EM-31.7

Category: **Board & Management Operations**
Topic: **Information Technology & Security**
Published: 4/18/2017

Overview

This section contains FCA's standard procedures for examining information technology and security; however, the guidance for most of the procedures is currently under development. In the interim, the following links provide related guidance that was contained in the old FCA Examination Manual and FCA IT Essential Practices Examination Manual:

- EM- 345 Other Assets
- EM- 450 Cash Management
- FCA IT Essential Practices- E-Commerce
- FCA IT Essential Practices- Operations
- FCA IT Essential Practices- System Development
- FCA IT Essential Practices- Technology Service Provider and Service Receiver
- FCA IT Essential Practices - Management
- FCA IT Essential Practices - Security
- FCA IT Essential Practices- Audit
- FCA IT Essential Practices- Glossary

Examination Procedures and Guidance

General

1. Governance & Management:

Evaluate the adequacy of the institution's overall governance and management of IT and security activities.

Guidance:

2. Security:

Determine if the institution's security program adequately safeguards assets and addresses the confidentiality, integrity, and availability of information assets, including the protection of hardware and infrastructure used to store and transmit such information.

Guidance:

3. Operations:

Evaluate the adequacy of management's processes and controls over IT operations.

Guidance:

4. Development & Acquisition:

Evaluate the adequacy of management's processes and controls to identify, acquire, install, and maintain appropriate information technology systems.

Guidance:

5. Payment Systems:

Evaluate the adequacy of management's processes and controls over payment systems.

Guidance:

6. Outsourcing Technology Services:

Determine if management maintains effective outsourcing processes and controls to govern technology service provider relationships.

Guidance:

7. E-Commerce:

Evaluate the adequacy of management's processes and controls for complying with E-Commerce regulations.

Guidance:

8. Audit:

Determine if the institution conducts an effective audit (scope, reporting, and follow-up) of IT and security.

Guidance:

The internal audit and review program is a key mechanism for ensuring IT and security processes are functioning effectively and in compliance with regulations and policies. The internal auditor (or other qualified, independent party) should review the adequacy of IT and security practices to ensure compliance with applicable criteria. The audit risk assessment and scope should address IT and security topics, and audit frequency should be commensurate with the complexity of the

institution's operations and risk profile. A reliable audit program provides the board reasonable assurance that IT and security processes are sound and that related reporting is complete and accurate.

Evaluative questions and items to consider when examining the audit function regarding IT and security include:

- ***Audit Coverage:*** **Is there periodic audit or review coverage of IT and security?** Audit or review coverage and frequency should be appropriate relative to risks, changes in the operating environment, regulatory requirements, and periodic testing needs. Coverage should also be consistent with the institution's risk assessment results and annual audit plan.

- ***Scope and Depth:*** **Are audit or review scope and depth sufficient to conclude on the adequacy, completeness, and timeliness of IT and security processes?** The scope should cover key processes and controls within the area being audited or reviewed. The depth of work should be sufficient to determine if internal controls are functioning as intended and regulatory requirements are met. The scope and depth of coverage should be consistent with the approved audit or review plan and engagement contract (if applicable). If audit or review work deviated materially from the original planned scope, the board (or Audit Committee, if so delegated) should be notified of the reasons for the change. Specific items that should be considered in the audit or review scope include:

    - IT and security policies, procedures, and other guidance.

    - Compliance with IT and security-related regulations, policies, and procedures. Audits or reviews should include sufficient testing to detect noncompliance with established criteria.

    - Board reporting systems for monitoring IT and security activities and incident response processes.

    - Access controls (both physical and logical) to ensure unauthorized attempts to gain access to the operating and application systems are recorded, monitored, and responded to by independent parties.

    - Computer operations, including physical and logical safeguards to critical systems, business resumption practices, network performance monitoring, and vendor management.

    - The quality of assistance provided to users, including the ability to handle problems.

    - Fraud-related threats and vulnerabilities, as well as anti-fraud controls.

- ***Reliability of Results:*** **Did FCA identify any concerns with audit and review reliability?** Evaluate the reliability of internal audit or review work by comparing the results to FCA's examination results in this area. This comparison often includes FCA testing of transactions that were covered in the internal audit or review (transactions are often loans or loan applications, but may include other types of transactional activity, as well). In addition to the audit or review report, examiners should request and review the workpapers and hold discussions with the auditor to obtain a more thorough understanding of work completed. Often, auditors and reviewers will complete line sheets, flowcharts, control matrices, standard work programs, workpaper forms, or other relevant documents when conducting

work. Workpapers should adequately document the work performed and support the final report. In addition, any proforma work programs, workpapers, or other tools should be accurate and sufficiently thorough. If there are material weaknesses identified by examiners that are not identified by internal audits or reviews, examiners should assess the underlying reasons.

- ***Reports:*** **Do internal audit reports sufficiently communicate IT and security review results and recommendations, if applicable?** Examiners should consider the following when evaluating the audit or review report:
    - Is the report prepared in accordance with the institution's guidelines?
    - Is an executive summary or overview included to provide the board with a general conclusion on audit or review results?
    - Is the report accurate, concise, supported, and timely in communicating the audit or review objectives, scope, results, conclusions, and recommendations?
    - Are conclusions and recommendations realistic and reasonable given the institution's size and complexity, with material and higher risk issues clearly identified and prioritized?
    - Are conclusions and recommendations supported by convincing evidence and persuasive arguments (condition, criteria, cause, and effect)?
    - Does the report conclude whether the institution adheres to policies, procedures, and applicable laws or regulations, and whether operating processes and internal controls are effective?
    - Does the report address potential vulnerabilities to fraud, if applicable?
- ***Corrective Action:*** **Are management responses to audit findings in this area reasonable, complete, and timely? Have corrective actions been effective?** Audits and reviews are only effective if corrective action is taken to remedy the weaknesses identified. As such, there should be a reasonable, complete, and timely management response to the audit or review report. In some cases, management commitments and agreements or any areas of disagreement are documented in the report or in a separate memo or tracking system. If corrective actions are not resolving the issues or concerns (based on repetitive audit findings, FCA findings, etc.), examiners should further investigate the reasons. For example, this could indicate the audit or review did not sufficiently identify the underlying causes or materiality of weaknesses, sufficient resources are not being directed toward corrective actions, or weaknesses exist in the institution's corrective action process, including board oversight of the process.