Division of Supervision and Consumer Protection

Information Technology

GENERAL WORK PROGRAM

APRIL 2004

Table of Contents

WORK PLAN QUESTIONS:

Questions
1. Audit
1a. When was the last audit of IT-related activities performed? How frequently does management perform audits of IT-related activities? Evaluate the institution's risk assessment methodology use to prioritize IT audit resources and to formulate the audit schedule and scope. **Comment:**
1b. Does the auditor routinely submit written reports and audit schedules to the Board of Directors or the audit committee? **Comment:**
1c. Review audit report(s) since the previous examination addressing IT activities. Indicate whether the report(s) adequately: • Describes scope and objectives. • Describes deficiencies. • Suggests corrective action and management's response (including commitments for corrective action and timelines for completion). • Details follow-up/correction of prior audit or regulatory examination exceptions. **Comment:**

Questions
1d. Does the internal and/or external auditor or designated officer or employee (someone not directly involved in the daily processing of activities) periodically review the following: • Back-office operations (including balancing, reconciling, input/output procedures, and controls over exception items)? • Segregation of duties? • Disaster Recovery Planning and Business Continuity Planning? • Data and physical security for critical platforms (e.g., mainframe, network and Electronic Banking)? • Programming and change control activities? • Vendor-provided software updates and releases (including installation of emergency changes)? • Wire transfer activities (including ACH, ATM, POS, and Fedline, if applicable)? • Internet banking activities? • Telephone banking activities? • Technology outsourcing arrangements? • Employee accounts? • Compliance with Section 501(b) of the Gramm-Leach-Bliley Act? **Comment:** **[364-B]**
1e. Does the auditor (or designee) have any conflicting duties? If so, list them. Skip this question if the IT audit is outsourced. **Comment:**
1f. Is audit expertise and training sufficient for the complexity of the system and the risk to the institution? **Comment:**
1g. Is audit software used? (If so, identify the program, describe uses and controls, and indicate when it was last used.) **Comment:**
1h. Is the auditor involved in hardware/software purchases (IS Steering Committee decisions, etc.)? Skip if IT audit is outsourced. **Comment:**

Questions
2. Management
2a. Assess the adequacy of management's actions to correct deficiencies noted in the previous IT examination reports, as well as internal and external audits, and address findings cited in the review of service providers where appropriate. **Comment:**
2b. Determine the adequacy of the Board and senior management in implementing both short- and long-term strategic planning. Evaluate any significant plans for changes in IT management personnel, software, hardware, or operating procedures. **Comment:**
2c. Review Board and/or IT related committee minutes and document significant matters. **Comment:**
2d. For outsourced services, assess the adequacy of contracts and service-level agreements (SLAs) for applications processed by servicers. **Comment:**
2e. Is adequate management succession provided for IT operations? Have an adequate number of financial institution personnel been trained to supervise and operate the system to reduce dependence on key personnel? **Comment:**
2f. Has management performed and documented an annual review of insurance coverage? **Comment:**
2g. Determine whether the bank has filed a notice of service provider relationship with the appropriate regulator as required by the Bank Service Company Act (BSCA) for services outsourced since the previous examination. **Comment:**

Questions
2.1. Information Security Program
2.1a. Has the Board or its designated committee approved a written Corporate Information Security Program that meets the requirements of the Information Security Guidelines? • If more than one information security program exists for the institution, are the programs coordinated across organizational units? • Has an effective process been established to adjust the information security program as needed? **Comment:** **[364-B]**
2.1b. If the Board has assigned responsibility for security program implementation and review of management reports to an individual or a committee, do they possess the necessary knowledge, expertise and authority to perform the task? **Comment:** **[364-B]**
2.1c. Consider the following when evaluating the Risk Assessment process: • Does the institution identify all reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems? • Does the institution identify and prioritize its risk exposure, decide on the risks it must mitigate, and create a mitigation strategy? Is the decision to accept risks documented and reported to the appropriate management levels? • Does the institution consider the criticality of the information being protected in creating a risk mitigation strategy? • Does the institution support its estimate of the potential damage posed by various threats? • Review the institution's existing controls to mitigate risks. Does the institution's analysis consider the current administrative, physical, and technical safeguards that prevent or mitigate potential damage? • Does the risk assessment include vendor oversight requirements? **Comment:** **[364-B]**

Questions
2.1d. Review written policies and procedures and determine whether the following controls have been considered where appropriate. • Logical and physical access controls. • Programming and change control procedures. • Dual control, segregation of duties, and employee background checks. • Disaster recovery and business continuity. • Encryption. Determine whether all applicable policies address any new products, services, or delivery channels impacted by electronic capabilities. Do senior management and the Board annually review IT-related policies and procedures and is the review documented? **Comment:** **[364-B]**
2.1e. Is staff adequately trained to implement the security program? **Comment:** **[364-B]**
2.1f. Determine whether key controls, systems, and procedures of the information security program are regularly tested by independent third-parties or qualified independent staff in accordance with the risk assessment. Consider the following: • Nature and frequency of testing consistent with risk assessment priorities. • Adequacy of testing. • Management review and response to testing results. **Comment:** **[364-B]**
2.1g. Does the institution have a process for identifying and classifying information (data and system components) according to sensitivity and confidentiality? How does it use this process in its risk assessment? **Comment:** **[364-B]**

Questions
2.1h. Determine the usefulness of risk assessment reports from management to the Board (or its designated committee). Do the reports adequately describe the overall status of the program, material risk issues, risk assessment, risk management and control decisions, service provider oversight, results of testing, security breaches and management's response, and recommendations for program changes? • How often does the Board (or its designated committee) review reports and determine the usefulness of these reports? **Comment:** **[364-B]**
2.1i. Summarize your responses to questions 2.1a – 2.1h to assess if the institution has complied with the requirements of Appendix B, Part 364, Standards for Safeguarding Customer Information. **Comment:** **[364-B]**
2.2. Vendor Management
2.2a. Does the bank have a vendor oversight program that includes analyzing SAS70 reports, financial statements and other reports on its significant vendor(s) and/or servicer(s)? **Comment:**
2.2b. Determine whether the Board, or an appropriate committee, approves new or significant changes to the service provider relationships based on a written business plan and risk analysis commensurate with the proposed/planned activity. The analysis should address the following: • Purpose and goals of the banking product offerings within the strategic and operating plans. • Review of projected financial impact of third-party arrangements. • Risks (definitions and acceptable levels) associated with each outsourcing arrangement. • Role of audit, compliance, and legal staff. • Extent of outsourcing and responsibility for managing the service provider relationship. • Whether management has implemented procedures to verify the accuracy and content of any information provided by a third-party. **Comment:**

3. Development and Acquisition

3a. Evaluate procedures for acquiring significant new software. Consider the adequacy of:

- The definition of user needs.
- Vendor evaluation – financial condition, talking with other clients, etc.
- Service provider access controls or internal segregation of duties surrounding change controls.
- Testing before implementing to production.
- Reporting to senior management on status.

Comment:

3b. Is a software contract or license agreement in effect for all software? If so, does it grant the institution:

- Possession of current source code and program documentation for each application?
- The ability to obtain, use and modify the software in the event the software vendor is unable or unwilling to properly maintain the program(s)?
- Independent assurances that the documentation and source code are current if contractually held under escrow agreement?

Comment:

3c. Are vendor updates, releases, and emergency program changes reported to senior management before implementation or as soon as possible thereafter? Have all vendor updates and releases been installed? If not, what is the affect on vendor support? Is senior management informed of:

- Delays in installing program updates and releases?
- Pre-change notification by vendor or development staff?
- Vendor access controls or internal segregation of duties surrounding change controls?
- Testing before implementing into production?
- Status reports to senior management?

Comment:

3d. For remote vendor access to the computer, is there adequate control such as:

- Senior management approval?
- Limiting and monitoring of activities performed?
- One-time dial-in password access controlled by the institution?
- No dial-in access without institutional action (turn on modem, open port, etc.)?
- Call-back or automated dial-back procedures before vendor access is allowed?
- Detailed activity log of software and data file access?

Comment:

4. Support and Delivery
4a. Is separation of duties and responsibilities adequate in the following areas: • Input preparation and balancing? • Data entry? • Operation of the computer system? • Handling of rejects for reentry? • Review and handling of unposted transactions? • Balancing of final output? • Statement preparation? **Comment:**
4b. Do supervisory personnel review reconcilements, exception items and activity reports regularly? Do they include the: • Receipt of all scheduled output reports even when the reports contain no activity? • Effective review of all output and exception reports? • Determination of whether rejected, unposted, and listings of captured items are independently balanced? **Comment:**
4c. Are master file change requests (such as address changes and due dates): • In writing? • Kept in a log book? • Formalized with procedures? • Reconciled to the change report by an independent individual? **Comment:**
4d. Is all computer output (printouts, microfiche, optical disks, etc.) adequately controlled and disposed of? **Comment:**
4e. Are negotiable items that are computer processed (e.g., CD interest checks) adequately controlled? Comment: **Comments:**

4f. Determine procedures for setting/changing in-house parameters (interest rates, service charges, etc.).

- Authorization/direction to change (i.e., approval for rate/fee changes in a source document).
- Verification by independent person after input. Are parameter change results verified the next day?
- Authorization check by independent person that change was approved/authentic.

Comment:

4g. Are activity, problem, and transaction files (or logs) maintained and reviewed in a timely manner? Are the logs adequate to monitor and evaluate IT activities?

- Are reports that record unsuccessful attempts to gain access (during and after business hours) to the telecommunications system, applications, or operating systems routinely reviewed? If so, how is the review documented?
- Is a transaction file maintained for all messages received from all terminals?

Comment:

4h. Evaluate the system's capacity and performance monitoring processes/programs. Determine whether:

- Services provided meet the needs of the institution.
- Adequate resources are available to ensure daily processing and backup routines are completed before start of next day demands.
- Processes are adequate to troubleshoot problems (network and application processing), monitor utilization of disk space, etc.
- Management is alerted to any outages in service or significant response time delays.

Comment:

4i. Are data processing personnel denied access to source programs and other documentation that are unnecessary to perform their duties?

Comment:

4j. Are sufficient controls in place to ensure that Automated Clearing House (ACH) transactions are processed in a secure manner?

- Are policies and procedures in place for ACH activities?
- Handling of rejects for reentry?
- Review and handling of holdover transactions?
- Daily balancing of system transactions?
- Separation of duties for transaction processing?
- Written agreements for all ACH customers?
- Have ACH activities been considered in the institution's insurance program?

Comment:

4k. If imaging systems are used (i.e. check truncation or document storage), are controls adequate?

- If required for legal documents, does the chain of custody for converting original documents to electronic images (scanning process) ensure that images can not be altered?
- Are controls over the indexing process adequate?

Comment:

4l. Are adequate controls for wireless networking technology (e.g. 802.11) in place?

- Does the bank have a wireless policy even if the bank does not utilize wireless?
- Do controls include monitoring for rogue devices?

Comment:

4.1. Data and Physical Security

4.1a. Review access rights and permissions for the following:

- Mainframe operating system
- Network operating system
- Application software (i.e. core banking applications)

Determine whether user access profiles are consistent with their job function.

Compare a sample of users' access authority with their assigned duties and responsibilities.

Comment:

4.1b. Is access to the system restricted by:

- Power-on passwords when the computer is turned on, a password must be entered before access to the network is granted?
- Passwords?
- Unique operator identification (user logon ID)?
- Functions available to specific terminals?
- Automatic timeout if left unattended? If so, how long?
- Automatic log-off after repeated failed access attempts? If so, how many? There should be no more than three.
- Time of day and day of week?
- Firewalls, routers, etc?

Comment:

4.1c. Determine password parameters (length, numeric/alphanumeric, composition, etc.).

- Are passwords changed at an appropriate time frame? If so, how often?
- Are passwords suppressed from all output?
- Are password files encrypted and restricted?

Comment:

4.1d. Are user IDs and passwords revoked when users:

- Leave the employment of the institution?
- Are absent for an extended period of time?

Comment:

4.1e. Determine whether sufficient controls are in place to prevent the corruption of data or software and to correct problems caused by computer viruses or operating system vulnerabilities. Assess:

- Virus detection practices for servers and workstations.
- Signature updates for virus detection applications (server- and workstation-based).
- Procedures for timely installation of vendor-supplied software patches.
- Periodic data file back up.
- Policies to establish the use of virus detection software and the products used.
- Whether virus detection software distribution is made through downloads from the bank's server.
- Whether the bank's software distribution process provides for virus detection/prevention.

Comment:

4.1f. Evaluate the adequacy of network architectures and the security of connections with public networks (including dial-in access through modems, e.g., credit bureau requests). Review the network topology (schematic diagram) to understand the relative connections between public networks, internal systems, and core banking applications. Consider the following:

- The presence of firewalls between public networks and internal systems.
- The adequacy and findings of the most recent network security assessment that was performed.
- Whether management's process for ensuring firewall(s) and other network devices receives updates/patches/fixes to mitigate newly discovered vulnerabilities.
- The methods used to authenticate, monitor, and control remote user access, either through dial-in, virtual private network (VPN), or other technologies.
- The presence of controls and approvals for modems on individual PCs.
- The use of intrusion detection systems (IDSs) and their effectiveness.

Comment:

4.1g. Evaluate the effectiveness of incident response practices. Consider the following:

- Establishment of appropriate escalation procedures to address varying alerts or incidents.
- Establishment of an incident response team to address incidents.
- Procedures governing actions to be taken based on incident reports received from outsource providers (Internet service providers [ISP], application processors, etc.).
- Procedures for reporting suspected crimes and computer intrusions on Suspicious Activity Reports (SARs).

Comment:

4.1h. Determine whether security administration practices provide adequate separation of duties and appropriate supervisory review of security system maintenance activities. Consider the following:

- Designation of an overall security administrator.
- Conflicting duties between data security and operations.
- Whether exception and other security-related reporting systems are enabled and the reports are reviewed by an independent party in a timely manner.

Comment:

4.1i. Are adequate safeguards in effect to ensure that only authorized personnel are permitted in the computer area?

Comment:

4.1j. Are compilers and utility programs with data or program altering capabilities adequately controlled by:

- Dual control procedures after removal from the system?
- A password system?
- Other acceptable methods? (Explain.)

Comment:

4.1k. Determine the controls and policies related to remote user's dial-in access capabilities.

Comment:

4.1l. Is the computer area adequately protected by:

- Heat and smoke detectors?
- A fire suppression system?
- Remotely monitored alarm systems?
- Other methods? (Explain.)

Comment:

4.1m. Is the computer area uncluttered and hazard free?

Comment:

4.1n. Is the computer(s) equipped with an appropriate uninterrupted power supply (UPS) or alternate power source?

Comment:

4.1o. Does the bank use encryption during the storage and transmission of information? If so, how did management choose the encryption method? How did management determine that the encryption was strong enough for the sensitivity of the information?

Comment:

4.1p. Does each employee sign a policy statement stating that he or she must:

- Use computer systems solely for corporate business purposes?
- Maintain the privacy and confidentiality of all confidential and institutional data?
- Use unique user-IDs and personal non-trivial secret passwords to access computer systems?
- Be responsible for all activities occurring with his or her user-Ids?
- Log out of all systems when leaving a computer system unattended?
- Report information security violations immediately?
- Adhere to virus control procedures?
- Refrain from connecting networked workstation to modems without approval?
- Never download unauthorized shareware programs or files for use without proper authorization?
- Never transmit any proprietary, confidential, or otherwise sensitive information without proper authorization?

Comment:

4.2. Disaster Recovery Planning/Business Continuity Planning

4.2a. Is electronic media stored in a fire resistant, limited access area both in the financial institution and at the backup site? Is access to on-site and off-site data files (tapes and/or disks) limited to authorized personnel?

Comment:

4.2b. Is a copy of all master files taken off-site promptly after updating and not left in the data center overnight or over a weekend? Consider the following:

- Length of time before data files are taken off-site and whether they remain off-site or are returned.
- The number of copies of back-up tapes maintained at the back-up site to ensure that there is a back-up in case of a bad tape or disk.
- The method and security of transport to the off-site storage site.
- The distance to the off-site storage location.

Comment:

4.2c. Is there adequate and current off-premises storage of:

- Data files?
- Source and object programs?
- System and program documentation?
- Operating systems and utility programs?
- Reserve supplies?
- User and operator instructions?
- A copy of the contingency plan and backup agreement?

Is there a current inventory list of the items?

Comment:

4.2d. Are employees familiar with their responsibilities under the emergency plan?

Comment:

4.2e. Does the contingency plan adequately address:

- Under what conditions the backup site would be used?
- Decision-making responsibility for use of the backup site?
- Procedures for notification of the backup site?
- A checklist of data files, programs, and other items to be transported to the backup site?
- Provisions for special forms and backup supplies?
- Remote terminal activities?
- Processing instructions and priorities?

Comment:

4.2f. Is a comprehensive written agreement in effect with the backup site?

Comment:

4.2g. Has the contingency plan, including the backup site, been tested within the past 12 months?

Comment:

4.2h. Evaluate the testing of the business continuity plan. Consider the following:

- The adequacy of the test for all mission-critical applications and the level of the bank's involvement.
- The adequacy of hardware and availability of processing time to capture or submit all critical daily transactions.
- The adequacy of processing time needed to complete daily processing of critical work, including daily backup routines.
- Usage of off-site materials to conduct the recovery test.
- The scope of the bank's contingency plan test program.

Comment:

4.2i. Has a report detailing the scope and results of the backup test been presented to senior management and the Board of Directors?

Comment:

4.2j. If the institution is serviced, does it subscribe to disaster recovery services offered by the servicer? If not, does the institution have contracts with any other third-party regarding a hot site, cold site, reciprocal agreements, etc.? Explain.

Comment:

4.2k. Does the emergency plan adequately provide for:

- Personnel evacuation?
- Assignment of action to be taken in specific emergencies including the safe storage of data files and documents?
- Power-off procedures?
- Restart and recovery procedures?

Comment: