Division of Supervision and Consumer Protection
Information Technology
IT-MERIT
PROCEDURES
SEPTEMBER 2002

Management

Strategic Management
1. Describe how management integrates technology strategic planning into the overall Corporate Business Plan.
Examiner Evaluation of the Bank's Response:

Technology Changes
2. Describe new technology implemented since the last exam or in the past two years, whichever is the shortest time period. Describe planned or anticipated technology changes in the next year.
Examiner Evaluation of the Bank's Response:

Risk Assessments
3. Explain management's process for identifying, risk ranking, and mitigating IT risks within the organization. • Who is responsible for this process? • What is the mechanism for reporting these risks to the Board? • What is management's process for determining the confidentiality of electronic and paper-based information? • How is the information protected?

Examiner Evaluation of the Bank's Response:

Board Reporting
4. Detail what reports and other communications are provided to the Board for its evaluation of IT risks within the organization. • What is the frequency of this communication?
Examiner Evaluation of the Bank's Response:

Network Diagram
5. Provide the bank's network topology/schematic diagram.
Examiner Evaluation of the Bank's Response:

Vendor Management
6. Describe management's vendor management process and ongoing due diligence program. • Provide a list of the bank's key IT vendors and consultants. • Are all of these vendors covered by a current contract? • How has management evaluated the vendors' procedures for conducting employee background checks?
Examiner Evaluation of the Bank's Response:

Information Security

Information Security Program
7. Has the Board or its designated committee approved a written Information Security Program? Do the polices addressing the Information Security Program cover the following: • Roles and responsibilities (central security coordination, segregation of duties, incident response, skill continuity)? • Personnel security (background checks, acceptable use training email/Internet)?

- Audit (scope, internal/external auditor qualifications, system log reviews, audit trails)?
- Vendor management?
- Access controls (mainframe/network logical controls, password parameters, authentication, etc.)?
- Configuration management (security patches, software upgrades, parameter changes)?
- Contingency planning (business continuity, backups, disaster recovery)?
- Virus protection?
- Telecommunications (firewalls, modems, intrusion detection, encryption)?
- Restricted access (terminal/data center access)?
- Safety (fire prevention/detection, housekeeping)?
- Inventory management (theft detection, media disposal, hardware, software, source documents, output)?

Who is responsible for maintaining the Information Security Program?

Examiner Evaluation of the Bank's Response:

Roles and Responsibilities

8. Who are the information security officer and the system administrator? Provide detail on their experience, training and certifications, and other duties within the organization.

Examiner Evaluation of the Bank's Response:

Access Controls

9. Describe the process for determining and reviewing user access levels?

Examiner Evaluation of the Bank's Response:

10. Provide details on the following password control features utilized by the bank's applications and operating systems:

- Password length.
- Change interval.
- Password composition rule.

- Password history.
- Lockout rule.

Examiner Evaluation of the Bank's Response:

Disaster Recovery
11. Describe the bank's disaster recovery testing process. Include the scope, results, and date of the bank's most recent disaster recovery test.
Examiner Evaluation of the Bank's Response:
12. Describe the bank's backup procedures. • What is backed up? • What is the rotation schedule? • Where are backup media stored? • How soon after backup media are created are the media taken off-site?
Examiner Evaluation of the Bank's Response:

Physical Security
13. How are critical technology resources physically secured (mainframe, servers, telecommunications equipment, wiring closet)?
Examiner Evaluation of the Bank's Response:

Audit

Audit Scope
14. How does management establish the scope and frequency of IT audits?
Examiner Evaluation of the Bank's Response:

Audit Methods

15. What validation methods (internal and/or external audits, security assessment, penetration study) does management use to determine compliance with written and approved corporate policies?

- Provide date, scope and frequency of the validation methods described above.
- Provide detail on management's process for addressing audit findings/corrective actions.
- Is this process documented?

Examiner Evaluation of the Bank's Response:

Audit Trails

16. Which of the following activity logs/exception reports are reviewed and who performs the review?

- New loans.
- File maintenance.
- Dormant.
- Parameter changes.
- Kiting.
- Employee accounts.
- Audit logs.
- Backup logs.
- System reports.
- Firewall logs.
- Intrusion Detection System (IDS) logs.

Examiner Evaluation of the Bank's Response: