Chapter 6

INFORMATION SYSTEMS AND TECHNOLOGY

TABLE OF CONTENTS

Chapter 6

INFORMATION SYSTEMS AND TECHNOLOGY

Examination Objectives

- Evaluate management's ability to recognize, assess, monitor, and control information systems and technology (IST) related risks
- Assess whether the credit union has sufficient expertise to adequately plan, direct, and control IST operations
- Determine whether the board of directors has adopted and implemented adequate policies and procedures
- Determine whether practices comply with established policies and procedures
- Determine adequacy of internal controls and oversight to safeguard assets (including IST assets) and members' information

Associated Risks

- Transaction risk occurs when internal controls do not sufficiently detect errors, omissions, or material misstatements;
- Compliance risk occurs when inadequate systems and lack of controls affects conformity with compliance laws and regulations; and
- Strategic risk occurs when management due diligence has not sufficiently planned for unforeseen events.

Risk-Based Examination Consider-ations

When determining whether to perform a review of the IST function during an examination, examiners need to understand the associated risks of the systems (hardware and software) used by the credit union, the types of services provided, sensitivity of the data stored, and controls implemented by the credit union to protect the systems and data. Other considerations include:

- Results of the last examination;
- Recent external or internal audit results;
- Results of most recent third-party review;

- Results of the most recent risk analysis and/or penetration test, if conducted;
- Occurrence of security breaches or unauthorized access;
- Filing of a claim or a loss related to IST;
- Material change in services, key personnel, policies, or practices;
- Material change in systems (hardware or software); or
- Change in vendors which provide:
  - Critical systems or services; or
  - Support systems or services for critical systems or services.

Overview

Examiners cannot consider reviewing a credit union's IST function as a separate examination issue. Most credit unions tightly integrate their information processing activities into the functional operation of the credit union. For example, credit unions often use stand alone or personal computers connected to a network to supplement integrated IST functions for such things as audio response systems, loan application and approval functions, credit report retrieval, budgeting, payroll systems, website and e-Commerce systems. The nature and complexity of IST processing may significantly increase the potential risk exposure to disaster, error, or fraud within or outside the credit union or service bureau operation. While the fundamental concepts of internal control (e.g., separation of duties, audit trails, back-up, monitoring, and contingency plans) remain the same in either a computerized or manual system, the techniques and approach required to review these systems differ.

The examiner's primary responsibility in reviewing IST operation is to recognize the procedures and internal controls that minimize the exposure to loss and disruption of service. The following conditions may raise questions about the IST operations of the credit union:

- A board or management unaware or uninterested in IST operations and services;
- Inadequate short- and long-term planning for computer operations;
- Conversion to a new information processing system or modification of an existing system since the previous examination;
- Significant evidence of inefficiency or inaccuracy (e.g., slow daily balancing, delayed closing of books, delayed distribution of members' statements, inaccurate statements or records, etc.);

- Weak physical or internal controls; and
- Negative comments by users (internal and external) of the systems.

Many credit unions use the Internet to provide financial services to their members. This IST environment exposes a credit union to external threats that previously were not an issue (see Appendix 6A for a discussion on e-Commerce issues.) As a credit union's IST environment changes (vendor, hardware, or software), management must re-evaluate the associated risks.

NCUA does not expect examiners to perform a detailed IST review. Based on their judgment, examiners may request additional resources such as an IS&T subject matter examiner (SME), regional office analyst, or central office information systems officer (ISO) for needed assistance. When determining the additional resources required, the examiner should consider the following:

- Associated risks;
- Complexity of products and services;
- Management experience and expertise;
- Asset size; and
- IST vulnerabilities (IST related losses or claims, system penetration, unauthorized access, website defacements, etc.).

Credit unions or others (e.g., CUSOs, vendors) may occasionally ask the examiner to express an opinion concerning specific hardware or software systems for use in credit union operations. NCUA examiners will not make recommendations concerning specific information processing systems or services for purchase, lease, or contracting by credit unions. Credit unions that purchase accounting services must comply with the *NCUA Rules and Regulations*, §701.26, Credit Union Service Contracts.

Processing Environment

Based on the physical location of the computer and the degree of credit union management control over the day-to-day operation of the computer system, credit unions can classify their IST operations into two broad categories:

- **In-house processing** means the computer is located on the credit union premises and credit union management directs the day-to-day operation of the computer. Distinguishing between the two classes of in-house processing depends on the degree of credit union involvement in the programming, system design, and program maintenance efforts required for an on-going IST operation:

  - Turnkey systems are in-house processing systems for which a credit union has no direct responsibility for programming, system design, or program maintenance. Turnkey systems include both the hardware and software necessary to process credit union information. The credit union only furnishes adequate space and personnel to operate the computer; an outside party provides programming and continuing support. The vendor supplying the turnkey system may also arrange training for credit union staff using the system.

  - User-designed systems are in-house processing systems for which the individual credit union retains responsibility for programming, system design, and program maintenance. Even though the credit union may purchase the initial software for a user-designed system, the vendor or systems designer will modify it to meet the credit union's specific needs. Credit unions may purchase hardware directly from the manufacturer or a hardware vendor. The size of these systems can vary widely; they are not limited to large mainframe computers.

  Responsibility for programming and maintenance remains the primary distinction between turnkey and user-designed data processing systems.

- **Service bureau processing** refers to information processing services located away from the credit union and managed by an outside party. Credit unions can obtain service bureau processing from several sources, including:

  - Another financial institution;
  - A credit union service organization (CUSO);
  - An independent information processing vendor; or
  - The credit union's sponsor.

Regardless of the processing source, the distinguishing characteristics of outside processing include the physical separation from the credit union's operations and the absence of direct management responsibility for computer operations.

Controls

IST controls prevent, detect, correct, and enable recovery from problems that can result from accidents, errors, misuse, sabotage, loss of equipment, loss of data, and any other occurrence that may lead to an unwanted or unexpected disruption of service. The three major categories of IST controls are (1) management controls, (2) general controls, and (3) applications controls.

Management Controls

The examiner should have a good understanding of how a credit union manages its information system and services. Similar control issues exist for this area as for those generally found in other operational areas, and they require similar review procedures. Good IST management includes the following:

- Organization. A credit union should have a well-defined organizational structure that includes the IST department or service area. Ideally, credit unions should establish IST as a separate entity that reports directly to management and not through another department. The IST department should maintain an up-to-date topology (a visual representation of the hardware layout) to describe how various systems interact and share data.

- Planning. The credit union’s short- and long-term plans should identify management’s direction regarding its IST operation. Management should regularly document, update, and review these plans, which should include well-thought-out designs for installation of new systems and the modification of existing ones. Effective planning includes input from various sources such as a team with representatives from senior management, information technology, human resources or personnel, legal, and customer service. A diversified team allows for different perspectives in development of IST plans and effective policies and procedures.

- Policies and Procedures. The credit union should have well-documented policies and procedures for the IST operation. Management should review and update written procedures regularly. Documentation should reflect the actual practices at the credit union.

- Monitoring Operations. The crucial oversight function of IST operations can involve the use of committees such as an IST management committee, IST steering committee, or the supervisory committee.

- Audit. Auditing the IST area is a cost of doing business. Credit unions should require regular internal and external reviews of IST operations and services. IST audits or reviews will differ from one credit union to another based on the importance of IST services to the credit union and the credit union's size and complexity.

- External Requirements. Credit unions must comply with the laws, regulations, and guidelines of various governmental and regulatory bodies (international laws, federal and state regulations, etc.) as they pertain to the IST operations (see Appendix 6A.)

General Controls

General controls apply to areas of an information processing system not specifically related to any one application or function. General control issues exist in any automated environment and remain essential to the proper day-to-day operation of an information processing system. Proper general controls address the following issues:

- Organizational. Credit unions should establish and maintain separation of duties, a key element of any IST operation. In an IST environment, good internal controls prevent any single employee from having control over the input, processing, and output of transactions. Compensating controls, such as frequent and detailed review of transaction logs, can help offset weaknesses in this area.

  Management should also address other important concerns of an IST environment including personnel issues, such as employment procedures, job descriptions, security statements to help control data, and termination procedures.

- Systems Design, Development, Modification, Testing, and Implementation, commonly referred to as System Development Life Cycle (SDLC). Credit unions should document the methods and procedures for developing and testing new and enhanced systems. Implementing these procedures will help maintain the integrity of programmed applications.

- Data Center Management. The operation of the data center includes, among other things, the control and scheduling of input and output, problem prevention and correction, and reporting. Credit unions should thoroughly document procedures and regularly update them.

- Software Controls. Credit unions must control access to software by unauthorized persons, especially the control and use of the operating system, software utilities, communications, and security packages. Control of production application software helps ensure the system's integrity. System logs are useful tools for monitoring activity and changes to the system if management produces and reviews them regularly.

- Hardware Controls. Credit unions should document and enforce external controls on hardware such as access controls, terminal usage, and system support and service. Computers have internal hardware controls, such as validity, parity, and echo checks that most users do not see, however, these hardware controls monitor and check for proper hardware function.

- Physical Security. The computer room or area should demonstrate evidence of physical controls such as access controls and logs, fire and theft protection, terminal access controls, and protection of data files and media. Log-on procedures, such as user IDs, passwords, and physical or electronic keys may provide additional access control to the system.

- Contingency Plan. The ability to retain, restart, and replace information processing activity quickly is an important control feature of an information processing system. Keys to a well-run and controlled IST operation include a written and tested contingency plan, proper backup and recovery actions and procedures, and management's commitment to contingency planning.

Application Controls

Application controls apply to the processing of data into, through, and out of the computer system. An awareness of IST controls enhances the review of automated parts of the process. While examiners do not extensively review application controls, conditions at the credit union may warrant an applications review. In these situations, the examiner should recommend that management obtain a third-party review. Application controls consist of the following:

- Data Origination. Credit unions should design source documents for easy and accurate data input. Management should properly authorize data before staff enters it into the system. Basic controls of data origination include batch totals, control totals, turnaround documents, and retention of source documents.

- Data Input. Controls of data input involve conversion, validation, editing, error handling, and separation of duties.

- Data Processing. External data processing controls maintain the operation of the system until completion of the application processing. These controls include system start-up procedures, backup and emergency procedures, error message debugging, and system and job status reporting. Internal processing validation and editing routines built into the programming check for errors. Upon completion of processing, the credit union should have in place error handling procedures to identify and correct transaction errors.

- Data Output. Management or staff should use all output from the system. Balancing and reconciliation, distribution, error handling, and records retention procedures (see *NCUA Rules & Regulations* §749 - Records Preservation Program And Record Retention Appendix) complete the application processing function.

Backup and Recovery

A multitude of problems that may cause breakdown, damage and other detrimental effects can plague computer systems. Users may question the integrity of the data in the system when problems occur. Credit unions must regularly and routinely back up computer data. Following are several considerations involved in the backup and recovery of computer information:

- Frequency. Credit unions should back up (1) data files at least daily; (2) application files both when they make changes and routinely, usually monthly or quarterly; (3) a current copy of the operating system, and (4) vital records every three months.

- Generations. Credit unions should have available at least three generations of backups; however, many credit unions keep five sets of data file backups, one made on each day of the week.

- Storage. Credit unions must store vital records offsite, at a location far enough from the credit union's offices, to avoid the simultaneous loss of both sets of records. Credit unions should keep backup files both on- and off-site, one set of backups at each location, in order to facilitate recovery of operations should an event occur.

- Management. Credit unions should routinely control, maintain, and test backup files for quality and accuracy.

- Recovery. Credit unions should address and document relevant issues such as the speed of data file recovery, who can recover them, and under what conditions.

Contingency Planning

Restoring operations to an acceptable level within a reasonable amount of time requires that all credit unions using any type of IST services have a comprehensive, written, accurate, up-to-date, tested contingency plan. Responsibility for developing this plan lies with management. The examiner may review the contingency plan during each examination.

Credit unions should develop detailed contingency plans. These plans should take into account local as well as region-wide disasters. Contingency plans should also consider any single point of failure issues (such as telecommunication and data lines, electrical services, etc.) Management should routinely test the contingency plan and document the results of those tests. Where the testing process identifies a failure or weakness, management should correct those issues and retest the plan. Management should ensure the contingency plan addresses the following considerations:

- Notification and contact procedures (staff, vendors, federal agencies, state agencies, local authorities, members, other appropriate third parties, etc.);
- Hardware and software requirements and needs;
- Timeframes, including acceptable downtime for the credit union and the time needed to bring processing services up after a disaster;
- Critical, priority, and support systems;
- Backup and recovery of operating system, application software, and data files;
- Current written documentation;
- Alternative sites for processing;
- Communications needs (telephone lines, fax capabilities, cell phones, data lines (T1, T3, fiber optic, etc.) and capabilities (bandwidth and throughput);
- Employees' knowledge (understanding of their duties and needs) and training;
- Administrative needs and supplies;
- Insurance coverage and requirements;
- Security for the credit union and the alternative sites; and
- Testing.

Examination and Audits

The examination and audits of the information processing and services, including both internal and external reviews, give the credit union assurance that the system’s design and operation function as intended. Internally, the credit union should perform, at a minimum, quality and accuracy checks on the system’s processing to ensure the presence of at least the minimum control requirements for the type of system in use. Depending on its size, type of system, and complexity, a credit union may need a complete third-party audit. Larger credit unions may need an internal IST auditor to perform routine, recurring reviews of the system.

Based on the risk-focused examination considerations discussed earlier in this chapter, examiners may perform some level of IST review during the examinations of credit unions having automated systems. Most credit unions rely on automated systems. Many credit unions could not operate at their present service level without these systems. The audit software available in AIRES allows for sampling and querying share and loan data. A download from the credit union's system helps the examiner analyze the data in the computer system by allowing the examiner to compare AIRES results with the credit union's reports. Examiners can review records for quality, completeness, and accuracy. Additionally, examiners can compare data from separate sources for consistency, and can summarize and sort data in various ways.

During the IST review, examiners should perform a review of IST management and general controls. Examiners can address review results in one or more of the following ways:

- No recommendations, based on the quality and acceptability of the review;
- Recommendation that management improve certain areas of the IST operation or services;
- Recommendation that management obtain a partial or complete third-party review; or
- Notification to the supervisory examiner of extensive problems in the system.

Effect of IST on the Auditor's Consideration of Internal Controls in a Financial Statement Audit

This section provides guidance on how the credit union's use of IST may affect internal controls relevant to the financial statement audit, the auditor's understanding of internal controls, and the assessment of control risk relative to IST.

The audit standards assert that the more complex the IST environment at a credit union, the higher the assessment of control risk and the more control testing the examiner should see in the audit documentation on internal controls regarding IST.

Generally accepted auditing standards (GAAS) state:

> When evidence of an entity's initiation, recording, or processing of financial data exists only in electronic form, the auditor's ability to obtain the desired assurance only from substantive tests[1] would significantly diminish.

Therefore, auditors should rely less on substantive tests and more on tests of controls as levels of automation increase. Consequently, the examiner should see an audit strategy designed to perform a greater degree of control testing to ensure the effectiveness of the controls. Examples of control testing can include:

- Testing system edits (e.g., posting rejects to non-existent accounts);
- Exception reporting (e.g., paid-ahead loan report or loans over a dollar limit);
- Testing authorization limits (e.g., wire transfers); and
- Testing security codes and structure (e.g., system rights).

The effect of IST on a credit union's internal controls relates more to the nature and complexity of the systems in use than to the credit union's size. Based on the complexity of the credit union, the examiner should review the audit scope or otherwise determine that the auditor considered the following:

- The adequacy of internal controls given the level and complexity of IST. For example, the credit union may have complex and highly integrated systems that share data for reporting, operations, and compliance objectives. Other examples include multiple user environment accessing a common database, web operations, or a shift from paper to an automated system.

- The types of controls significant to the audit and the testing of those controls. These may include authorization controls, reporting limits, controls to initiate transactions, security levels, and backup procedures.

- Whether the auditor used individuals with specialized knowledge. Determinants include the complexity of the system, extent of changes to existing systems, establishment of new systems, extent

[1] Independent tests that are quantitative in nature performed to support a financial statement assertion or contention.

of data sharing, and availability of audit evidence existing only in electronic form.

- The auditor’s understanding of the financial reporting process. Typically, within the audit documentation for more complex credit unions, the examiner would find a system diagram, schematic, or questionnaire denoting the data flow from initiation to reporting with control points identified allowing the auditor to pinpoint potential weaknesses.

The audit scope and program must assess and address IST risks or it may be considered inadequate.

Service Bureaus

Credit unions that use service bureau operations (also called service centers) to process their information have many of the same responsibilities as those using in-house services. Management can make a serious mistake by relying heavily on a service bureau without providing adequate oversight. Management should recognize and monitor important issues including ownership and control of data, timeliness, accuracy and completeness of information processing functions, contractual obligations, contingency planning, backup and recovery of data files, financial stability of the service bureau, and service bureau audits (financial, SAS 70, etc.)

Examiners should pay particular attention to the contract between the service bureau and the credit union. A written contract must specify responsibilities of both parties. Credit union management must understand the contents of the contract with the service bureau. The provisions often contained in an IST service contract include:

- Specific work that the service bureau agrees to perform, and the frequency and general contents of the related reports;
- The basis of costs, including development, conversion, and processing, together with additional charges for special requests;
- Established time schedules for receipt and delivery of work;
- Audit responsibility, including the right of user representatives to perform audit procedures (such as a SAS 70 Report);

- Backup and record protection provisions (equipment, program, and data files) to ensure timely processing by the service bureau in emergencies;
- Establishment of liability for source documents while in transit to and from the service center (the service center should have adequate insurance coverage for those liabilities for which it bears responsibility);
- Maintenance of adequate insurance for data losses from errors and omissions;
- Confidential treatment of records;
- Ongoing compliance with federal regulations;
- Ownership and escrow of computer programs and related documentation;
- Ownership of master and transaction data files and their return in machine-readable format upon the termination of the contract or agreement;
- Price changes, cost and method of cancellation of the contract, or withdrawal from the servicing arrangement by either party, including adequate time allowance;
- Notification from the service center to the users of all systems of changes that would affect procedures, reports, etc.; and
- Financial information that the service bureau agrees to provide periodically (preferably at least annually) to credit unions.

Outsourcing

Credit unions often rely on third parties to provide and support technology-related functions and services. Outsourcing arrangements can help manage costs, provide expertise, and expand and improve services offered to members. The credit union may outsource the system or service; however, management ultimately remains responsible for managing the risks associated with the system or service. The following four key points pertain to managing outsourced technology:

- The board of directors and senior management bear responsibility for understanding the risks associated with outsourcing arrangements for technology services and ensuring implementation of effective risk management strategies and practices;

- Once the credit union has completed its risk assessment and determined its risk acceptance level, management should evaluate service providers to determine their operational and financial abilities to meet the credit union's needs;

- Credit unions should require clearly written and sufficiently detailed contracts that provide assurances for performance, reliability, security, confidentiality, and reporting; and

- Credit unions should implement an oversight program to monitor each service provider's operations and controls, financial condition, and performance standards.

(For a more in depth discussion on outsourcing, see NCUA Letter #00-CU-11, *Risk Management of Outsourced Technology Services*.)

Security and Privacy

NCUA developed the security and privacy guidelines in §716 and revised §748 of the *NCUA Rules & Regulations* in response to the Gramm-Leach-Bliley Act (GLBA).

Security

NCUA Rules and Regulations §748.0 requires each federally-insured credit union to develop a written security program. This program must strive to:

- Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;
- Ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;
- Assist in the identification of persons who commit or attempt such actions and crimes; and
- Prevent destruction of vital records, as defined in §749.

The appendix to §748 provides guidelines to assist credit unions in meeting the above four criteria. The guidelines, while not mandatory, provide a good framework from which credit unions can work to develop their policies and procedures.

Security Policies and Procedures

Credit unions may find the following considerations useful when developing security policies and procedures:

- Identifying the services provided and systems (hardware and software) used;
- Identifying the risks and threats associated with each system and service;
- Determining the likelihood the risk or threat could occur;
- Identifying and evaluating various methodologies to mitigate the risks or threats;
- Developing the policies and procedures to address the risks or threats;
- Monitoring, and adjusting if necessary, the policies and procedures to achieve the desired results;
- Reviewing policies and procedures at least annually; and
- Training and educating staff.

Though not required, credit unions should establish a security team assigned with the responsibility of developing, implementing, monitoring, and revising security policies and procedures. Team members should include representatives from senior management, information technology department, human resources or personnel department, legal department, and customer service department. A diversified team will provide input from different perspectives in development of effective policies and procedures (see *NCUA Rules and Regulations* §748 and Appendix).

If a credit union demonstrates a weakness in one or more of the preceding steps, examiners should address that concern in a manner consistent with the risk and potential effect on the credit union.

Privacy

Credit unions must ensure their IST policies, procedures, practices, systems design, and operations comply with the privacy requirements in *NCUA Rules and Regulations* §716 (see NCUA Letter #01-CU-02, *Privacy of Consumer Financial Information* for a detailed discussion.)

Credit unions must also work with their vendors to ensure that their vendors comply with the credit union's privacy statements.

IS&T Questionnaires

AIRES contains three questionnaires to assist the examiner in performing and documenting the IST review. The purpose and description of each questionnaire is:

- e-Commerce I (EC1). EC1 is a high-level questionnaire designed to assist examiners in their review of credit union e-commerce services. EC1 primarily focuses on credit union management's actions regarding the planning, implementation, and oversight of e-commerce systems and services;

- e-Commerce II (EC2). EC2 is a detailed questionnaire designed to assist examiners in conducting an in-depth review of e-commerce systems and services. Generally, examiners use EC2 when the results of EC1 indicate problems or issues exist which, in the examiner's judgment, warrants further review. EC1 and EC2 have eleven identical major sections allowing examiners to identify concerns using EC1 and then use the corresponding section in EC2 to perform additional examination procedures as warranted. Examiners also use EC2 in large and complex credit unions; and

- Electronic Data Processing Review (EDPR). EDPR is a technical questionnaire designed to assist examiners in their review of credit union IST systems. Generally, examiners use EDPR when they wish to perform a review of a credit union's automated systems (not just e-Commerce) or, when in their judgment, a review is warranted due to:

  - Significant weaknesses noted in IST areas;
  - Lack of an adequate internal or external review program for IST systems;
  - Lack of adequate management oversight, risk analysis, or risk control;
  - Lack of adequate policies, procedures, and practices; or
  - EC1 and/or EC2 review results reveal IST concerns regarding e-Commerce systems and services (if concerns exists for e-

Commerce systems and services, similar concerns may exist for core processing systems and services.)

CAMEL Impact

Examiners should use the Management component of the CAMEL rating to address IST concerns. As part of this assessment, examiners should consider the following:

- Strategic Plan & Goals:
  - Has management developed a strategic plan for the credit union's IST systems and services?
  - Has management developed strategic goals, policies, and procedures to implement the strategic plan?
  - Are those strategic goals, policies, and procedures adequate in relation to the following:

    i. Size and complexity of the credit union;
    ii. Type of services offered;
    iii. Volume of IST activity;
    iv. Member demand, usage, and expectations; and
    v. Criticality[2] of systems and services?

- Risk Analysis:
  - Has management performed a risk analysis? If so, does the analysis include the following components:

    i. Assessment;
    ii. Impact analysis/evaluation;
    iii. Mitigation;
    iv. On-going/periodic monitoring; and
    v. Reporting procedures?

[2] Management should determine whether IST systems and services are critical or non-critical to the credit union's operations. Management should base this determination on factors such as, but not limited to, the following: risk exposure (transaction, security, compliance, etc.), type of services offered, transaction volume (number and dollar), interconnectivity impact with other credit union technology systems, member usage, and member expectations and perceptions.

- Policies:

  - Has management developed appropriate and adequate policies that address the following:

    i. Security;
    ii. Compliance;
    iii. Business continuity/resumption;
    iv. Disaster recovery; and
    v. Vendor management?

- Oversight:

  - Does management provide adequate oversight including:

    i. Adequate staffing;
    ii. Knowledgeable/informed staff (in IST activities); and
    iii. Adequate reporting procedures at various management levels?

  - Has the internal and/or external review program been modified to include reviewing procedures for IST activities?

  - Does management address issues/concerns effectively, adequately, and timely?

  - Does management have adequate vendor oversight policies, procedures, and practices?

Workpapers and References

- Workpapers
  - Electronic Data Processing Review (EDPR)
  - E-Commerce I (EC1)
  - E-Commerce II (EC2)
- References
  - Federal Laws/Regulations
    - ▪ Computer Fraud and Abuse Act (CFAA)
    - ▪ Electronic Funds Transfer Act (EFTA, REG E)
    - ▪ Expedited Funds Availability Act (EFAA, REG CC)
    - ▪ Child On-Line Privacy Protection Act (COPPA)
    - ▪ Gramm-Leach-Bliley Act (GLBA)

  - Electronic Signatures in Global and National Commerce Act (E-Sign)

- *NCUA Rules and Regulations*
  - 701.26 - Credit Union Service Contracts
  - 712 - Credit Union Service Organizations
  - 716 - Privacy of Consumer Financial Information
  - 721 - Federal Credit Union Incidental Powers
  - 748 - Credit Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance
  - 749 - Records Preservation Program And Record Retention Appendix

- Regulatory Alerts
  - 01-RA-07 *Children's Online Privacy Protection Act* (COOPA)
  - 01-RA-06 *Regulation E (Electronic Fund Transfers)*
  - 01-RA-03 *Electronic Signatures in Global and National Commerce Act (E-Sign Act)*
  - 00-RA-01 *Electronic Transfers Accounts*
  - 98-RA-08 *Electronic Transfer Act*
  - 98-RA-04 *Interagency Guidance on Electronic Financial Services and Consumer Compliance*
  - 97-RA-12 *Guidance for Reporting Computer-Related Crimes*

- Letters to Credit Unions
  - 01-CU-04 *Integrating Financial Services and Emerging Technology*
  - 01-CU-02 *Privacy of Consumer Financial Information*
  - 00-CU-11 *Risk Management of Outsourced Technology Services*
  - 00-CU-09 *AIRES 2000 Loan and Share Record Layout Specifications*
  - 00-CU-07 *NCUA's Information Systems & Technology Examination Program*
  - 00-CU-04 *Suspicious Activity Reporting*
  - 00-CU-02 *Identity Theft Prevention*
  - 98-CU-12 *Business Resumption Contingency Planning*
  - 98-CU-02 *Year 2000 Contingency Planning*

  - 97-CU-05 *Interagency Statement on Retail On-line PC Banking*
  - 97-CU-03 *Corporate Business Resumption and Contingency Planning*
  - 97-CU-01 *Automated Response System Controls*
  - 96-CU-04 *Internal Control Structure*
  - 109 *Information Processing Issues*

- *Accounting Manual for Federal Credit Unions*

- Statement of Auditing Standards (SAS) No. 94

- *FFIEC Information Systems Examination Handbook*

- Websites
  - Cybercrime: http://www.cybercrime.gov/
  - Computer Crime and Intellectual Property Section (CCIPS): http://www.usdoj.gov/criminal/cybercrime/compcrime.html #CC
  - Federal Computer Incident Response (FedCIRC): http://www.fedcirc.gov/
  - Financial Crimes Enforcement Network (FinCen): http://www.treas.gov/fincen/
  - Federal Trade Commission (FTC): http://www.ftc.gov/
  - Internet Fraud Complaint Center (IFCC): https://www.ifccfbi.gov/
  - National Infrastructure Protection Center (NIPC): http://www.nipc.gov/
  - Electronic Privacy Information Center (EPIC): http://www.epic.org/
  - Incidents.org-By The SANS Institute: http://www.incidents.org/
  - Internet Security Systems, Inc.: http://www.iss.net/
  - National Institute of Standards and Technology Resource Center: http://csrc.ncsl.nist.gov/
  - SecurityFocus (BugTraq): http://www.securityfocus.com/
  - CERT® Coordination Center: http://www.cert.org/
  - Internet Fraud (IFW): http://www.fraud.org/internet/intset.htm

- Information Technology Association of America: http://www.itaa.org/
- SANS Institute Online: http://www.sans.org/newlook/home.htm
- Security & Exchange Commission-Division of Enforcement - Complaint Center: http://www.sec.gov/enforce/comctr.htm

INTERNET AND e-COMMERCE - APPENDIX 6A

Overview

Many credit unions offer services to members via electronic means, often through the Internet and World Wide Web. Electronic financial services pose inherent risks to credit unions. Management must understand those risks and take measures to mitigate them.

Electronic financial services (EFS) comprise those services that a credit union provides via electronic means including, but not limited to, the following:

- Electronic Commerce Systems and Services:
  - Internet/World Wide Web services;
  - Home Banking (direct dial in) Services;
  - Wireless Services;
  - Audio Response/Phone Based;
  - Kiosk; and
  - e-Commerce Account Transaction Processing Services. Online e-Commerce account services include, but are not limited to, the following:

    i. Account Inquiry;
    ii. Check Order Requests;
    iii. Loan Applications;
    iv. Bill Payment;
    v. Funds Transfers;
    vi. Third-Party Transfers;
    vii. Stop Payment Requests;
    viii. On-Line Wire Transfers;
    ix. Automated Clearing House (ACH) Originations; and
    x. Account Aggregation/Screen Scraping.[1]

[1] Account aggregation and screen scraping are two different methods used to gather user account information from various sources and then compile that information in one location for the user.

- Electronic Payment Systems:

    - ACH Transactions;
    - Stored Value Cards;
    - Electronic Money; and
    - Electronic Wallets.

- ATM Systems.

There are three types of website systems:

- Informational. An Informational system displays general information such as loan/share rates, credit union contact information, and privacy notices;

- Interactive. An Interactive system contains features of an Informational website plus members can request information such as share balances, loan balances, account statements, and disclosure statements. Members can complete loan applications, member applications, share account applications, etc.; and

- Transactional. A Transactional system contains features of an Interactive website plus members can initiate and perform transactions such as paying bills, making loan payments, transferring money or funds (between one or more credit union accounts; between the credit union and third-parties), and opening new share accounts.

The introduction of website services (whether hosted internally or externally) exposes a credit union to increased risk. In addition, the type of website affects the level of risk the credit union assumes (i.e., transactional websites generally have a higher level of risk than an interactive website.)

The following four tools will assist examiners in their risk-based approach to evaluating credit union management in the area of electronic financial services:

- e-Commerce I (EC1) - high level e-Commerce questionnaire;
- e-Commerce II (EC2) - detailed review program for reviewing a credit union's e-Commerce activities;
- EDP Review (EDPR) - Electronic Data Processing Review Program for reviewing a credit union's overall information and technology systems; and
- Computer Desktop Encyclopedia computer disk.

AIRES contains the first three tools. The Computer Desktop Encyclopedia is on a computer disk with updates issued periodically throughout the year.

Threats and Vulnerabilities

Credit unions that provide web-based services face additional threats and vulnerabilities. Generally, these concerns arise because the credit union has adopted an "open environment." This is one in which external parties have access to one or more of the credit union's internal systems. Typical threats and vulnerabilities associated with the Internet and web-based services include:

- Eavesdropping or Packet Sniffing;
- Snooping or Downloading;
- Tampering;
- Spoofing;
- Jamming or Flooding (Distributed Denial of Service (DDoS));
- Injecting Malicious Code (viruses and Trojan Horses);
- Exploiting Flaws; and
- Cracking.

Effective policies, procedures, and practices, which address the following, provide the best way to deal with these threats and vulnerabilities:

- Risks assessments;
- Security measures;
- Monitoring requirements;
- Incident response procedures;
- Vendor oversight; and
- Contingency planning and business resumption contingency planning.

Risk Assessments

The credit union should have implemented a risk assessment procedure that enables it to do the following:

- Identify the threats and vulnerabilities;
- Assess the risk (likelihood of occurrence and effect on credit union);
- Establish risk tolerance thresholds (how much given risk is the credit union willing to assume);
- Implement risk mitigation strategies; and
- Monitor and adjust, as needed, risk mitigation strategies on a regular basis.

Security Measures

The types of security measures a credit union employs depends on the types of systems and services it provides, the complexity of those systems and services, the credit union's risk tolerance thresholds, and the experience of IST management. *NCUA Rules & Regulations* §748 delineates the security requirements credit unions must meet and provides guidelines they may employ to meet those requirements. A business decision by the board addresses how the credit union will implement security for its systems and data. When providing web-based services, best practices suggests using the following:

- Routers (to route data to the appropriate destination);
- Firewalls (to filter incoming and outgoing traffic);
- Virus protection (to prevent or control viruses and Trojan horses);
- Intrusion detection (to alert management when an intruder is attempting to breach, or successfully has breached, the credit union's perimeter security systems);
- Vulnerability assessments and penetration testing (to identify and determine weaknesses associated with individual systems and the IST environment as a whole);
- Security bulletin and alert monitoring (to remain aware of new security issues and install new updates and patches in a timely manner);
- Incident response procedures and employee training (to limit damage once an incident has occurred); and
- Vendor oversight program (to ensure vendors and contracts meet the credit union's minimum requirements.)

Monitoring Requirements

Each credit union should establish monitoring requirements for all phases of its IST activities, from monitoring internal systems (e.g., systems log reviews) to monitoring the operations of the vendors. Monitoring procedures allow a credit union to determine what works and what does not. This provides management the ability to make appropriate adjustments to policies, procedures, and practices.

Incident Response Procedures

The credit union's incident response plan should provide assurance that the credit union has the ability to deal with various types of incidents within reasonable timeframes, thus minimizing the risk of loss. Key factors for dealing with incidents include (1) what action to take, (2) when to take it, and (3) how to implement that action. The amount of detail in a credit union's incident response plan should relate to the size of the credit union, the complexity of its operations, and the structure of its IST environment. For example, a credit union operating in a complex in-house developed IST environment would have a different incident response plan from a credit union solely operating in an outsourced environment.

Vendor Oversight

A credit union should establish a vendor oversight program that ensures its vendors meet pre-established criteria such as security and privacy. The credit union should carefully review its vendor contracts to ascertain each party's rights and obligations and to ensure that service level agreements meet the credit union's expectations and needs. If available, credit unions should obtain and review vendor financial statements to determine the short- and long-term viability of their vendors. The credit union should decide whether obtaining a copy of a vendor's SAS 70 or other audit report (if available) would assist in determining the quality of the vendor's management, various controls, policies, procedures, and practices. Credit unions should regularly communicate with their vendors to obtain current information regarding the vendors' hardware and software systems.

Contingency Planning and Business Resumption

A credit union should determine the importance of its web-based services and products to its operations. Based on the level of criticality, the credit union needs to develop appropriate procedures to ensure an incident or disaster will minimally impact, or impact only to a predetermined acceptable level, member services and credit union operations. Occurrence of an incident or disaster can result in significant harm. Therefore, credit unions should address not only the disruption of services and potential financial loss (volume and dollar transactions), but also the long-term costs to their members, the credit union, and the industry.

Bond Insurance Coverage

Credit unions should have implemented a risk management program to manage the risks inherent in their operations. Insurance can play a role in mitigating risks to an acceptable level so the credit union can achieve its strategic objectives.

NCUA Rules and Regulations §713, Fidelity Bond and Insurance Coverage for Federal Credit Unions, requires that each federal credit union board review its insurance coverage for adequacy in relation to the potential risks facing the credit union. The board must review the insurance coverage at least annually. A thorough risk assessment process would help determine the adequacy of the coverage in relation to the credit union's activities, including e-Commerce.

A credit union should reevaluate insurance needs whenever it considers a new product, service, or vendor relationship. These may introduce new risks for which insurance coverage may require modification.

Risks associated with e-Commerce are wide-ranging. An insurance carrier's product offerings may cover these risks in various places such as the fidelity bond, electronic computer crime coverage, and other optional coverage. The credit union and, if necessary, the examiner should review each type of coverage closely to determine its adequacy in relation to the credit union's risk exposure. The following types of insurance may cover EDP activities:

- Fidelity bond coverage principally covers the direct loss due to a physical crime such as theft of certain defined property (e.g., negotiable items) stolen by a first party (e.g., employee from an employer);

- Electronic computer crime coverage fills some of the gaps in fidelity bond coverage. It typically covers the direct loss due to an electronic computer crime resulting in the loss of defined property (e.g., negotiable items). Moreover, it can cover the risk of viruses and the manipulation or destruction of data and programs; and

- Other optional coverage fills some of the gaps in the fidelity and electronic computer crime coverage. These may cover indirect losses (e.g., business interruption or resumption and extortion) and expand defined property to include confidential member and credit union data. Some may cover additional related liabilities or expenses (even in relation to external service providers and litigation.)

Coverage varies among insurance carriers. Moreover, carriers often bundle their insurance offerings in different packages with unique marketing names. The coverage afforded by these policies may change in the future based on the insurance industry's perceived risk and claims experience.