect the aggregate risk posed by the company's activities.

The Agency-In-Charge (AIC) will coordinate the risk ranking of each TSP under its supervision. The ERP ranking form **should not** be modified or edited in any way.

At the conclusion of each examination the AIC is responsible for

- Completing Sections I through V of the EPR for each TSP.
    - *Section III Business Line Risk Ranking*—If a business line is checked in more than one risk ranking category, the AIC should assess **all** of the business lines and risks together before arriving at an overall Business Line Risk Rank.
    - *Section IV Service Provider Risk Category*—If factors are selected from more than one risk-ranking category, the AIC should assess **all** of the risks before arriving at an overall "Service Provider Risk." Rating one risk factor "Higher Risk" **does not** automatically result in the TSP having an overall "Higher Risk" rank.
- Distributing copies of the completed EPR to its counterparts at the other FFIEC agencies.
- Collecting from its counterparts the EPRs indicating agency agreement/disagreement, consolidating the findings under section VI, and resolving any priority disagreements to the extent possible. The AIC should retain all documentation supporting the priority designation and agency agreement/disagreement. The FFIEC IT subcommittee may request submission of the supporting documentation on a random basis or in instances of agency disagreement.
- Documenting the basis for the disagreement in the comment, section VII, for those rare occasions when a resolution cannot be reached.
- Forwarding the completed ERP to the other agencies' representatives.

Agency representatives receiving EPR from the AIC are responsible for

- Reviewing sections I through V;
- Completing sections VI and VII as applicable;
- Returning the completed form to the AIC by the requested response date; and
- Retaining a copy for their records.

APPENDIX C: REPORT OF EXAMINATION

GUIDELINES FOR COMPLETING

Each FFIEC agency may supplement the following guidelines with additional instructions. Examiners must complete all required pages.

SECTIONS OF ROE

The ROE will include a transmittal letter. This letter, sent to the board of directors, includes the rating assigned to the TSP. This is to prevent ratings disclosure to, or discussions with, the serviced financial institutions. The lead agency designee should sign the transmittal letter.

The open section of the report should contain all significant matters. The open section is distributed to examined entities. FFIEC agencies may distribute the open section to serviced financial institutions receiving the services covered by the examination.

Examiners should reflect matters of a proprietary nature in the administrative section of the report. Examples of proprietary information include, but are not limited to, marketing plans, development plans, and certain contract terms. The administrative section is confidential and for regulatory agency use only.

OPEN SECTION—REQUIRED AND OPTIONAL PAGES

COVER PAGE (REQUIRED)

Interagency reports of examination should use the standard interagency cover page. Each agency has the option of using either its own cover page or the standard FFIEC cover page on its institution's examinations.

TABLE OF CONTENTS (OPTIONAL)

The use of this page is at the discretion of the respective FFIEC agencies. If an agency decides to use this section, they should list sections in the order of their appearance in the report.

EXAMINER'S CONCLUSIONS (REQUIRED)

Information should include

- *Scope and Objectives of the Examination*—A description of areas examined and procedures employed.
- *Summary of Major Findings*—A general description of major examination findings. Examiners should present findings in the order of their importance. Examiners

should include references to areas where they identified significant operational and procedural deficiencies or internal control weaknesses. Examiners should refer readers to the specific "Supporting Comments" page(s) for detailed descriptions of these findings and recommendations for corrective action.

The last paragraph under this subheading should include a list of who attended meetings where examination findings were discussed. The list should be limited to those persons with broad responsibility for the major areas examined (i.e., IT audit, IT management, development and acquisition, and support and delivery). Senior management responsible for information systems operations should always be included.

Examiners should direct comments in the summary section to the attention of the board of directors and senior management. Comments should be brief, non-technical, and limited to the most significant issues. Examiners should describe the findings in terms of the risk(s) presented and potential effect on the serviced financial institutions and their customers.

- *Conclusions*—A summary of the overall condition of the information systems examined, including comments on the improvement or deterioration of the operation. Examiners should avoid single-word evaluations, such as "good," "fair," "poor," "strong," or "weak." The summary should include, as appropriate, brief comments about past performance (with emphasis on effecting corrective measures), the seriousness of existing weaknesses, and future prospects for the information system. Information on any corrective action that management agreed to take should be included.
- *Composite Rating*—These remarks should document the performance evaluation of the entity. Following the numerical composite rating, the exact language for that rating, found in Appendix D, should be inserted so board members and management have a clear and common understanding of the examiner's overall conclusions. Supporting comments should precede the composite rating in this section of the report. However, the rating and definition are not included in the open section of the reports on entities servicing other data centers and/or financial institutions.
- *Signatures*—The authoring EIC must sign the report at the bottom of the "Examiner's Conclusions" page. Other signatures required by the authorizing agency should follow and include appropriate titles.

VIOLATIONS OF LAWS AND REGULATIONS (OPTIONAL)

Examiners should complete this page when they discover specific violations of laws or regulations. Examiners should cite the law or regulation violated followed by a brief description of the violation and management's response/corrective measures.

SUPPORTING COMMENTS (REQUIRED)

This ROE section should include comments addressing operating and procedural deficiencies and internal control weaknesses identified during the examination. Detailed comments should support the findings cited in the "Examiner's Conclusions" section. Supporting comments should be categorized within the URSIT component categories in the order of relative importance consistent with the "Examiner's Conclusions" page.

Each URSIT component section (audit, management, development and acquisition, and support and delivery) should start with a summary supporting the rating assigned to that component. Comments should convey a clear assessment of the condition of each function. The actual numerical rating should not be included on the supporting comments pages, but should be included in the confidential section and on the "Examiner's Conclusions" page if appropriate in accordance with the instructions for that page. Items deemed confidential in nature should be included only in the closed section of the report. Ratings justifications contained on the "Supporting Comments" page should not be duplicated in the confidential pages.

Comments for each deficiency should, at a minimum, include

- A detailed description of the deficiency, identifying the risk to the organization and serviced financial institution if not addressed by management;
- Examiner's recommendation to address the deficiency;
- Management's response and corrective action plan; and
- The examiner's analysis of management's response (if necessary).

The description of examination findings must be in terms of the risks they present and their effect on the organization and its financial institution customers.

Examiners should make every effort to obtain management's commitment to a reasonable time frame for implementing corrective measures. Examiners should highlight and reinforce deficiencies noted in consecutive examinations. If a significant number of repeat deficiencies are noted, this information should be reported in the "Examiner's Conclusions" section of the report and should be commented upon in the management section of the report.

Note: The "Supporting Comments" section should only contain substantive items. Examiners should discuss less significant items with management. If appropriate, examiners may list less significant items separately. That list should be provided to management and a copy retained in the work papers for the examination. Management's responses should be noted on the list. If appropriate, the list can be referenced on the "Supporting Comments" pages or in the "Examiner's Conclusions" section.

DIRECTORS' SIGNATURE PAGE (REQUIRED)

This page should be included in all IT ROEs. Once the final ROE is returned to the directors, they should be instructed in the transmittal letter sent by the supervisory agency

to fully review the IT ROE at a following board of directors meeting. Once this review has occurred, the directors must sign and date the "Director's Signature Page" to attest to the fact that each of them has personally reviewed and understands the contents of the IT ROE.

ADMINISTRATIVE SECTION—REQUIRED AND OPTIONAL PAGES

This section should only contain matters that are considered inappropriate for disclosure in the open section of the examination report. In addition, financial data should be included for all TSPs. Basic information about the TSP, the type of examination, and the participating supervisory agencies should also be included in the administrative section. The "Type of Examination-Agency" subsection should indicate whether the examination is joint or rotated and the authoring agency identified by the appropriate abbreviation, (e.g., FDIC, FRB, NCUA, OCC, OTS). For multi-site examinations, examination hours reported in the corporate report should include the total time for all locations examined.

ADMINISTRATIVE REMARKS (REQUIRED)

These remarks should document the performance evaluation of the entity in accordance with the URSIT. For multi-site examinations, all subsidiary data center ratings should be included in this section and summarized. The numeric ratings and accompanying comments should include recommendations for follow-up action and any additional comments.

STATISTICAL DATA (REQUIRED)

This section should contain statistical information necessary to supervise the institution/TSP adequately and process the report. Examiners should request this information at or before the beginning of the examination. Instructions for completing these pages include:

- Applications – Present a list of the major applications processed by the TSP for itself and for serviced financial institutions that are federally insured. Examiners should number the applications sequentially, i.e., 1, 2, 3, 4, under the heading "Code." The sequence number will serve as a key for the "Serviced Financial Institutions" portion. The "Application listing" should include the software package name and the name of the vendor and the vendor's location (city and state). The "Application" portion should indicate the processing mode(s) for each application listed.
    - *Batch updating*—Daily transaction activity accumulates off line. Updating of master files takes place at the end of the processing cycle (usually daily).
    - *Memo post/On-line updating*—Transaction activity is posted to a copy of the master files throughout the day as deemed appropriate by the

institution in order to show updated balances. Actual posting to accounts occurs via batch updating at the end of the processing cycle.

- *Real-time updating*—Transactions are posted to the customer's (master) file as they occur.

Note: If appropriate, indicate the combinations of these processing modes.

- Serviced Financial Institutions—List names and locations of federally insured serviced financial institutions. The list must be grouped by regulatory category first, followed by state:
  - National banks
  - State member banks
  - State nonmember banks
  - Savings associations
  - Credit unions

  Note: This listing can either be included in the IT ROE or in a separate document. Examiners should identify applications processed in the right-hand columns, using the keys assigned in the application section.
- Other Servicing—Reflect the number of nonbank entities which the TSP provides services to and the types of processing performed for these organizations.

SYSTEM AND ORGANIZATION INFORMATION (REQUIRED)

- *System Description*—Provide details of the major hardware, software, and, if applicable, networking configurations used by the facility.
  - Hardware: At a minimum, specify the manufacturer, model numbers, and core storage capacity of the mainframe used. Detail other information as appropriate or as required by the individual agencies.
  - Software: Indicate the primary programming languages used and the major sources of software; e.g., developed in-house, software packages, contract programmers, etc. If purchased/licensed software packages are used, list the vendor(s).
  - Network: Indicate the general configuration of the system, specifying remote entry sites and free standing satellite centers.
- *Organizational Structure*—Provide general staffing and examination contact information. The total number of employees may not necessarily be the sum of the numbers appearing in the spaces for development and acquisition and support and delivery personnel. Also, list principal officers and managers responsible for the center's operation by name, title, telephone number, and e-mail address. If the organization is a financial institution, provide total asset and deposit figures. If the organization is not a financial institution, the ownership portion of this section should reflect the name and type of the organization (if the owner is not a person). Types of organi-

zations might include financial institution (bank, savings and loan, or credit union), financial institution or holding company subsidiary, bank service corporation, private corporation, joint venture, facilities management (specify contracting financial institution), partnership, etc.

FINANCIAL DATA (REQUIRED FOR ALL TECHNOLOGY SERVICE PROVIDERS)

Examiners should complete this page for all TSPs that are not financial institutions. At a minimum, examiners should include data for the last three fiscal years.

Examiners should request and analyze audited financial statements. If they are not available, unaudited statements will be acceptable. Examiners should clearly note if the statements analyzed are audited or unaudited. Examiners should reflect any interim financial statements they obtain on a separate page, footnoted to indicate that they are interim statements, and inserted behind the year-end statements. Examiners should note in their analysis any regulatory information (i.e., shared national credit rating) or industry information (i.e., Standard & Poor's, Moody's, or Moody's KMV) that is available.

Examiners should summarize any significant financial statement footnotes on a blank insert page at the end of the financial data.

If the servicer is part of a regulated financial organization, the examiner should use existing regulatory financial and analytical information (CAMELS rating, BOPEC rating, etc.) in the review and analysis of the parent company.

Examiners should request and analyze consolidated and company financial statements of TSPs that are a subsidiary of a nonbank holding company or other nonfinancial corporation. Consolidated statements should be detailed on separate pages, footnoted to indicate they are consolidated statements, and inserted after the company year-end and interim statement.

ADDITIONAL INFORMATION (OPTIONAL)

Examiners may use this page to address specific requirements of the various regulatory agencies. Information included would be items such as the location of work papers.

Federal
Financial
Institutions
Examination
Council

Information Technology Examination

of MDPS (Multi-regional Data Processing Servicer)
or TSP (Technology Service Provider)
or Financial Institution

(SERVICER NAME)
(CITY, STATE)
As of (Date of Exam)

THIS REPORT OF EXAMINATION IS STRICTLY CONFIDENTIAL

This copy of the examination report is the joint property of the FFIEC Member Agencies, and it is furnished for the confidential use of the examined entity. The information contained in this document is based upon the records and books of the entity, upon statements made by directors, officers, and employees, and upon information obtained from other sources believed to be reliable and correct.

This examination is not an audit and should not be construed as such. It is emphasized that this examination does not replace, nor relieve the management of its responsibility for making or providing for adequate audits of the examined entity.

Under no circumstances shall any recipient of this report, or any of its directors, officers, employees, outside auditor or legal counsel disclose or make public this report or any portion thereof. Unauthorized disclosure of any of the contents of this report is subject to the penalties in 18 U.S.C. 641. The agency that transmitted this report must be notified immediately if the examined entity receives a subpoena or other legal process calling for the production of this report.

FFIEC
Information Technology
Report of Examination

Data Center: [Name of MDPS/TSP/Financial Institution]

City: _____ **County:** _____ **State:** _____ **Zip:** _____

Date of examination:

_____

Participating Agencies

Agency	Region/District	Number

EIC: _____ **Examiner:** _____

Examiner: _____ **Examiner:** _____

Examiner: _____ **Examiner:** _____

Examiner: _____ **Examiner:** _____

Examiner: _____ **Examiner:** _____

ID No_____

ID/Charter No.

TABLE OF CONTENTS

Examiner's Conclusions…….……C-10

Violations of Law and Regulations ……...C-12

Supporting Comments…….……...C-12

Directors' Signature Page…….…….C-13

ID/Charter No.

EXAMINER'S CONCLUSIONS

Start text here ...

ID/Charter No.

VIOLATIONS of LAW and REGULATIONS

Start text here ...

ID/Charter No.

SUPPORTING COMMENTS

Start text here ...

ID/Charter No.

DIRECTORS' SIGNATURE PAGE

We, the undersigned directors of the [Name of MDPS/TSP/Financial Institution], [City], [State and ZIP], have personally reviewed the contents of the report of examination dated [Date of Exam].

NAMES	SIGNATURES	DATES
Type first name here		
Second name here		
Third name here		

NOTE: This form should remain attached to the report of examination and be retained in the institution's file for review during subsequent examinations. The signature of committee members will suffice only if the committee includes outside directors and a resolution has been passed by the full board delegating the review to such committee.

Administrative Section

Region/District
[District/Region]
ID/Charter Number
[######]

Name & Location of MDPS/TSP/Financial Institution

[Name of MDPS/TSP/Financial Institution]

[Street]

[City], [State and ZIP]

Examination Opened	Examination Closed	Type of Examination-Agency
[Date of Exam]	[Close Date of Exam]	[Exam Type]

Prior Exams					
Date:	**Rating:**	**Agency:**	**Date:**	**Rating:**	**Agency:**

	Working Hours	
	In House	**Outside**
[Name of EIC], Examiner-in-Charge Examiner 2 Examiner 3 Examiner 4		
TOTAL	0	0

GRAND TOTAL (Less Training)

ID/Charter No.

Administrative Section

Applications

Code	Application	Batch	On-line	Real Time
1	Demand Deposits	X, M	I	F
2	Savings Accounts	X, M	I	F
3	Loans	X	I	F
4	General Ledger		I	X

X = All Processing
I = Inquiry Only
M = Memo Post
F = File Maintenance

Serviced Financial Institutions

Name & Location [10]Application (By Code)

National Banks

First National Bank of Anytown
Anytown, Illinois — 1,2,3,4,5,6,7,8,9,10,11,12,13,14

State Member Banks

Anytown State Bank
Anytown, Illinois — 1,2,3,4,5,6,7,8,9,10,11,12,13,14

State Non-Member Banks

The State Bank
Anytown, Illinois — 1,2,3,4,5,6,7,8,9,10,11,12,13,14

Savings Associations

Anytown Savings Bank
Anytown, Illinois — 1,2,3,4,5,6,7,8,9,10,11,12,13,14

Credit Unions

Anytown Credit Union
Anytown, Illinois — 1,2,3,4,5,6,7,8,9,10,11,12,13,14

[10] The EIC is responsible for ensuring this information is in the above format.

ID/Charter No.

Administrative Section

RECAP:

Totals for all Institution Types:

Total National Banks:
Total State Member Banks:
Total State Non-Member Banks:
Total Thrifts:
Total Credit Unions:

Total All Institutions:

OTHER SERVICING:

# of Customers:

Applications Processed:

ID/Charter No.

Administrative Section

System Description
(Mission Critical Systems Only)

Hardware:
Operating System:

Software:

Networks:

Organizational Structure

Staff Size: S&D _____ D&A _____ Total 0

Examination Contact:

Officers/Managers:

If financial institution, give total assets: _____ Total deposits: _____

Ownership:

Directors:

ID/Charter No.

Financial Information

Part 5 - Condensed Balance Sheet and Income Statement for Nonfinancial Institution Servicer

	CONDENSED BALANCE SHEET As of December 31			
	200X	200X	19XX	19XX
ASSETS				
Cash				
Accounts Receivable				
Prepaid Expenses				
Other Current Assets				
CURRENT ASSETS	0	0	0	0
Real Estate				
Furniture & Fixtures				
Software				
Software Amortization				
Hardware				
Hardware Depreciation				
Other Assets				
Goodwill & Other Intangible Assets				
TOTAL ASSETS	0	0	0	0
LIABILITIES AND CAPITAL				
Notes Payable Banks				
Notes Payable Others				
Accounts Payable				
Accrued Expenses				
Taxes				
Other Current Liabilities				
CURRENT LIABILITIES	0	0	0	0
Term Debt				
Other Debt				
Subordinated Debt				
Long Term Capital Leases				
TOTAL LIABILITIES	0	0	0	0
EQUITY CAPITAL				
TOTAL LIABILITIES & EQUITY	0	0	0	0

ID/Charter No.

Financial Information

CONDENSED INCOME STATEMENT As of December 31

	200X	200X	199X	199X
OPERATING INCOME				
Data Processing Servicing Income				
Other Income				
TOTAL OPERATING INCOME	0	0	0	0
OPERATING EXPENSES				
Mainframe Hardware and Software				
Lease and Rental				
Depreciation				
Repairs and Maintenance				
Contract Programming				
License Fees and Amortization				
Other				
Other Operating Expenses				
Compensation				
Data Communication				
Occupancy Expense				
Benefits and Travel				
Public Relations & Advertising				
Other Operating Expenses				
TOTAL OPERATING EXPENSES	0	0	0	0
NON-OPERATING				
Non-operating Income				
Interest Income				
Other Non-operating Income				
Non-operating Expenses				
Interest Expense				
Other Non-operating Expenses				
NET NON-OPERATING INCOME	0	0	0	0
INCOME BEFORE TAXES	0	0	0	0
Income Tax				
NI BEFORE EXTRAORDINARY ITEMS	0	0	0	0
Extraordinary Losses				
Extraordinary Gains				
NET INCOME	0	0	0	0

ID/Charter No.

Financial Information

Statement of Cashflow				
	200X	**200X**	**199X**	**199X**
Cash provided by operations				
Net Income				
Adjustments not requiring outlay of cash				
Cumulative effect of accounting changes				
Depreciation and amortization of property, plant and equipment				
Amortization of goodwill and other intangibles				
Deferred income taxes				
Changes in working capital and other accounts				
Account receivables				
Inventory				
Account payables				
Other				
Net cash provided from operating activities				
Cash flows from Investing Activities				
Capital expenditures				
Disposition of property, plant and equipment				
All other investing activities				
Cash flow from financing activities				
Proceeds from borrowings				
Retirement of debt				
All other financing activities				
Net cash provided from financing activities				
Increase (decrease) in cash and equivalents during year				
Cash and equivalents at beginning of year				
Cash and equivalents at end of Year 2000				

ID/Charter No.

Financial Information

SUMMARY OF KEY OPERATING RATIOS	200X	200X	200X	1999
Asset Growth				
Liability Growth				
Capital/Total Assets				
Return on Assets				
Return on Equity				
Net Operating Income/Gross Operating Income				
Current Assets/Assets				
Total Liabilities/Equity Capital				
Current Assets/Current Liabilities				
Debt/Tangible Net Worth				

Operating Ratio Definitions

1. ***Asset Growth -*** (Current Total Assets - Prior Period Total Assets)/Prior Period Total Assets. A significant increase or decrease in total assets may be an indication of problems and should be investigated and explained.
2. ***Liability Growth -*** (Current Total Liabilities - Prior Period Total Liabilities)/Prior Period Total Liabilities. A significant increase in Total Liabilities is a potential indication of cash flow problems and should be investigated and explained.
3. ***Capital/Total Assets -*** Equity Capital/Total Assets. This ratio provides an indication of the amount of losses that can be absorbed before insolvency.
4. ***Return on Assets -*** Current Period Net Income/((Current Period Total Assets + Prior Period Total Assets)/2). Return on Assets is an indication of how efficiently the assets are used. Ratio should be annualized if less than 12 months used.
5. ***Return on Equity -*** Current Period Net Income/((Current Period Equity + Prior Period Equity)/2). An indication of the return on the capital invested. Ratio should be annualized if less than 12 months used.
6. ***Net Operating Income/Gross Operating Income -*** An indication of the efficiency of the operation.
7. **Current Assets/Assets -** An indication of liquidity.
8. ***Total Liabilities/Equity Capital -*** An indication of company's leverage position.
9. ***Current Assets/Current Liabilities -*** An indication of liquidity.
10. ***Debt/Tangible Net Worth –*** Total Liabilities/(Equity Capital – Goodwill & Other Intangible Assets). This ratio provides an indication of the company's leverage position.

Consistent with the risk-based examination strategy, the EIC should include a narrative analysis of the entity's financial condition. This analysis should include the EIC's conclusions regarding the financial condition and stability of the TSP.

ID/Charter No.

Administrative Section

SUBSEQUENT EXAMINATION STRATEGY

Include the examination priority ranking and support.

EXAMINATION REQUEST LETTER

Send to:
[Name of MDPS/TSP/Financial Institution]
[Street]
[City], [State and ZIP]

REPORT DISTRIBUTION

Data Center Copy:	[Name of MDPS/TSP/Financial Institution] (Do not include the confidential section).
File Copy:	*File Copy Location*
Washington Copy:	*Washington Copy Location*
FDIC:	*Regional Office*
FRB	*Federal Reserve Bank*
OCC:	*Washington Office*
OTS:	*Regional Office*
Field Office:	O*rganization*

WORK PAPER INFORMATION

Detail where the work papers are located. Are they hard copy or electronic? Who should the next examiner contact to gain access to these work papers?

APPENDIX D: UNIFORM RATING SYSTEM FOR INFORMATION TECHNOLOGY

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 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 exhibit 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 formulated 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 board's and management's ability 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 de-

cisions 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 which 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; and
- 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.