Information Technology Examination Program

Examination Objectives

To determine the adequacy and/or effectiveness of the trust department's information technology. Consider whether:

- the risks involving the savings association's use of electronic capabilities have been analyzed;
- compliance with applicable law is considered;
- credible management reports are prepared and good oversight practices are apparent;
- quality policies, procedures and internal controls are established to monitor and control information technology risk;
- good physical security controls are maintained; and
- deficiencies are identified and prompt corrective action initiated.

Examination Procedures

Wkp. Ref.

Level I

Level I procedures first focus on a review of the examination scoping materials. The next step consists of interviews with trust department personnel to confirm their qualifications and levels of expertise; to determine if the trust department's practices conform to written guidelines; to establish whether any significant changes in personnel, operations or business practices have occurred; or whether new products and/or services have been introduced. If items of concern are uncovered during Level I procedures or if problems are identified during the preexamination monitoring and scoping; the examiner may need to perform certain Level II procedures.

1. Review examination scoping materials related to information technology functions of the trust department. Scoping material should include:
    - Risk profile
    - Relevant PERK documents
    - ECEF reports

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Previous trust and asset management examination report
- Workpapers from the previous examination
- Previous safety and soundness examination report
- Previous safety and soundness IT Program 341
- Information technology examination report, if conducted

2. Evaluate the information technology policies and procedures for adequacy. Consider whether they address:

   - Information integrity
   - Operations technology
   - Vendor management
   - Internet services
   - Electronic mail
   - Critical file backup
   - Contingency planning
   - From the evaluation, assess the information technology infrastructure including local area networks (LANS), wide area networks (WANS) and other information technology resources.

3. Determine if significant changes to outsourcing arrangements have occurred.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

4. Evaluate whether management has the knowledge and expertise to manage its information technology. Determine if any significant personnel and/or organizational changes occurred.

5. Determine the role and importance information technology plays within the organization and whether this presents any unique issues. Assess whether the savings association's use of information technology is appropriate to the size and complexity of the trust department.

6. How does management monitor the performance of all third party service providers? Assess management's due diligence and vendor selection process.

7. Determine whether any new information technology type products or services have been installed. Also, determine whether any new trust and asset management services required new or an adaptation of existing technologies. Consider whether:

   - internal audit assessed the new systems or programs prior to implementation;
   - management maintained the level of expertise necessary to manage these technology products and services;
   - technological advances are kept up with, such as online payment, digital signatures and/or wireless technology;
   - information systems are protected from external intrusion; and
   - system reliability and performance are considered.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

8. Has an audit or other review been performed on all service providers? Did management obtain a copy and review the results?

9. Assess the adequacy of audit coverage of the trust department's information technology. Determine whether information technology audit plans and audit schedules are commensurate with the department's information technology environment and risks.

10. Consider whether the following risk contributors (if applicable) have been addressed:

- Does management fully understand all aspects of information technology?
- Does management anticipate and respond well to market and technological change?
- Do management information systems and reports provide credible and comprehensive information?
- Are prudent due diligence efforts used in the selection of service providers when this function is delegated?
- Does management quickly identify weaknesses and take appropriate action?
- Do material, unresolved issues noted in audit, compliance or examination reports remain uncorrected?
- Do policies and procedures address all significant activities?

The completion of the Level I procedures may provide sufficient information to make a determination that no further examination procedures are necessary. If no determination can be made, proceed to Level II.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

Level II

Level II procedures focus on an analysis of trust department documents such as reports and outsourcing contracts. The examiner should complete the appropriate Level II procedures when the completion of Level I procedures does not reveal adequate information on which to base a conclusion that the trust department meets the examination objectives. Neither the Level I nor the Level II procedures include any significant verification.

1. Review the savings association's web site as it relates to trust and asset management activities. If the website is a transactional website, confirm that the savings association notified OTS and was granted approval.

2. Review the savings association's policies and procedures to determine whether there is adequate security to prevent unauthorized access and entry to customer information and accounts. Evaluate if the web site is managed in a secure manner.

3. Determine if management verified the accuracy and content of financial planning software or interactive programs (between internal and external users) available through deployed systems.

4. Determine if the savings association's contingency plan addresses information technology as it relates to trust and asset management activities.

5. Assess the guidance for employees pertaining to information integrity. Does it address the need to protect the confidentiality of customer and corporate information?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

6. Is there a segregation of duties among system developers and operations personnel?

7. Has management kept up with marketplace changes such as decimalization and has it planned for future changes such as T+1 settlement and straight through processing?

8. If the savings association operates a fedline terminal in the trust department, are there procedures in place to ensure that controls are adequate?

9. Review all exception reports. Assess management's actions and determine whether the exceptions pose any significant risk to the savings association.

10. If there are unresolved exceptions present in internal, external, compliance or examination reports, discuss corrective action with management.

If the examiner cannot rely on trust and asset management Level I or Level II procedures or data contained in department records or internal or external audit reports to form a conclusion; proceed to Level III.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

Level III

Level III procedures include verification procedures that auditors usually perform. Although certain situations may require that Level III procedures be completed, it is not the standard practice of Office of Thrift Supervision (OTS) examination staff to duplicate or substitute for the testing performed by auditors.

1. Determine if the findings of the audit/compliance review are consistent with examination findings. If not, discuss with management the reasons for any discrepancy.

2. Do the operating systems contain sufficient firewalls?

3. Are criminal background checks of key IT employees and contractors performed?

4. Is there an immediate revocation of system access rights for ex-workers?

5. For electronic funds transfers, compare the daily reconcilement of wire transfers with correspondent and general ledger accounts to detect any errors or misapplications of funds.

6. Determine if someone with proper authority has been given responsibility for assigning qualified individuals as users of fedline terminals. Determine if passwords are changed frequently and only legitimate users have access to the terminals. Determine if dual controls have been implemented. Determine if terminated employees are promptly removed from accessibility.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

7. Determine if there is an adequate procedure for backing up critical files. Test the process to determine whether it is being followed. Consider whether diskettes containing significant or critical information are labeled and stored in a secure location (on- or off-site).

8. If there are significant examination concerns, contact the OTS information technology examination division.

Examiner's UITRS Rating, Summary, Conclusions and Recommendations:

References – 510P

Laws

Code of Federal Regulations

Office of Thrift Supervision Publications

TB 11-1 Purchased Software Evaluation Guidelines

Other

FFIEC Information Systems Handbook

Workpaper Attachments – 510P

Exam Date:
Prepared By:
Reviewed By:
Docket #:

Optional Topic Questions

The following list of questions is offered merely as a tool and reference for the examiner and is not a required part of the examination process.

Audit Process

▪ Does the auditor have specialized information systems audit training?
▪ Is the scope of the audit program commensurate with the extent of information systems activities? Does the audit program concentrate on issues such as contract administration, insurance, operational controls, on-line access controls, contingency planning and PC/LAN/WAN controls?
▪ Does the audit program test balancing procedures of automated applications including the disposition of rejected and unposted items?
▪ Does the audit program sample customer record files (master files) to verify them against source documents for accuracy and authorization?
▪ Does the audit program spot-check computer calculations such as fee charges, past due loans, etc.?
▪ Does the audit program verify output report totals, check the accuracy of exception reports, trace transactions to final disposition to determine adequacy of audit trails and perform customer confirmations?
▪ Do the audit procedures cover the flow of critical data through interrelated systems from the point of origin to point of destination?
▪ Does the audit process include a review of the servicer's third-party review report? If so, is an evaluation made of any exceptions and recommended corrective action?

Outsourcing Arrangements

▪ Are outsourcing arrangements with vendors and subcontractors included in the savings association's compliance reviews?
▪ Determine if management investigates and documents its selection process for new service providers? Does it include the following: • Alternative services? • Pricing of services, including special charges for forms, equipment, etc.? • Quality of reports and user documentation? • Financial stability of the servicer? • Contingency planning? • The ability of the servicer to handle future processing requirements? • Requirements for termination of service? • Insurance requirements?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Review of service contract by savings association's legal counsel?
- Does the servicer provide the institution with current, understandable user instruction manuals for each application and do the employees use them?

- Determine whether the service contract provisions include:
  - Description of work performed and time schedules for processing and delivery of work.
  - Fee schedules and other charges.
  - On-line communication access and security.
  - Audit responsibility.
  - Opportunities for the savings association to review independent annual audits and similar reports.
  - Provisions for contingency backup processing and record protection.
  - Notice required (both parties) for termination of service and the return of customer records in machine-readable form.
  - Confidentiality of data files and programs.
  - Insurance carried by the servicer.
  - Liability for documents damaged or lost in transit.

- Determine whether the contract administration policies and procedures provide for monitoring and management of the information system service provider's performance in areas such as:
  - Service level performance and service charges
  - Financial condition
  - Ability to meet future needs
  - Performance reports by information system service provider

- Are there reasonable requirements for periodic due diligence reviews of third-party providers, including contractors, subcontractors, support vendors and other parties?

Operations Technology

- Are procedures in place to control customer transfers of funds from each access point?
- Are safeguards in place to detect and prevent duplicate transactions within each system deployed?
- Do policies and procedures address the savings association's use of electronic mail?
- Do policies and procedures address transmissions among all user groups, including customers, officers and employees?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

▪ Are file maintenance changes to customer account record files (master files) requested in writing (Note: In on-line systems, this procedure is handled as part of the system access controls and supervisory override feature)? Are the changes and requests reviewed by staff and, when appropriate, a supervisor? Are the changes verified for correctness after processing?
▪ Are microfilm, digitized records, paper copies of checks and data entry source documents secured? If so, verify that: • Documents and microfilm/microfiche are stored on- or off-site in a secure location with limited access; • An inventory or usage log is maintained at the storage site location and the quality of the microfilm is checked periodically.

Critical File Backup

▪ Does the savings association have procedures and a training program to promote awareness on the use and care of PCs?
▪ Is the trust department processing significant applications on a PC and reconciling the input and output for accuracy?
▪ If yes, has the department developed a security policy that contains minimum control standards for PCs as described in Thrift Bulletin 29 End-User Computing?
▪ Is there an established program for ongoing review of each system used for content, continued appropriateness, accuracy, integrity, security, controls, system updates, obsolescence, system capacity and strategic direction?

Information Security

▪ For interactive systems, does management require a review of the interactive components and processes to ensure compatibility and security?
▪ Has senior management established appropriate levels of access to information and applications for officers, employees, system vendors, customers and other users? Are access levels formally established and reviewed on a regular basis?
▪ Have appropriate procedures been established to monitor for unauthorized attempts to access the savings association's system? Verify that policies require formal reporting in the event of attempted or actual attacks against any of the savings association's systems.
▪ Are terminals with service provider access controlled by user logon codes, passwords known only to specified individuals or encryption and when necessary, physical keys and physical configuration?
▪ Are users with terminal access controlled by unique user log-on codes or passwords known only to the user?
▪ Is access to PCs restricted due to physical security (keyboard locks, secure rooms) and software security (passwords) and enforced?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

▪ Are PCs linked to a LAN or WAN? If so, are passwords used to grant access and functional authorization on the system? Are passwords changed periodically? Does each user have a unique user identification code and password?
▪ Have periodic changes been made to user log-on codes, passwords and supervisory override passwords? Are they adequately controlled with regards to personnel authorized to make changes, the security of documentation and monitoring and reporting of violations?
▪ Are users or terminals controlled as to the applications they can access, the transactions they can initiate, and specific hours of operation? ▪ Are there sign-off procedures or an automatic sign-off after a period of inactivity?
▪ Are security passwords and user identification codes suppressed on all video and printed output displays?
▪ Does the trust department have any direct connection between its internal operating system(s) and the system that hosts the external electronic service or activity (for example, a Web site)? If the savings association does have a direct connection, an IT examiner should be consulted.
▪ Does the trust department establish the legitimacy of each party requesting an account action or submitting related instructions or data?
▪ Are appropriate exception reports generated and reviewed on a periodic basis? In addition, do the reports indicate: • All transactions made at a terminal by an operator • Restricted transactions • Correcting and reversing entries • Dates and times of transactions • Unsuccessful attempts to access the system and restricted information • Unusual activity

Web Site

▪ Has the savings association incorporated a web site in its business plan?
▪ Has management assessed the annual operating and maintenance costs (including telecommunications, hardware, software, personnel, etc.) in operating a web site?
▪ Do the savings association's policies and procedures address authentication concerns relating to those customers that may not physically visit the savings association?
▪ Do the savings association's policies and procedures address fraud and how it will deal with those situations perpetrated outside its geographical area and/or legal jurisdiction?
▪ Does the trust department have encryption techniques used to process all data, from the end-user personal computer back through the firewall (or DMZ) and to the main data processing site? Refer review of complex web site technology to IT examination staff.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

▪ Are account inquiries and fund transfers processed end-to-end? (If website is "transactional" refer to IT examinations staff.)

Contingency Plan

▪ For contingency planning purposes, is there a backup system or method established for users to conduct normal activity in the event the system is not available for an extended period of time?
▪ Are there instruction guides and other support materials that address the backup system or method?
▪ Has management established a reasonable procedure to notify users in the event of a problem?
▪ Is the saving association's plan compatible with its service bureau's plans?
▪ Does the plan identify all critical resources, including data communication networks?
▪ Does the plan provide for in-house communication hubs?
▪ Does the plan require the savings association to participate in service bureau disaster recovery tests?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____