Chapter 303

INFORMATION SYSTEMS AND TECHNOLOGY

Introduction

A corporate credit union's (corporate) information systems and technology (IST) program provides information services needed to effectively manage the organization. The board of directors and senior management have the responsibility to determine what information is needed to make informed decisions in line with business objectives and to monitor activities of the corporate. Additionally, the board and senior management are responsible for properly securing information systems. Part 748 of the NCUA Rules and Regulation requires a corporate to establish a written information security program to protect the institution's information systems. A written information security program will have at least the following four essential parts:

1. *Risk Assessment* – A rigorous ongoing process to identify risks to information assets. There are various risk assessment models available for reference (e.g., National Institute of Standards and Technology [NIST] Special Publication 800-30, OCTAVE [Operationally Critical Threat, Asset and Vulnerability Evaluation] and ISO [International Electrotechnical Commission] 17799). The following list taken from the NIST method is an example of what steps are necessary to perform an information security risk assessment. These steps would be applied to each asset to determine the level of risk exposure.

    - System Characterization
    - Threat Identification
    - Vulnerability Identification
    - Control Analysis
    - Likelihood Determination
    - Impact Analysis
    - Risk Determination
    - Control Recommendations
    - Results Documentation

2. *Policy* – Creates and governs controls deemed necessary to mitigate information security risks identified as a result of risk assessments.

3. *Controls* – Administrative or technical efforts to manage, monitor or protect systems.

4. *Testing* – Various procedures such as audits, penetration tests and vulnerability assessments. The frequency and nature of these tests should be based on the results of the risk assessment.

Corporate Role

As corporates fill the role of service providers for credit unions, the information security risks facing the corporate network also represent a systemic risk for the industry. Problems with information systems at the corporate level can have a downstream effect on the security**,** reputation and well being of credit unions.

Corporate Objectives

There are a number of objectives a corporate must address to ensure the security of its information systems. They are as follows:

- *Availability*—The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.

- *Integrity of Data or Systems*—System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

- *Confidentiality of Data or Systems*—Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.

- *Accountability*—Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

- *Assurance*—Assurance addresses the processes, policies, and controls used to develop confidence technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity,

confidentiality, and accountability. Assurance highlights the importance secure systems provide the intended functionality while preventing undesired actions.

Focus Areas

Examiners will review and assess information systems using four primary focus areas.

1. *Audit* - A well-planned, properly structured audit program is essential to evaluate risk management practices, control systems, and compliance with corporate policies.

2. *Management* - Management of (information technology) IT is critical to the performance and success of an institution. Sound management of technology involves aligning its IT infrastructure to support its business strategy. The board of directors and executive management should understand and take responsibility for IT management as a critical component of overall corporate governance efforts.

3. *Development and Acquisition* – The development, acquisition, and maintenance process includes numerous risks in today's dynamic and changing technology environment. Effective project management in development and acquisition will help reduce the possibility of loss resulting from inadequate processes, personnel, or systems.

4. *Support and Delivery (Operations)* - Effective support and delivery from IT operations is vital to the performance of most critical business lines in the institution. The risks, however, involve more than just IT technology and controls. They also include processes and staff.

The review of each of the four areas will help the examiner assess the adequacy and effectiveness of the controls put in place by management.

The following provides a narrative to be utilized in evaluating the four functional areas.

Audit

In order to determine the adequacy of the audit function an examiner will want to evaluate how well the risk assessment process feeds into the audit function. The results of risk assessments likely will call for

mitigation strategies which will lead into additional controls to improve security. Those controls should be governed by policy. The audit function itself should be governed by formal policy as well.

When looking at the audit type, frequency and scope the examiner will determine if it is adequate given the technology employed by the corporate. Audit reports should be submitted to the board of directors or designated audit committee for review and proper follow-up on exceptions. Audit staff must be technically qualified to perform the reviews. Other considerations include separation of duties, potential conflicts of interest and audit staff involvement in the software development life cycle.

Management

Board Oversight

In order to determine the adequacy of board and senior management oversight there are several areas to evaluate. The examiner will want to look at whether the board approved an adequate framework to govern the IT function. Strategic planning should be coordinated with the corporate's business objectives. Significant changes planned for business processes, technology employed, key personnel, service providers or software development should be reviewed by the examiner. Management is responsible to adequately resolve IT deficiencies noted in internal and external reviews. Of primary importance is management's compliance with Part 748 of the Rules and Regulations requiring the development of an information security program. This requirement is discussed below. All corporates develop and/or acquire software so management must provide adequate oversight of software development and acquisition. Additionally, management is required to adequately plan for business continuity as well as mitigating business disruptions.

Outsourcing

The examiner will consider several items to determine the adequacy of the board's and senior management's oversight relating to outsourced technology services. A vendor management program should be governed by adequate formal policies and procedures. These would include proper due diligence completed prior to outsourcing technology services. (i.e. financial stability, GLBA, security, BCP, etc.) Adequate contracts will include confidentiality requirements and other important clauses and should be reviewed by the legal department. The vendor management program should include periodic review of critical service providers to ensure financial stability, adequate control environment, and adequate performance of service

level agreements. Outsourced services should be included in the risk assessment and risk mitigation process as well.

Security Program

The security program has become the primary mechanism to protect a corporate's information assets as well as non-public personal information addressed by the Gramm, Leach, Bliley Act (GLBA). In order to determine the adequacy of the information security program the examiner will review and assess the critical risk assessment process. As with all functional areas the essential security program will be governed by policy. The risk assessment process should be governed by a board-approved framework with a methodology robust enough to identify risks to the corporate. Essentially the methodology should include a characterization of its systems and an assessment of the risks to information assets. (Refer to the introduction section of this chapter for examples of risk assessment methodologies).

In reviewing the risk assessment process the examiner should determine whether the corporate has:

- Identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to member non-public information as well as the risks to the institution;
- Identified all reasonably foreseeable threats to the financial institution assets;
- Analyzed its technical and organizational vulnerabilities; and
- Considered the potential effect of a security breach on members as well as the institution.

The examiner will also evaluate the risk assessment process for the effectiveness of the following key practices:

- Multidisciplinary and Knowledge Based Approach—A consensus evaluation of the risks and risk mitigation practices requires the involvement of users with a broad range of expertise and business knowledge. Not all users may have the same opinion of the severity of various attacks, the importance of various controls, and the importance of various data elements and information system components. Management should apply a sufficient level of expertise to the assessment.
- Systematic and Central Control—Defined procedures and central control and coordination help to ensure standardization, consistency, and completeness of risk assessment policies and procedures, as well as coordination in planning and

performance. Central control and coordination will also facilitate an organizational view of risks and lessons learned from the risk assessment process.

- Integrated Process—A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide evidence to the risk assessment process that the controls selected and implemented are achieving their intended purpose. Testing can also validate the basis for accepting risks.
- Accountable Activities—The responsibility for performing risk assessments should reside primarily with members of management in the best position to determine the scope of the assessment and the effectiveness of risk reduction techniques. For a mid-sized or large institution, those managers will likely be in the business unit. The information security officer(s) is (are) responsible for overseeing the performance of each risk assessment and the integration of the risk assessments into a cohesive whole. Senior management is accountable for abiding by the board of directors' guidance for risk acceptance and mitigation decisions.
- Documentation—Documentation of the risk assessment process and procedures assists in ensuring consistency and completeness as well as accountability. This documentation provides a useful starting point for subsequent assessments, potentially reducing the effort required in those assessments. Decisions to mitigate or accept risk should be documented in order to achieve accountability for risk decisions.
- Enhanced Knowledge—Risk assessment increases management's knowledge of the institution's mechanisms for storing, processing, and communicating information, as well as the importance of those mechanisms to the achievement of the institution's objectives. Increased knowledge allows management to respond more rapidly to changes in the environment. Those changes can range from new technologies as well as threats to regulatory requirements.
- Regular Updates—Risk assessments should be updated as new information affecting information security risks are identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change). At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered.

As weaknesses are identified by the risk assessment the corporate may need to implement new or additional mitigation strategies. The

examiner should test specific areas of the risk assessment to validate it against industry best practices. Once mitigation strategies are determined they should be addressed in governing documents. (i.e., policy, procedures, baselines) Following both the risk assessment as well as the policy and control formulation parts of the security program, management must provide an adequate audit function to validate those mitigation strategies.

In evaluating the risk assessment process the examiner will want to make sure it includes such areas as outsourced services and software development and acquisition. As the risk assessment is a key part of the security program it should provide adequate support for the security strategy, controls, and monitoring the financial institution has implemented.

Timing of risk assessments is very important. The institution should update the risk assessment prior to making significant system changes, implementing new products or services, or confronting new external conditions affecting the risk analysis. If these conditions do not apply, the risk assessment must be reviewed at least once a year.

An important part of the security program is the incident response program. This should be board-approved and, as with any control, it should be tested periodically. This can be done with simulations and walk-through exercises. The examiner should review and evaluate the corporate's incident response program pursuant to the requirements of Appendix B, II, A of Part 748 of the NCUA Rules and Regulations.

A yearly security program report is required by Appendix A, III, F of Part 748 of the NCUA Rules and Regulations. The appendix delineates specific items that should be included in the annual reporting to the board or an appropriate committee of the board. This report describes the overall status of the information security program and the corporate's compliance with the program's guidelines.

Development and Acquisition

Corporates engage in varying levels of development and/or acquisition efforts. In order to determine the adequacy of oversight relating to software development and acquisition an examiner will evaluate several items. The development and acquisition area should be governed by formal policies and procedures. As with any project management effort or strategic planning proposal, the software development project initiatives should also be aligned with business objectives. Adequate due diligence should be performed prior to software development. In reviewing this area the examiner will determine if the software development initiative is meeting project

objectives (i.e., schedules, budgets, functionality). As noted, a risk assessment should be performed before any significant project is undertaken. Security and code reviews should be part of the software development life cycle used by the corporate.

Support and Delivery [Operations]

Network **A**rchitecture

All network designs should adequately address security through the use of firewalls and other devices. The examiner will review the network diagram for reasonableness based on the size and complexity of the network. The arrangement known as a demilitarized zone (DMZ) isolates incoming network traffic for evaluation before forwarding to the internal network. A DMZ should be used for publicly accessible servers such as web servers. Remote access from untrusted sources**;** that is, those not controlled by the corporate, should also terminate in a DMZ. The development area of a network should be segmented from production. The network design should adequately meet business objectives. With the majority of programs being accessed through the internet, robust perimeter security is of primary importance.

Intrusion Detection and Response

Intrusion detection and response is an important component for security of information assets. There must be a formal incident response plan as required by Part 748 of the Rules and Regulations in the event of a breach of data or systems. This should be governed by policy and tested periodically.

From a technical standpoint, in order for a network intrusion to be detected and mitigated timely, the corporate must have adequate intrusion monitoring. There are several methods and levels of intrusion detection. Intrusion Detection System (IDS) devices can be placed at various points within the network to protect internal areas of the network. Software can be placed on hosts to protect critical systems. The method or levels chosen by the corporate should be based on its risk assessment. The examiner will verify the intrusion detection method and response also includes outsourced services.

Physical Access to Critical Equipment

Access to critical equipment should be limited to personnel with a need to access the equipment to perform their daily duties. The equipment must be physically secured from unauthorized access. Locks with keypad or card access are common for most data centers.

There should be a level of monitoring to track who has accessed the data center. Often this is accomplished with keypad or card access software and/or sign-in forms.

System Access Levels

All computer equipment should be set up with access levels based on the user's job function and "least privilege" concept. The concept requires limiting access only to the systems and services actually needed by the user. The corporate should have a process in place to periodically review access levels. There should be an adequate and timely process in place to assure access is removed when an employee is terminated or when employees are absent for an extended period. The examiner will want to evaluate whether access level change procedures are appropriate. Administrative access to systems should be adequately restricted. Management should maintain an administrative access account and password offline in case of emergency.

Computer Systems Security

The security of computer systems should be adequately governed by formal policy and procedures. The patch management process must be sufficient to keep pace with the increasing threats to information assets. Management should also establish appropriate baselines for critical equipment. These baselines should have been addressed in a risk assessment to determine the level of risk and mitigation needs. Malware in the form of viruses, worms, Trojan horses, and key loggers are an ever present and changing threat. All institutions must have adequate malware protection.

Change Management Processes

The corporate should have a formal change management process that includes governing documents and procedures. No significant changes should be made to critical systems without formal management approval. Change management includes all hardware and software in the organization. Management should establish adequate baselines for change management.

Environmental Hazards

All critical equipment must be adequately protected by an uninterruptible power supply. The environment housing critical data processing equipment should be adequately controlled by an HVAC system. All critical equipment should be covered by a fire detection

and suppression system, preferably a chemical based system as opposed to water. The computer room should be uncluttered and free from hazards.

Business Continuity Planning

Management is responsible for developing and testing a business continuity plan (BCP) to be invoked when various levels of interruptions occur to critical information systems. The portion of the IS BCP will be integral to the enterprise-wide BCP and should be coordinated appropriately.

Examination Objectives

The objectives for reviewing the information system processing are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control data processing risk.

2. Determine that the corporate complies with the FCU Act, NCUA Rules and Regulations, NCUA issued Directives, the Accounting Manual for Federally Insured Credit Unions, and GAAP, as they directly or indirectly apply to information system processing.

3. Evaluate the adequacy of security policies relative to the risk to the institution.

4. Evaluate vendor management related security controls.

5. Assess the adequacy of the corporate's security controls.

6. Initiate corrective action when the corporate's internal IST controls, policies, procedures, and practices are deficient.

Examination Procedures

See Corporate Examination Procedures - Information Systems Processing (OCCU 303P).

Examination Questionnaire

See Corporate Examination Questionnaire - Information Systems Processing (OCCU 303Q).

References

1. NCUA Rules and Regulations
2. FFIEC Information Technology Examination Handbooks
3. FFIEC Information Security Booklet of July 2006
4. OCCU Guidance Letters