

## **Examination Report Guidelines for Inspection of Payment System and Technology Service Providers (PSSP/TSP)**

### **Purpose**

This document provides guidelines for the inspection of Payment System Service Providers and Technology Service Providers (PSSP/TSP). It documents the entire inspection process from pre inspection planning to the final recommendations and where appropriate, the tracking on sanctions and enforcement actions. Specific formats are provided that must be followed and completed. The goals of the inspection process are as follows:

- Identify existing or potential risks associated with the PSSP/TSP that could adversely affect serviced financial institutions;
- Evaluate the overall integrity and effectiveness of the PSSP/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 PSSP/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 PSSP/TSP's products, services, or risk management practices that would adversely affect its risk profile or those of its client financial institutions. Identify existing or potential risks associated with the TSP that could adversely affect serviced financial institutions;
- Evaluate the overall integrity and effectiveness of the PSSP/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 PSSP/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 PSSP/TSP's products, services, or risk management practices that would adversely affect its risk profile or those of its client financial institutions.

## **Risk-Based Supervision**

The CBE should base their examination process on the concept of on-going, risk-based supervision. Risk-based supervision of PSSP/TSPs is designed to:

- Identify existing or potential risks associated with the PSSP/TSP that could adversely affect serviced financial institutions;
- Evaluate the overall integrity and effectiveness of the PSSP/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 PSSP/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 PSSP/TSP's products, services, or risk management practices that would adversely affect its risk profile or those of its client financial institutions.

The CBE's risk-based supervision consists of the identification and selection of PSSP/TSPs warranting examination, 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 PSSP/TSPs including electronic funds transfer switches, Internet banking providers, item processors, etc. Examinations will be required for all licensed PSSP/TSPs in Egypt.

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

The focal points for the assessment of risk for the PSSP/TSP's are as follows;

- *Management of Technology* — The planning and overseeing of technological resources and services ensuring they support the strategic goals and objectives of the PSSP/TSP and financial institution participant.
- *Integrity of Data and Security* — 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 and availability of liquidity due to older technology assets or the potential for cash shortages during times

requiring rapid growth. Financial difficulties at the PSSP/TSP can negatively affect the serviced financial institution by lowering the 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 the PSSP/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. These other PSSP/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 PSSP/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 PSSP/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, PSSP/TSP's 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 PSSP/TSP at each examination. Their assessments of a PSSP/TSP's degree and quality of risk management should be discussed with PSSP/TSP management and factored into the PSSP/TSP's supervision strategy. Examiners should also explain how the PSSP/TSP's deficiencies increase the risk to the serviced institutions. For example, inadequate business resumption plans at the PSSP/TSP may increase the transaction and reputation risks at serviced institutions.

The quantity of transaction/operational risk at a PSSP/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 PSSP/TSP
- Number of client institutions serviced

- Volume (both value and quantity) of transactions processed for serviced financial institutions
- Aggregate size (both 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 PSSP/TSP's policies;
- The adequacy of the PSSP/TSP's control and operational processes;
- The extent of the PSSP/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 CBE should use the Uniform Rating System for Information Technology (URSIT) developed in the United States to assess and rate risks within the PSSP/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 PSSP/TSP'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 Banking Supervision and Payment System Departments should employ this rating methodology for both Banks and PSSP/TSP's. This will ensure consistency and a common base line for measurement of risk in payment systems.

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 shall 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 CBE recognizes that management practices, particularly as they relate to risk management, vary considerably among financial institutions, PSSP's and TSP's, depending on their size and sophistication, the nature and complexity of their business activities, and their risk profile.

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

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

PSSP/TSP's, 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 CBE should 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. PSSP/TSP's with an effective risk-based auditing program typically require less examination work by regulatory agencies.

## **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:

1. Statutory and policy-based examination requirements

2. 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.

The supervisory strategy for each inspection should be documented and approved by CBE management prior to the actual inspection. The goal is to ensure that inspection resources have properly prepared and that the inspection plan addresses issues specific to this PSSP/TSP. This will increase the efficiency of the examination process and yield results that address vendor specific issues.

The EIC should base supervisory objectives for a PSSP/TSP examination on the PSSP/TSP's risk profile and appropriate statutory 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 and resources. 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 PSSP/TSP (e.g., reports of examination, meeting with the board of directors).

### **Examination Responsibilities**

The EIC is responsible for the administration and overall performance of the examination. These responsibilities include:

- 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 CBE departments;
- Communicating examination plans with the PSSP/TSP to coordinate onsite 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.

### **Examination Planning**

Examination planning is essential to effective supervision. 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 examination team leader must gather, organize, and analyze available information prior to beginning an on-site examination. The extent of advance preparation depends on the complexity of the PSSP/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 PSSP/TSP's Web site.

### **CBE Information Request and Initial Meeting with the PSSP/TSP**

The examination team leader should schedule an entrance meeting with the key PSSP/TSP staff members to introduce the examination team and to identify primary points of contact for specific areas of review. Prior to that, the team should make a request for information from the PSSP/TSP at least four weeks in advance of the meeting. The request should include the following:

- Changes in management or structure since last examination;
- Current financial statements (formats will be addressed later in this document);
- Actions taken since the last examination in conformance with previous examination team recommendations;
- Significant changes in operations, strategy or products offered;
- Details on any system changes since the last examination (hardware, software, operating system changes, upgrades, new application software, etc.);
- Updated list of system participants;
- Any economic conditions or competitive issues that may be affecting the PSSP/TSP business or operations;

- Audit results (either internal or external) that may have taken place since the last examination;
- Any specific issues that the PSSP/TSP would like to address with the examination team.

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 PSSP/TSP and its customers.

The examination team should also plan to meet frequently with PSSP/TSP management to inform them of the progress of the review.

### **Examination Scope**

The examination team leader should determine the scope of examination work and estimate the workdays required for completion. The scope should cover the headquarters location and data center at a minimum. The team leader 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 should outline the objectives of the examination, assignments, work plan and other relevant information.

### **Pre-examination Approval**

A pre-examination review is to be conducted by the examination team leader to determine the scope of the overall examination, identify resource requirements, schedule events, and determine which data centers, based on their level of risk, will be examined. Based on this review, the examination team leader 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 must be presented to and approved by the Payment System Department Director prior to the start of the examination process.

### **Report Preparation**

The examination team leader is responsible for preparing the examination report. The report should give an overall view of the organization and include an evaluation of each data center

examined. The report should contain an assessment of the major risks to the financial institutions serviced by the PSSP/TSP organization, recommendations for reducing or managing those risks, and management's responses to the findings and recommendations. The examination report should be prepared following the guidelines in this handbook.

## **Rating**

Each on-site examination will include one set of component ratings and one composite rating, based upon the overall condition of its entire operation. The ratings will follow URSIT (see Appendix D). The ratings are disclosed separately to the PSSP/TSP and are not included in the report provided to the serviced financial institutions.

## **Examination Report Content**

### Examiner's Conclusions

1. Scope and Objectives of the Examination — A description of areas examined and procedures employed.
2. Summary of Major Findings — A general description of major examination findings.
  - a. Examiners should present findings in the order of their importance.
  - b. Examiners should include references to areas where they identified significant operational and procedural deficiencies or internal control weaknesses.
  - c. Examiners should refer readers to the specific "Supporting Comments" page(s) for detailed descriptions of these findings and recommendations for corrective action.
  - d. 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.
  - e. Examiners should describe the findings in terms of the risk(s) presented and potential effect on the serviced financial institutions and their customers.
3. 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.
4. 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.
5. 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.

6. Signatures — The authoring examination team leader 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.

### **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 PSSP/TSP’s or TSP’s that were rated a three or below. Examiners have the discretion to schedule board meetings for TSPs rated one or two when justified by the issues or other factors.

## **Appendix A: Examination Planning**

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

1. Organize appropriate 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 PSSP/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 who provides IT servicing to the PSSP/TSP, if applicable.
5. Initiate the process for obtaining data on serviced customers. A letter from the CBE requesting feedback on the quality of service and any outstanding issues that may exist with the PSSP/TSP.
6. Begin the process for obtaining data on serviced customers. This must include institution name, type of institution and location.

## Appendix B: Examination Procedures

### *Assessment of Changes and Identification of Potential Risks*

1. Review information gathered from the pre-examination request with senior PSSP/TSP management. This should include the following information:
  - a. Changes in management or structure since last examination;
  - b. Current financial statements (formats will be addressed later in this document in Appendix C);
  - c. Actions taken since the last examination in conformance with previous examination team recommendations;
  - d. Significant changes in operations, strategy or products offered;
  - e. Details on any system changes since the last examination (hardware, software, operating system changes, upgrades, new application software, etc.);
  - f. Updated list of system participants;
  - g. Any economic conditions or competitive issues that may be affecting the PSSP/TSP business or operations;
  - h. Previous examination reports, or if not applicable, the results from the assessment of the licensing application and results of any audits (either internal or external) that may have taken place since the last examination.
2. Interview management and review examination information to identify changes to the technology infrastructure or new products and services that might increase the institution's risk from information security issues. Consider:
  - a. Products or services delivered to either internal or external users
  - b. Network topology including changes to configuration or components
  - c. Hardware and software listings
  - d. Loss or addition of key personnel
  - e. Technology service providers and software vendor listings
  - f. Changes to internal business processes
  - g. Key management changes
  - h. Internal reorganizations
3. Review the financial institution's response to issues raised at the last examination. Consider:
  - a. Adequacy and timing of corrective action.
  - b. Resolution of root causes rather than specific issues.
4. Existence of outstanding issues. Determine the extent to which this requires a change in inspection scope or process.
5. Review and discuss with the PSSP/TSP results of the feedback from participants surveyed and any additional correspondence received regarding this specific PSSP/TSP.

6. Review the inventory of systems, applications and products offered by the PSSP/TSP. Note any changes that may have occurred since the initial licensing review or the last inspection, whichever is most appropriate.
7. Identify the systems that have recently undergone significant change, such as new hardware, software, configurations, and connectivity. Correlate the changed systems with the business processes they support, the extent of customer data available to those processes, and the role of those processes in funds transfers.
8. Document any changes in the list of participants from either the initial licensing review or the last inspection, whichever is appropriate.
9. Identify and obtain through discussions with PSSP/TSP management:
  - a. A description of the retail payment system activity performed, including transaction volumes, Egyptian Pound amounts and scope of operations including check item processing, ACH, bankcard issuing and acquiring, clearance, settlement, and ATM and EFT/POS terminal and network activity as appropriate.
  - b. The payment system functions performed through outsourcing relationships with other service providers.
  - c. Any significant changes in payment system policies, personnel, products, and services since the last examination, particularly the introduction of new payment systems.
  - d. A listing of all clearinghouse settlement arrangements in which the PSSP/TSP participates.

### *Management*

10. The performance of management has a significant impact on the quality of risk management. As such, the following assessments should be performed regarding management capacity, degree of oversight and knowledge and ability to address issues. The following assessments should be performed reflecting the strength of the management team.
  - a. The level and quality of oversight and support of the IT activities by the board of directors and management;
  - b. 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;
  - c. The ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner;
  - d. The adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
  - e. The effectiveness of risk monitoring systems;

- f. The timeliness of corrective action for reported and known problems;
  - g. The level of awareness of and compliance with laws and regulations;
  - h. The level of planning for management succession;
  - i. 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;
  - j. The adequacy of contracts and management's ability to monitor relationships with third-party servicers;
  - k. 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
  - l. The ability of management to identify, measure, monitor, and control risks and to address emerging information technology needs and solutions.
  - m. The financial condition and ongoing viability of the entity;
  - n. 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.
11. Assess management's ability to manage relationships with participant institutions, other PSSP/TSP's and suppliers (hardware, network and software vendors) to evaluate the adequacy of support the PSSP/TSP is able to offer its system participants. The assessment should consider the following:
- a. Adequacy of contract provisions including service levels, performance agreements, responsibilities, liabilities, and management monitoring.
  - b. Management's compliance with applicable financial institution, consumer regulations and other third-party requirements. (e.g. bankcard association, interchanges, etc.).
  - c. Provisioning for personnel, equipment, and related services.
  - d. Ability to generate management information systems (MIS) needed to support performance defined in the service level agreements with participant institutions.
  - e. Evaluate management's ability to control security risks within the computing environment.
  - f. Adherence to bankcard association rules and bylaws and regulatory guidance.
12. Determine the quality of oversight and support provided by the board of directors and management regarding the operational aspects of the organization. Determine the quality and effectiveness of the PSSP/TSP's management of the following:
- a. Data center and network management and the quality of internal controls over ATM, EFT/POS and bankcard networks.
  - b. Departmental management and the quality of internal controls for procedures related to bankcards, ATM and debit card, ACH, check items, and electronic banking payment transaction processing, clearance, and settlement activity.
13. Review the participant rules and assess management commitment to compliance through;

- a. Review of participant agreements looking for instances of non compliance on the part of either the participant or the PSSP/TSP,
  - b. Review PSSP/TSP management actions taken to resolve situations where non compliance occurred.
14. Review management actions resulting from either internal or external audits and understand the level of independence observed in the case of an internal audit.
15. Observe and comment on management’s assessment of financials (Schedule C) and assess any trends that appear to demonstrate a negative direction or company weakness.

### *Management of Technology*

16. Evaluate the effectiveness of PSSP/TSP staff. Considering:
- a. Adequacy and quality of staff resources.
  - b. Effectiveness of policies and procedures outlining department duties including job descriptions.
17. Identify whether the institution effectively documents changes and updates the risk assessment prior to making system changes, implementing new products or services, or confronting new external conditions that would affect the risk analysis. Identify whether, in the absence of the above factors, the risk assessment is reviewed at least once a year.
18. Identify what procedures are in place for the documentation of system configurations and software including operating system and layered products and application level software. Also review procedures for documentation of software versions, change control, testing of application software and related tasks.
19. Evaluate and assess the processes and procedures associated with the operation of systems within the PSSP/TSP. Considerations should include:
- a. Depth of experience of personnel and level of back-up for key personnel.
  - b. Evaluate documented procedures and adherence to same.
  - c. Evaluate testing procedures related to the release of a new system or new version of an application, operating system, etc.

### *Integrity of Data and Security*

20. Identify whether external standards are used as a basis for the security program, and the extent to which management tailors the standards to the PSSP/TSP’s specific circumstances.
21. Determine the extent of network connectivity internally and externally, and the boundaries and functions of security domains.

22. Determine what assurances are given in the agreement between the PSSP/TSP and the participant regarding the confidentiality of participant data. Confidentiality should be clearly stated.
23. Review PSSP/TSP security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution.
  - a. Authentication and Authorization
    - i. Acceptable-use policy that dictates the appropriate use of the PSSP/TSP's technology including hardware, software, networks, and telecommunications.
    - ii. Administration of access rights at the time of initial enrollment, when duties change, and upon employee separation.
    - iii. Appropriate authentication mechanisms including token-based systems, digital certificates, or biometric controls and related enrollment and maintenance processes as well as database security.
    - iv. Appropriate authentication mechanisms for participants that ensure high access security, for example, use of passwords and frequency of change.
    - v. Evaluate system administration abilities of the PSSP/TSP as regards authorization, authentication and password control.
    - vi. Evaluate the processes that management uses to define access rights and privileges (e.g., software and/or hardware systems access) and determine if access is based upon business requirements.
    - vii. Ensure that access to operating systems is based on either a need-to-use or an event-by-event basis.
    - viii. Obtain an understanding of the PSSP/TSP's monitoring plans and activities, including both activity monitoring and condition monitoring.
  - b. Network Access
    - i. Security domains
    - ii. Perimeter protections including firewalls, malicious code prevention, outbound filtering, and security monitoring.
    - iii. Appropriate application access controls
    - iv. Remote access controls including wireless, VPN, modems, and Internet-based
  - c. Host Systems
    - i. Secure configuration (hardening)
    - ii. Operating system access
    - iii. Application access and configuration
    - iv. Malicious code prevention
    - v. Logging
    - vi. Monitoring and updating
  - d. User Equipment
    - i. Secure configuration (hardening)

- ii. Operating system access
  - iii. Application access and configuration
  - iv. Malicious code prevention
  - v. Logging
  - vi. Monitoring and updating
- e. Physical controls over access to hardware, software, storage media, paper records, and facilities
  - f. Encryption controls
  - g. Malicious code prevention
  - h. Software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management.
  - i. Personnel security
  - j. Media handling procedures and restrictions, including procedures for securing, transmitting and disposing of paper and electronic information
  - k. Service provider oversight
  - l. Business continuity
  - m. Insurance

#### *Audit*

24. The audit function (be it internal or external) should be based upon the assessment of the following factors:
- a. The level of independence maintained by audit and the quality of the oversight and support provided by the board of directors and management;
  - b. The adequacy of the auditor's risk analysis methodology;
  - c. The scope, frequency, accuracy, and timeliness of internal and/or external audit reports;
  - d. The extent of audit participation in application development, acquisition, and testing, to ensure the effectiveness of internal controls and audit trails;
  - e. The adequacy of the overall audit plan in providing appropriate coverage of IT risks;
  - f. The auditor's adherence to codes of ethics and professional audit standards;
  - g. The qualifications of the auditor, staff succession, and continued development through training;
  - h. The existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses; and
  - i. The quality and effectiveness of internal and external audit activity as it relates to IT controls.

#### *IT Support and Delivery*

25. Assessment of the IT organization to support and deliver should be based on the following reviews and assessments:
- a. The ability to provide a level of service that meets the requirements of the business;
  - b. The adequacy of security policies, procedures, and practices in all units and at all levels of the PSSP/TSP;
  - c. The adequacy of data controls over preparation, input, processing, and output;
  - d. The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers and business units;
  - e. The quality of processes or programs that monitor capacity and performance;
  - f. The quality of assistance provided to users and system participants, including the ability to handle problems;
  - g. The adequacy of operating policies, procedures, and manuals;
  - h. The quality of physical and logical security, including the privacy of data; and
  - i. The adequacy of firewall architectures and the security of connections with public networks.
  - j. In addition to the above, factors such as the following are included in the assessment of support and delivery at service providers:
  - k. The adequacy of customer service provided to clients; and
  - l. The ability of the entity to provide and maintain service level performance that meets the requirements of the client.

#### *Availability of Services*

26. Evaluate the adequacy and effectiveness of the service provider contingency and business continuity planning. Review the measures taken to safeguard technical operations and performance including,
- Ability to recover transaction data and supporting books and records based on retail payment system business line requirements and time lines.
  - Level of testing conducted to ensure system and application integrity for new applications and changes to existing applications.
  - Disaster recovery and redundancy of networks and systems that support core PSSP/TSP product offerings. This should include the schedule of testing for the back-up systems in the secondary site.
  - Business continuity plan to be affected in the event of failure of the back-up systems located at the secondary site. This should also include a review of the dates the process was actually tested.
  - Uptime reports for networks and terminals operated such as ATM's, POS and EFTPOS. These uptime reports must include monthly percentages of uptime. These should be reviewed and compared with the service level agreements agreed upon with the PSSP/TSP clients.

**Appendix C: Report of Examination**

**Central Bank of Egypt  
Information Technology  
Report of Examination**

**Data Center:** (Name of PSSP/TSP)

---

**Full Address:**

---

**Date of Examination:**

---

**Examiner in Charge (EIC) and Department Name:**

---

**Examiner Name and Department Name:**

---

**Table of Contents**

**\*Examiner’s Conclusions.....X**

**\*Violations of Law and Regulations .....X**

**\*Supporting Comments.....X**

**\*Composite Rating (URSIT).....X**

**Directors’ Signature Page.....X**

**Administrative.....X**

**Financial Information.....X**

\*There is no set format for each of these pages. The goal is for the EIC to review the basis for their assessment with supporting information in each of the topical areas.

**Director’s Signature Page**

We, the undersigned directors of the (Name of Payment System Service Provider), (Address), have personally reviewed the contents of the report of examination dated (Date of Exam).

<b>Name of Director</b>	<b>Signature</b>	<b>Date</b>
_____	_____	_____
_____	_____	_____
_____	_____	_____

**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**

**Payment System Service Provider/Technology Service Provider**

(Name)

---

(Address)

---

**Examination Open/Close/Type**

<b>Opening of Examination</b>	<b>Close of Examination</b>	<b>Type of Examination</b>
(Date of Exam)	(Close Date of Exam)	(Exam Type)

**Examination History**

<b>Prior Exam 1</b>	<b>Prior Exam 2</b>	<b>Prior Exam 3</b>	<b>Prior Exam 4</b>
Date:	Date:	Date:	Date:
Rating:	Rating:	Rating:	Rating:
Name of EIC:	Name of EIC:	Name of EIC:	Name of EIC:

**Work Associated with Examination**

<b>Working Hours</b>	<b>In House</b>	<b>Outside</b>	<b>Total</b>
Name of Examiner in Charge (EIC)			
Examiner 2			
Examiner 3			
Examiner 4			
<b>Grand Total</b>			

**Type of Processing and Associated Risk Assessment**

<b>Higher Risk</b>	<b>Average Risk</b>
Asset Management Processing	ACH Processing
Clearing and Settlement	Aggregation and Other Emerging Technologies
Core Bank Processing	ATM/POS Processing and Switching
Disaster Recovery Services	Asset Liability Management
Wholesale Payments	Credit Card Merchant Processing
<b>Lower Risk</b>	Credit card Network/Switching
Bill Payment Services	Credit Scoring
Check Processing	Employee Benefit Account Processing
Credit Card Issuance	Loan and Mortgage Processing
Imagin and Electronic Safekeeping	Investment Processing
Web Hosting (informational)	Retail Electronic Banking/Transactional Web Hosting

**Administrative Section**

**Applications**

<b>Code</b>	<b>Application</b>	<b>Batch</b>	<b>On-line</b>	<b>Real Time</b>
1	Debit Transfers	X	I	F
2				
3				
4				

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

**Serviced Financial Institutions**

---

Name and Location	Applications under Review (*using predefined code)
-------------------	---

---

**Institutions should be listed by classification:**

Financial Institutions

- Government Banks
- Foreign Banks
- Private Banks

Technology Service Providers

- Payment System service Providers
- Internet Banking Service Providers
- Core Banking Service Providers
- Application Specific Application Providers

\*a coding system needs to be set up by the CBE to define the specific applications based on the experience and need.

**Administrative Section**

**System Description  
(Mission Critical Systems Only)**

Hardware:

Operating System:

Software:

Networks:

**Organizational Structure**

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

Examination Contact:

Officers/Managers:

If financial institution, give total assets:

Total deposits:

Ownership:

Directors:

## Financial Disclosure and Analysis

### Condensed Balance Sheet (As of 31 December)

	200X	200X	200X	200X
<b>ASSETS</b>				
Cash				
Accounts Receivable				
Prepaid Expenses				
Other Current Assets				
<b>CURRENT ASSETS</b>	0	0	0	0
Real Estate				
Furniture & Fixtures				
Software				
Software Amortization				
Hardware				
Hardware Depreciation				
Other Assets				
Goodwill & Other Intangible Assets				
<b>TOTAL ASSETS</b>	0	0	0	0
<b>LIABILITIES AND CAPITAL</b>				
Notes Payable Banks				
Notes Payable Others				
Accounts Payable				
Accrued Expenses				
Taxes				
Other Current Liabilities				
<b>CURRENT LIABILITIES</b>	0	0	0	0
Term Debt				
Other Debt				
Subordinated Debt				
Long Term Capital Leases				
<b>TOTAL LIABILITIES</b>	0	0	0	0
<b>EQUITY CAPITAL</b>				
<b>TOTAL LIABILITIES &amp; EQUITY</b>	0	0	0	0

**Condensed Income Statement (As of 31 December)**

	200X	200X	200X	2000X
<b>OPERATING INCOME</b>				
Data Processing Servicing Income				
Other Income				
<b>TOTAL OPERATING INCOME</b>	0	0	0	0
<b>OPERATING EXPENSES</b>				
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				
<b>TOTAL OPERATING EXPENSES</b>	0	0	0	0
<b>NON-OPERATING</b>				
Non-operating Income				
Interest Income				
Other Non-operating Income				
Non-operating Expenses				
Interest Expense				
Other Non-operating Expenses				
<b>NET NON-OPERATING INCOME</b>	0	0	0	0
<b>INCOME BEFORE TAXES</b>	0	0	0	0
Income Tax				
<b>NI BEFORE EXTRAORDINARY ITEMS</b>	0	0	0	0
Extraordinary Losses				
Extraordinary Gains				
<b>NET INCOME</b>	0	0	0	0

### Cashflow Statement

Statement of Cashflow				
	200X	200X	200X	200X
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				
<b>Cash flows from Investing Activities</b>				
Capital expenditures				
Disposition of property, plant and equipment				
All other investing activities				
<b>Cash flow from financing activities</b>				
Proceeds from borrowings				
Retirement of debt				
All other financing activities				
Net cash provided from financing activities				
<b>Increase (decrease) in cash and equivalents during year</b>				
<b>Cash and equivalents at beginning of year</b>				
<b>Cash and equivalents at end of Year 200X</b>				

### Summary of Key Operating Ratios

Ratios	200X	200X	200X	200X
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** -  $(\text{Current Total Assets} - \text{Prior Period Total Assets}) / \text{Prior Period Total Assets}$ . A significant increase or decrease in total assets may be an indication of problems and should be investigated and explained.
2. **Liability Growth** -  $(\text{Current Total Liabilities} - \text{Prior Period Total Liabilities}) / \text{Prior Period Total Liabilities}$ . A significant increase in Total Liabilities is a potential indication of cash flow problems and should be investigated and explained.
3. **Capital/Total Assets** -  $\text{Equity Capital} / \text{Total Assets}$ . This ratio provides an indication of the amount of losses that can be absorbed before insolvency.
4. **Return on Assets** -  $\text{Current Period Net Income} / ((\text{Current Period Total Assets} + \text{Prior Period Total Assets}) / 2)$ . 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** -  $\text{Current Period Net Income} / ((\text{Current Period Equity} + \text{Prior Period Equity}) / 2)$ . 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** –  $\text{Total Liabilities} / (\text{Equity Capital} - \text{Goodwill \& Other Intangible Assets})$ . This ratio provides an indication of the company's leverage position. Consistent with the risk-based examination strategy, the examination team leader should include a narrative analysis of the entity's financial condition. This analysis should include the examination team leader's conclusions regarding the financial condition and stability of the PSSP/TSP.

## **Appendix D: Uniform Rating System for Information Technology**

### **Introduction**

The following rating system is derived from the United States Federal Financial Institutions Examination Council (FFIEC) Supervision of Technology Service Providers Examination Handbook dated March 2003. This is directly applicable for the ratings of Financial Institutions and payment system service providers (PSSP/TSP's) in Egypt.

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

The first step in developing an IT composite rating for an organization is the assignment of a performance rating to the individual Audit, Management, Development and acquisition and Support and delivery components (AMDS). 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 auditor in charge of the PSSP/TSP examination should notify other CBE departments prior to issuing URSIT composite ratings of 3, 4, or 5 or engaging in informal or formal enforcement actions.

### **Use of Composite 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 payment system 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 payment system 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 payment system 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 payment system 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 payment system 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 payment system 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 the payment system service provider:
- The financial condition and ongoing viability of the entity;
- The impact of external and internal trends and other factors on the ability of the entity to support continued servicing of client financial institutions; and the propriety of contractual terms and plans.

## **Ratings**

- *A rating of 1* indicates strong performance by management and the board. Effective risk management practices are in place to guide IT activities, and risks are consistently and effectively identified, measured, controlled, and monitored. Management immediately resolves audit and regulatory concerns to ensure sound operations. Written technology plans, policies and procedures, and standards are thorough and properly reflect the complexity of the IT environment. They have been formally adopted, communicated, and enforced throughout the organization. IT systems provide accurate, timely reports to management. These reports serve as the basis of major decisions and as an effective performance-monitoring tool. Outsourcing arrangements are based on comprehensive planning; routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided. Management and the board have demonstrated the ability to promptly and successfully address existing IT problems and potential risks.
- *A rating of 2* indicates satisfactory performance by management and the board. Adequate risk management practices are in place and guide IT activities. Significant IT risks are identified, measured, monitored, and controlled; however, risk management processes may be less structured or inconsistently applied and modest weaknesses exist. Management routinely resolves audit and regulatory concerns to ensure effective and sound operations; however, corrective actions may not always be implemented in a timely manner. Technology plans, policies, procedures, and standards are adequate and are formally adopted. However, minor weaknesses may exist in management's ability to communicate and enforce them throughout the organization. IT systems provide quality reports to management that serve as a basis for major decisions and a tool for performance planning and monitoring. Isolated or temporary problems with timeliness, accuracy, or consistency of reports may exist. Outsourcing arrangements are adequately planned and controlled by management, and provide for a general understanding of vendor contracts, performance standards, and services provided. Management and the board have demonstrated the ability to address existing IT problems and risks successfully.
- *A rating of 3* indicates less than satisfactory performance by management and the board. Risk management practices may be weak and offer limited guidance for IT activities. Most IT risks are generally identified; however, processes to measure and monitor risk

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

- *A rating of 4* indicates deficient performance by management and the board. Risk management practices are inadequate and do not provide sufficient guidance for IT activities. Critical IT risks are not properly identified, and processes to measure and monitor risks are not properly identified, and processes to measure and monitor risks are deficient. As a result, management may not be aware of and is unable to control risks. Management may be unwilling or incapable of addressing audit and regulatory deficiencies in an effective and timely manner. Technology plans, policies and procedures, and standards are inadequate, have not been formally adopted or effectively communicated throughout the organization, and management does not effectively enforce them. IT systems do not routinely provide management with accurate, consistent, and reliable reports, thus contributing to ineffective performance monitoring or flawed decision-making. Outstanding arrangements may be entered into without planning or analysis, and management may provide little or no supervision of vendor contracts, performance standards, or services provided. Management and the board are unable to address existing IT problems and risks, as evidenced by ineffective actions and longstanding IT weaknesses. Strengthening of management and its processes is necessary. The financial condition of the service provider may threaten its viability.
- *A rating of 5* indicates critically deficient performance by management and the board. Risk management practices are severely flawed and provide inadequate guidance for IT activities. Critical IT risks are not identified, and processes to measure and monitor risks do not exist or are not effective. Management's inability to control risk may threaten the continued viability of the institution or payment system 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 payment system 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 payment system service provider's purchase of hardware or software, development and programming performed by the institution or payment system 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 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 than 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.