FORM 20A.9 SAMPLE AUDIT PROGRAM FOR TESTING IT CONTROLS

Workpaper Reference *Date(s) Completed*

Organization and Staffing

1. Prepare or update documentation describing the forms and procedures used to define the organization of the IT Department. _______________ _______________

2. Review the organization chart for completeness, accuracy, and appropriateness to the situation. _______________ _______________

3. Review the minutes of the IT Steering Committee meetings to determine the frequency of meeting and the level of the Steering Committee's involvement. _______________ _______________

4. Prepare or update documentation describing the forms and procedures used to segregate duties within the IT Department. _______________ _______________

5. Review the IT organization chart noting the degree to which IT functions are segregated. Ensure duties are segregated among operations, system development, security administration, and end user data control. _______________ _______________

6. Prepare or update documentation describing the forms and procedures used to administer personnel policies for IT employees. _______________ _______________

7. Review vacation schedules to note compliance with policy. _______________ _______________

8. Review the procedures followed during the last instance in which a programmer or operator was terminated to note compliance with policy. _______________ _______________

Program Changes and Program Libraries

1. Prepare or update documentation describing the forms and procedures used to provide support for Program Change Requests (PCRs). _______________ _______________

2. Review a random sample of five PCRs from the last six months to note compliance with the above controls to provide adequate support. _______________ _______________

3. Prepare or update documentation describing the forms and procedures used to ensure authorization of all program changes. _______________ _______________

4. Review a random sample of five PCRs to note compliance with the above controls to provide authorization. _______________ _______________

5. Prepare or update documentation describing the forms and procedures used to control the implementation of program changes. _______________ _______________

6. Account for a block of five PCRs as being completed or in process. _______________ _______________

7. Prepare or update documentation describing the forms and procedures used to promote the accuracy and propriety of program changes. _______________ _______________

8. Review a random sample of five PCRs to note management's review and acceptance of test results. _______________ _______________

9. Prepare or update documentation describing the forms and procedures used to establish an audit trail over all program changes. _______________ _______________

10. Review a random sample of five PCRs to note indication of the names of programs that were changed. _______________ _______________

11. Review the program listings that relate to the five PCRs selected previously to note identification of the coding changes. _______________ _______________

12. Prepare or update documentation describing the forms, procedures, and methods used to secure program libraries. _______________ _______________

13. Identify five occurrences of access to the program libraries and determine the adequacy of support for these accesses. _______________ _______________

Documentation

1. Prepare or update documentation describing the forms and procedures used to update documentation. _______________ _______________

2. Review a random sample of five PCRs to note indication of whether related documentation has been updated. _______________ _______________

3. Prepare or update documentation describing the forms and procedures used to provide uniform documentation of computer systems. _______________ _______________

4. Review documentation standards of checklist for completeness; note any deficiencies found. _______________ _______________

5. Review selected documentation of major applications and determine whether it complies with documentation standards. _______________ _______________

6. Prepare or update documentation describing the forms and procedures used to protect and update documentation. _______________ _______________

7. Review the Program Change Log for the past six months. Select three program changes that appear to require documentation changes. Trace these changes to all the documentation (systems, operations, user) to note timeliness and performance of updates. _______________ _______________

8. Confirm the existence of an off-site copy of all documentation. _______________ _______________

9. If off-site documentation is not available, determine the adequacy of physical protection for the on-site copy. _______________ _______________

Operations

1. Prepare or update documentation describing the forms and procedures used to provide adequate operations supervision. _______________ _______________

2. Obtain a copy of the IT Department organization chart; note adequacy of operations supervision. _______________ _______________

3. Obtain copies of the history for a recent week.
   a. Note indication of history review by IT management. _______________ _______________

   b. Identify any incidents of the use of the utility program. Trace to operations management authorization and documentation. _______________ _______________

4. Locate two histories that are at least three months old. _______________ _______________

5. Prepare or update documentation describing the forms and procedures used to promote accuracy and propriety of computer operations. _______________ _______________

6. Determine the location of source program libraries and documentation. Note adequacy of procedures or methods to restrict operations personnel from accessing these items. _______________ _______________

7. Review operations rotation schedules to note the extent of cross-training practiced. _______________ _______________

8. Prepare or update documentation describing the forms and procedures used to promote proper handling of data media. _______________ _______________

9. Examine external labels on 10 tapes or diskettes picked at random and note adequacy of label information. Select three of these and print their labels. Note agreement of internal and external labels with regard to volume, name, contents, and date. _______________ _______________

10. Determine the adequacy of the on-site file library organization. _______________ _______________

11. Prepare or update documentation describing the forms and procedures used to maintain hardware performance. _______________ _______________

12. Examine current maintenance contracts for the following components: CPU, consoles, disk storage devices, and line printer. Note adequacy of the hours covered. _______________ _______________

Security

1. Prepare or update documentation describing the forms and procedures used to ensure authorized usage of on-line terminals. _______________ _______________

2. Examine documentation concerning assignment of passwords to note the frequency with which they are changed. _______________ _______________

3. Using a valid password, attempt to initiate an activity restricted from that password. _______________ _______________

4. Observe terminals that are not in immediate use to note whether they are signed off. _______________ _______________

5. Prepare or update documentation describing the forms and procedures used to control processing performed online. _______________ _______________

6. Attempt to enter restricted transactions and note whether they were rejected or not. _______________ _______________

7. Locate five consecutive access logs to note their retention and indication of management's review. _______________ _______________

8. Prepare or update documentation describing the forms and procedures used to provide processing of on-line functions on a batch basis. _______________ _______________

9. For each major on-line accounting system, determine the existence of programs that provide batch processing for (normally) on-line transactions. _______________ _______________

10. For each major on-line accounting system, determine the adequacy of forms and procedures that provide for manual input of transactions which are normally entered in an on-line mode. _______________ _______________

11. For each major on-line accounting system, determine the availability of hardcopy reports to replace on-line inquiry and review them for adequacy. _______________ _______________

12. Prepare or update documentation describing the forms and procedures used to control access to the IT Department. _______________ _______________

13. Observe operations throughout the audit and note compliance with access restrictions. _______________ _______________

14. Review access levels of all employees and compare that to their current responsibilities. Determine their access is necessary based on current job duties. Ensure no terminated employees still have access to the bank's systems. _______________ _______________

15. Review procedures around terminated employees and how system access is removed, keys are obtained, and combinations are changed. _______________ _______________

16. Obtain and review the bank's current computer use and e-mail use policies and verify employees are required to sign for reading them. _______________ _______________

17. Verify the bank has policies requiring passwords to be changed periodically and never to be written. _______________ _______________

18. Review all external access points to the network and mainframe and ensure they are properly documented, reviewed on a regular basis, and access is monitored. _______________ _______________

19. Review firewalls surrounding the internal network and systems. Verify intrusion detection procedures are in place and regularly monitored. _______________ _______________

20. Review the use of encryption for the transmission of sensitive information within the bank's systems and information going outside the bank. _______________ _______________

Safety Measures

1. Prepare or update documentation describing the physical protection of the IT Department. _______________ _______________

2. Tour the computer room to note the presence and location of:
   - a. Portable fire extinguishers (are they recently inspected?) _______________ _______________
   - b. Fire detection sensors and alarms _______________ _______________
   - c. Automatic fire extinguishing system _______________ _______________
   - d. Electric power shut-off switch _______________ _______________
   - e. Telephone _______________ _______________
   - f. Emergency lighting _______________ _______________
   - g. "No smoking" signs _______________ _______________
   - h. Emergency exit signs _______________ _______________

3. Review physical security (locked doors, etc.). _______________ _______________

4. Review the emergency action/disaster recovery plan for adequacy and content:
   - a. Actions to be taken (e.g., equipment shutdown) _______________ _______________
   - b. Individuals to phone _______________ _______________
   - c. Materials to be removed from the computer room _______________ _______________

Backup Systems

1. Prepare or update documentation describing the forms and procedures used to help ensure the capability of off-site processing facilities. _______________ _______________

2. Confirm backup agreements with the management of the primary backup facility. _______________ _______________

3. Prepare or update documentation describing the forms and procedures used to help ensure the availability of backup resources. _______________ _______________

4. Verify the presence of the off-site file containing the copy of the operating system. _______________ _______________

5. Verify the presence of the off-site files containing the copies of source and object program libraries. _______________ _______________

6. Select one major application and verify that all master files and transaction files are present, by printing the labels of the off-site backup files. _______________ _______________

7. Examine off-site copies of documentation to verify their existence and ensure that they are reasonably complete. _______________ _______________

8. Determine the date of the last off-site program backup and evaluate its timeliness. _______________ _______________

9. Evaluate the physical protection of the off-site backup location. _______________ _______________

10. Prepare or update documentation describing the forms and procedures used to plan the off-site processing of data. _______________ _______________

11. Obtain a copy of the contingency plan and review it for completeness and currency. _______________ _______________

12. Review results of most recent test of contingency plan and back-up site. Testing should be performed at least annually. _______________ _______________

13. Verify a copy of the disaster recovery/contingency plan is maintained off-site. _______________ _______________

14. Prepare or update documentation describing the forms and procedures used to plan the off-site processing of data. _______________ _______________

15. Verify an IT risk assessment has been performed. _______________ _______________

Insurance

1. Obtain a copy of the most recent report of the IT Insurance Review and note any recommendations or weaknesses. _______________ _______________

2. Obtain copies of the IT insurance policies and note that effective dates are current. _______________ _______________

3. Review insurance policies and note stipulations or requirements that must be met by the IT Department to prevent voiding the insurance coverage. Verify that IT management is aware of these requirements and has instituted policies or procedures to meet these requirements. _______________ _______________

4. Prepare or update documentation describing the forms and procedures used to control data processing performed for outside organizations. _______________ _______________

Customer Service

1. Review service contracts to find one for each service customer. Ensure the contracts are current. _______________ _______________

2. Examine contracts to find that terms include:

   a. Description of work to be performed and established time schedule _______________ _______________

   b. Formula for processing fees _______________ _______________

   c. Statement of bank liability _______________ _______________

   d. Signatures of both parties _______________ _______________

3. Determine that service logs are complete and currently maintained. _______________ _______________

4. Determine that customer personnel signatures are current by comparing signatures on recently received work with the samples of authorized signatures. _______________ _______________

5. Obtain and review SAS 70s for third-party processors. Follow up on any weaknesses noted. _______________ _______________

Information Security

1. Review the bank's information security program and verify all requirements of the Gramm-Leach-Bliley Act (GLBA) are included. _______________ _______________

2. Review the controls over the exchange of nonpublic customer information with both internal and external parties and ensure compliance with GLBA. _______________ _______________

Internet Banking

1. Review the bank's Web site for compliance issues, including FDIC insured and equal housing lender logos and terms and conditions. _______________ _______________

2. Review the internal controls surrounding access and distribution of customer PINs and passwords, including changes to them. _______________ _______________

3. Obtain and review the third-party provider's SAS 70 and follow up on any significant weaknesses. _______________ _______________

4. Review the adequacy of the third party's intrusion detection and monitoring procedures. _______________ _______________