Information Technology

Conclusion: URSIT composite rating is (1,2,3,4,5).

Complete this section's objectives to assign the information technology (IT) composite rating using as a guide OCC Bulletin 99-3, "Uniform Rating System for Information Technology (URSIT)." The composite URSIT rating should reflect:

- The adequacy of the bank's risk management practices.
- Management of IT resources.
- The integrity, confidentiality, and availability of automated information.
- The degree of supervisory concern posed by the institution.

In assigning the rating the examiner should consult the EIC, the examiners assigned to review management and audit, and other examining personnel, as appropriate. Although the OCC does not assign URSIT component ratings to the financial institutions it supervises, risks arising from the areas covered by the component ratings are considered when assigning the URSIT composite rating.

Standard Core Assessment Objectives

Objective 1: Determine the scope of the information technology review.

Note: Information technology scope decisions should be coordinated with the examiner responsible for completing the audit objectives in the "Management" section of the core assessment.

1. Review the examination information to identify any previous problems that require follow-up in this area.

2. If not previously provided, obtain and review lists describing the complexity of the bank's processing environment and reports management uses to supervise the IT area, including but not limited to:

   □ A list of technology vendors/servicers, description of the products or services provided, and bank's analysis of vendors'/servicers' financial condition.

□ A list of computer systems and networks.
□ A list of software and applications that support financial information processing or the risk management process.
□ Reports used to monitor computer activity, network performance, system capacity, security violations, and network intrusion attempts.

3. Determine during early discussions with management:

- How management administers and controls IT activities throughout the organization.
- Any significant changes in systems, applications, distribution channels, or personnel since the prior examination or any planned changes.
- How management monitors the quality and reliability of outsourced services and support functions.

Using the information obtained above, decide which systems and applications will be reviewed during this examination. Examples of systems/applications are financial applications, wire transfer, item capture for transmission to a remote processing site, PC- or LAN-based programs or spreadsheets, image processing systems, and Internet banking. Consider:

- The significance of the system or application in supporting bank products and services.
- The volume of transactions processed.
- The average dollar size of the transactions processed.
- The degree of reliance placed on the application or its output by management.
- Recent audit coverage provided internally or externally.
- The most recent OCC examination coverage and changes since that review.

4. If the bank is doing in-house programming or providing automated services to other financial institutions, expand the review as necessary to assess the additional risks inherent in such activities using procedures from the *FFIEC IS Examination Handbook*.

   Procedures should be expanded, as necessary to address complex activities or to provide additional guidance to less experienced examiners.

Objective 2: **Assess the adequacy of IT management.**

1. Obtain technology-related information from the examiner assigned to review board minutes. Review and brief, as appropriate, minutes of any committees responsible for overseeing and coordinating IT resources and activities to determine user involvement and organizational priorities.

2. Review organizational charts, job descriptions, compensation, turnover, and training programs to ensure that the bank has a sufficient number of technology personnel and that these personnel have the expertise the bank requires (consider the bank's outsourcing arrangements, as appropriate).

3. **Review the effectiveness of the bank's management and monitoring of vendor/servicer activities.** Consider the guidance in OCC Advisory Letter 2000 -12, " Risk Management of Outsourcing Technology Services" in evaluating the following:

   - Vender/servicer selection process.
   - Contract guidelines, including customer privacy protections.
   - Monitoring of vendor/servicer performance under the contract, including availability of financial information and access to operations and security audits of the servicer.
   - As applicable, availability of, or access to, application source code and documentation for programs not developed or maintained by the bank. (Generally applies to turnkey software.)

4. Review documentation supporting major projects or initiatives to determine the effectiveness of technology planning, implementation, and follow-up activities. Consider:

   - The decision process, including options considered and the basis for final selection.
   - The reasonableness of implementation plans, including periodic milestones.
   - The effectiveness of monitoring of implementation activities.
   - Whether validation testing of new programs or systems is conducted prior to putting the programs into production.

5. **Review the bank's information security program for conformance with 12 CFR 30, Appendix B, "Guidelines Establishing Standards for Safeguarding Customer Information."[1] Program must:**

   - **Be approved and overseen by the Board of directors**
   - **Be adjusted, as appropriate, for changes in the bank's (or servicer's) processing environment or systems.**
   - **Include an annual report to the board (or committee) describing the overall status of the program and bank's compliance with the Guidelines.**

6. **Review MIS reports for significant IT systems and activities to ensure that risk identification, measurement, control, and monitoring are commensurate with the complexity of the bank's technology and operating environment.** MIS should be timely, accurate, complete and relevant. Consider:

   - Systems capacity including peak processing volumes.
   - Up-time performance and processing interruptions.
   - Network monitoring including penetration attempts and intruder detection.
   - Activity logs and security reports for operations, program and parameter changes, terminals use, etc.
   - Volume and trends of losses from errors, fraud, or unreconciled items.

Objective 3: **Assess the adequacy of controls to assure the integrity of data and the resulting MIS.**

Note: The review should be coordinated with the examiners responsible for the major CAMELS areas and the internal control portion of the management review to avoid duplication of effort.

1. **Evaluate the separation of duties and responsibilities in the operation and data processing areas.** Consider:

   - Input preparation and balancing.

[1] The guidelines contained in OCC Bulletin 2001-8 were a joint-agency issuance and mandated by Section 501 of GLBA. They become effective July 1, 2001.

- Data entry.
- Operation of the computer system.
- Processing of rejects and unposted transactions.
- Balancing of final output.
- Statement and report preparation and distribution.

2. **Evaluate the adequacy of input/output controls and reconcilement procedures for batch capture and image capture systems.** Consider:

   - Establishment of dollar and item count control totals.
   - Review of output and exception reports.
   - Reconcilement of application balances to general ledger accounts.
   - Balancing and reconcilement of ATM and ACH activity.

3. **Review controls and audit trails over master file change requests (such as address changes, due dates, loan payment extension/renewal, loan or deposit interest rates, and service charge indicator).** Consider:

   - Individuals authorized to make changes and potential conflicting job responsibilities.
   - Documentation/audit trail of authorized changes.
   - Procedures used to verify the accuracy of master file changes.

4. **Assess adequacy of controls over changes to systems, programs, data files, and PC-based applications.** Consider:

   - Procedures for implementing program updates, releases, and changes.
   - Controls to restrict and monitor use of data-altering utilities.
   - Process management uses to select system and program security settings (i.e., whether the settings were made based on using sound technical advice or were simply default settings).
   - Controls to prevent unauthorized changes to system and programs security settings.
   - Process and authorizations to change application parameters.

5. Determine whether employees' levels of online access (blocked, read-only, update, override, etc.) match current job responsibilities.

6. **Evaluate the effectiveness of password administration for employee and customer passwords considering the complexity of the processing environment and type of information accessed.** Consider:

   - Confidentiality of passwords - (whether only known to the employee/customer).
   - Procedures to reset passwords to ensure confidentiality is maintained.
   - Frequency of required changes in passwords.
   - Password design (number and type of characters).
   - Security of passwords while stored in computer files, during transmission, and on printed activity logs and reports.

7. Determine whether the bank has removed/reset default profiles and passwords from new systems and equipment and determine whether access to system administrator level is adequately controlled.

Objective 4: **Evaluate the effectiveness of controls to protect data confidentiality; i.e., to prevent the inadvertent disclosure of confidential information.**

1. Evaluate systems used to monitor access and identify unauthorized attempts to access the bank's systems (i.e. intruder detection).

2. **Evaluate control and security for data transmitted to or from remote locations.** Consider:

   - Type of data transmitted.
   - Use of encryption or other security techniques (e.g., firewalls).
   - Access to network components (servers, routers, phone lines, etc.) that support data transmission.

3. Evaluate controls over remote access (by modem or Internet link) to ensure use/access by authorized users only.

Objective 5**: Assess the adequacy of the bank's policies and procedures to ensure the availability of automated information and ongoing support for technology-based products and services.**

1. **Review the written business resumption contingency plan to ensure**

that the plan is consistent with the requirements of interagency guidelines. Consider:

- Whether the plan complies with the corporate-wide focus of interagency guidelines.
- Whether the board of directors or a board committee annually reviews the plan.
- Whether the plan adequately addresses all mission-critical activities or services.

2. Review the annual validation of the contingency plan, including backup/alternate site test findings. Determine whether the board and senior management were apprised of the scope and results of the backup test.

3. **If third-party servicers provide mission-critical activities or systems, ensure the bank's recovery plan is compatible with the business recovery plans of the servicers.**

4. **Evaluate planning for event management activities.** Consider:

- Emergency procedures and evacuation plans.
- Response to network attack or penetration.
- Reporting to appropriate regulatory or law enforcement agencies.

Assess processes and procedures to prevent destruction of electronic files and other storage media. Consider:

- Frequency of file backup.
- Access to backup files and storage media (disks, tapes, etc.).
- Location of off-site file storage.
- Virus protection for networks and PCs.

6. **Determine whether only authorized personnel have access to the computer area, electronic media, supplies of negotiable items, and whether equipment and networks supporting mission-critical services are appropriately secured.** Consider physical security as well as environmental controls.

Objective 6: **Assess the bank's information security risk and transaction risk**

management processes based on completion of prior objectives, discussions with key managers, and analyses of applicable internal or external audit reports.

1. Determine whether the volume and nature of fraud and processing losses; network and processing interruptions; customer-reported processing errors, or audit criticisms lower the quality of automated activities and services.

2. **Determine if the bank's risk assessment process for customer information and its test of key controls, systems and procedures in the bank's information security program are commensurate with the sensitivity of the information and with the complexity and scope of the bank's activities.**

3. Assess the timeliness, completeness, accuracy, and relevance of MIS for transaction risk. Consider the source of reports, controls over report preparation, and independent validation of report accuracy. Risk management reports should cover major sources of transaction risk identified above.

4. Using the findings from performing the previous objectives, combined with the information from the EIC and other appropriate examining personnel, make preliminary judgments on the quality of transaction risk management systems. Consider:

   - Weaknesses in recognizing and understanding existing risk.
   - Evidence that risk is not measured in an accurate or timely manner.
   - Failure to establish, communicate, and control risk limits.
   - Whether management accurately and appropriately monitors established risk limits.

Objective 7: Using the findings from meeting the foregoing objectives, determine significant risk exposures identified from the review of information technology.

Develop preliminary assessments of quantity of transaction risk, quality of transaction risk management, aggregate transaction risk, and direction of transaction risk. Refer to the section "Risk Assessment System," as needed. Comment as necessary.

In consultation with the EIC and other examining personnel, identify any findings from the information technology review that have significance for other risk rating categories.

Objective 8: Determine whether to expand the procedures or develop a plan for corrective action. Consider:

- Whether management is able to adequately manage the bank's risks.
- If management is able to correct the bank's fundamental problems.
- Whether to propose a strategy to address the bank's weaknesses and discuss the strategy with the supervisory office.

Refer to the appropriate booklets of the *Comptroller's Handbook* or *FFIEC IS Examination Handbook* for expanded procedures.

Objective 9: After completing any expanded procedures, determine whether additional verification procedures should be performed.

Obtain appropriate approvals from the ADC and district deputy comptroller, and contact the Enforcement and Compliance Division and district accountant prior to performing any direct verification procedures.

Verification procedures should be performed only if there is reason to believe that the impact of unresolved safety and soundness issues will be material.

Objective 10: Conclude the review of the bank's IT activities.

1. Provide management with a list of deficiencies for consideration.

2. Use the results of the foregoing procedures and any other applicable examination findings to compose comments (e.g., IT, MRA) for the report of examination.

3. Update, organize, and reference work papers in accordance with PPM 5400-8 (rev).

4. Update the OCC's electronic information system (e.g., ratings, core knowledge, MRA, violations).

5. In discussion with the EIC, provide preliminary conclusions about:

   - The quantity of risk.
   - The quality of risk management.
   - The aggregate level and direction of transaction risk or any other applicable risk. As appropriate, complete the summary conclusions in the section "Risk Assessment System."