Introduction to Information Technology

(This section substantially repeats the information provided in Section 341 of the OTS Thrift Activities Handbook.)

Savings associations are becoming increasingly dependent on the use of information technology (IT). Such dependence presents risks to the financial condition and operating performance of the institution that management and the board of directors must effectively manage. Accordingly, in a risk-focused supervision framework, examiners must consider the risks associated with information technology in evaluating the institution's trust and asset management activities and the effectiveness of the risk management process. Significant negative findings should be referred to the OTS regional office and the manager of the IT examination function.

Increasingly, savings associations are focusing on opportunities presented by electronic services, the Internet and the World Wide Web in an effort to remain competitive, improve customer service and reduce operating costs. Consequently, the electronic environment and technology employed by savings associations in connection with the products and services it offers is continually and rapidly evolving. Whether the institution's deployment of technology is limited to the use of personal computers (PCs) or has been expanded to include transactional capabilities over the Internet or account aggregation services for customers, the rapid pace of change in technology calls for increased examiner attention to the IT function.

Regardless of the level of sophistication, risks are inherent in all electronic capabilities. Threats can come from both internal and external sources. Outside hackers, disgruntled employees and inadvertent errors can adversely affect IT reliability. For instance, unauthorized parties may alter an information-only World Wide Web site used for advertising purposes. Electronic mail containing confidential or proprietary information may be accessed or distributed in error. Unauthorized parties might access networked systems that are directly connected to a savings association's main operations database. If these risks are not recognized and the subsequent problems promptly detected and addressed, they can lead to significant monetary and reputational losses for a savings association.

Operating Environment

Savings associations have a number of choices available to meet their constantly changing and evolving information system and technology needs. Most savings associations use one or more of the following sources to deploy and operate systems and technology:

- Personal computers and local and wide area networks
- An in-house computer center and client server system
- Outsourced vendors

A savings association's decision to select the appropriate information technology strategy can depend on several factors:

- In-house expertise;
- Capital to acquire the necessary resources;
- Facilities to house the resources;
- Cost of outsourcing to vendors; and
- Management’s ability and willingness to use information technology to build a competitive advantage within a safe, sound and secure infrastructure.

Personal Computers and Local and Wide Area Networks

The personal computer has become a prominent tool in today’s business environment. It is used in information processing in either a stand-alone or network arrangement. Local and wide area networks of PCs have offered substantial benefits in productivity and information access. Institutions growing use of PCs to deploy new technology is dependent on a network environment. The electronic network facilitates interaction between the savings association and the users (staff and customers). Telephone banking, PC banking, automated teller machines, automatic bill payments, and automated clearinghouse systems for direct deposit or payment, are familiar examples of existing and evolving services that savings associations can offer to their customers through an electronic network. Such access, however, also means that those control procedures, previously limited to the central operations, must be reapplied and extended to the PC user level.

Basic controls and supervision of PCs often have not been introduced or expected at the PC user level. The technological advantages, expediency and cost benefits of the PC have been the primary focus. Recognition of the increased exposure has not kept up with the demand for expanded information processing power.

While each PC requires certain operational type controls such as physical security (lock and key), logical security (password) and file backup, the more pronounced risks involve those operations using PCs as stand-alone processors.

PC users frequently engage in program development directly on their desktop computers. This may involve the original creation of a software program or the customization of existing routines from vendor software. With both methods, adequate control techniques for the programming, testing and documentation are necessary to ensure the integrity of the software and the production of accurate data.

PC users can also perform other functions separate from any centralized operating controls. For example, users can download and manipulate information from main databases. They can also originate data. Each of these activities can create information that management will use in making decisions that affect corporate strategies and customer relationships. Therefore, the evolution of the PC-based system has not eliminated the need for adequate operating controls. Rather, the focus of control was shifted to the PC user level.

In-house Computer Centers and Client Server Systems

In-house computer centers vary in size and complexity, type and number of data processing professionals, number and types of applications processed, transaction volume, and processing deadlines. Computer equipment may vary in size from large “mainframe” to smaller microcomputer systems. For example, in-house information systems used to generate revenues, such as loan origination systems, are frequently operated on microcomputer-based systems. Software for in-house computer systems may be purchased or licensed from outside vendors or developed internally.

Less expensive and faster computers have resulted in the emergence of client server technology. While stand-alone mainframe or personal computers make it difficult to share information with other information systems, client server technology allows a savings association to link multiple computers together to provide enough power to allocate data processing capabilities to a network. High-speed data transmission and network file servers are common characteristics in a client server computing environment.

Outsourcing

Some savings associations may determine that their need of information technology is too sophisticated or dynamic for effective support by internal resources. These institutions may determine that some or all of their technology needs should be outsourced to a facilities management company, service bureau or other third-party contractor.

This delegation does not lessen the burden on management to supervise and control all aspects of the savings associations' IT activities. An institution's delegation of responsibilities through outsourcing requires reasonable due diligence efforts throughout the term of the engagement. Conditions, rights and responsibilities of the savings association and the vendor should be governed by written agreements. This is particularly important in an electronic environment because short-term engagements, new developments and untested entities are not uncommon. Further, management must coordinate all outsourcing arrangements to ensure that security, reliability and integrity are not compromised. Examiners should ensure that all outsourcing arrangements are executed with the same access, control, monitoring and reporting environment that would be expected for a savings association with proprietary systems.

Service Bureau

Service bureaus provide standardized information system services to multiple institutions. They are common among smaller savings associations with a limited number of customer accounts and low transaction volume. Due to the costs and technical resources required to maintain an in-house computer center, some larger savings associations also find service bureaus a cost-effective alternative. Service bureaus provide the savings association with experience, proven software and reliable hardware.

Typically, data is forwarded to the service bureau computer center via on-line data entry terminals or by tape, diskette or paper copy transported by courier. Output reports are returned to the savings association in the same manner. A regulator appointed by the FFIEC examines major service bureaus providing service to federally regulated financial institutions. Savings associations should ensure they receive copies of the service bureau's IT examination report.

Contracts

When employing the services of an outside vendor, management should carefully review any proposed service contracts or agreements with an eye toward minimizing the savings association's exposure to risk. The guidelines listed below should be considered when executing any contract with an outside vendor. In addition, the savings association's legal counsel should review the draft contract to determine that the interests of the institution are adequately protected. Some guidelines when contracting with an outside vendor are to:

- Consider the following points prior to entering into any service arrangement:
    - Alternative vendors and related costs
    - Financial stability of the vendor
    - Requirements for termination of service
    - Quality of the service provided
- Ensure that any contract specifies the duties and responsibilities of the savings association and the service provider.
- Review the contract's penalty provisions for reasonableness in the areas of contract length, fees and compensation of the savings association for loss of income.
- Ensure that the following items are included in the service contracts:
    - The service provider agrees to submit to an examination by OTS, which will evaluate and monitor the soundness of the provider in order to limit the savings association's risk. Specifically, the following language should be incorporated in the contract:

        > "By entering into this agreement, the service provider agrees that the Office of Thrift Supervision will have the authority and responsibility provided to the other regulatory agencies pursuant to the Bank Service Corporation Act, 12 U.S.C. 1867(C) relating to services performed by contract or otherwise."

    - The service provider provides the OTS regional director of the region in which the data processing center is located, a copy of any current third-party review and the current audited financial statements.
    - The service provider agrees to release the information necessary to allow the savings association to develop a contingency plan that will work in concert with the service provider's plan.

Management Controls for Evaluating and Controlling Risks

Savings associations should adopt a risk management program to address unique aspects of an electronic environment. While most deficiencies in information technology tend to be directly related to operational risk, information technology also can affect other business risks (credit, market, financial, legal and reputation) depending upon the specific circumstances. Information technology elements should be viewed in an integrated manner with the overall business risks of the institution and its business lines and products. A deficiency in any one of the IT elements could have a substantive adverse effect on the institution.

The risk-focused supervisory process places emphasis on the evaluation of information technology and its effect on an institution's trust and asset management operations. Accordingly, examiners should specifically consider information technology when developing risk assessment and supervisory plans. They should determine the appropriate level of review of IT activities given the characteristics, size and business activities of the institution. In general, examiners should:

- Develop a broad understanding of the institution's approach, strategy and structure with regard to information technology. This requires a determination of the role and importance of information technology to the institution and any unique characteristics or issues.

- Incorporate an analysis of information technology systems into risk assessments and action plans. The analysis should include identification of critical information technology systems, related management responsibility and the major technology components. An organization's information technology systems should be considered in relation to the size, activities and complexity of the organization, as well as the degree of reliance on these systems.
- Assess the institution's critical systems, that is, those that support trust and asset management activities and the degree of reliance those activities have on information technology systems. The level of review should be sufficient to determine that the systems are delivering the services necessary for the institution to conduct its business in a safe and sound manner.
- Determine whether the board of directors and senior management are adequately identifying and controlling the significant risks associated with information technology for its trust and asset management business line.

An effective risk management control program will minimize the negative effects of a problem situation. Minimizing the potentially negative effects can be particularly difficult in an electronic environment that offers speed, sophistication and access to many users, regardless of their legitimacy. Further, because systems will likely affect all activities to one degree or another, a single problem can have an effect on several areas including product management, marketing, customer service and operations.

For instance, electronic advertising can provide information about products, services, rates and fees. Incorrect information can lead to customer complaints, contingent liabilities or lost opportunities and income. As a result of unauthorized system access, content may be altered to include inappropriate material that can be viewed by the general public. If the savings association has weak controls and security, users may be able to access, disclose or improperly use confidential information.

Practices to Control Risks

- Input and Output Controls

  Control practices that govern input and use of information are important to safeguard. Historically, control weaknesses have contributed to fraud and recordkeeping problems. Most operational charge-offs can be traced to problems related to the input and use of information.

  A savings association should require specific data controls for technology that is used to process information that has a direct monetary effect on the institution or its trust and asset management customers. At a minimum, these controls should include the requirement that there be a segregation of duties between the input of information and the review of that information after it is processed. Such controls should also require the reviewer to reconcile the processed information. Institutions should require that most functions relating to processing assets be performed under dual control. Appropriate controls should be established in the early stages of development and deployment and described in detail in the savings association's operating policies and procedures.

  The savings association should also establish data editing routines to help ensure that data entering a system is error-free. This control is important whether the data is being manually entered or electronically transferred from another system.

- Information Security

  The savings association should have a security system in place that controls access by unauthorized internal or external users. With the increasing use of personal computers and local and wide area networks, it is possible for an institution to expand access to applications and data to all staff. As the number of users increases, however, so does the threat of unauthorized use. Similarly, activities conducted through other interactive devices, such as the Internet, automated teller machines, telephones and televisions, open the computer system to outside and potentially unauthorized users. Although the access devices and distribution channels vary, the issues are the same regardless of the type of access device or distribution channel.

Management should control access to prevent a security compromise of its systems. Data is particularly vulnerable to unauthorized access or alteration during transmission over public networks. Management should develop methods to maintain confidentiality, ensure that the intended person receives accurate information and prevent eavesdropping by others. In addition, evidence of participation by both the sender and the receiver in a transaction should be created.

Effective security does not rely on one solution, but on several measures that, together, serve to identify and control risk. Although not all-inclusive, the following potential risks and mitigating controls should be considered in developing a system security program:

Authorization: Authorization involves the predetermination of permissible activities. Management should ensure that customers have access only to their own accounts and perform only authorized functions.

Access Controls: Traditional access controls, such as user identification, passwords and personal identification numbers, should be implemented for all users. However, since the effectiveness of these controls is greatly influenced by the user, management should take all possible steps to educate the user in this area. For example, new users typically use their name or social security number as a password or write their password on a piece of paper for ease of reference. Management should educate users on the risks of such practices and promote the use of alphanumeric passwords.

Secure Data Storage: Confidential information or highly sensitive data should be stored securely. Management should consider storing sensitive data in encrypted form and implementing stringent access controls.

Encryption: Encryption technology disguises information to hide its meaning and enhances confidentiality by restricting information access to intended users. Encryption-based methods can also be used to verify message authenticity and accuracy. Information is encrypted and decrypted with a cipher and key using specialized computer hardware or software. Secrecy of the key and complexity of the cipher are crucial for the success of encryption controls.

Firewalls: Firewalls are physical devices, software programs, or both, that enhance security by monitoring and limiting access to computer facilities. They create a security barrier between two or more networks to protect the computer system from unauthorized entry.

Authentication: Authentication controls are used to verify and recognize the identity of parties to a transaction. Such controls typically include acknowledgment, computerized logs, digital signatures, edit checks and separation of duties. Weak authentication controls can allow the accuracy and reliability of data to be compromised by unauthorized fabrication, errors introduced in the system or corruption. Savings associations should utilize authentication controls to preserve the integrity of data.

***Acknowledgment**:* Acknowledgment controls include batch totaling, sequential numbering and one-for-one checking against a control file to verify that electronic transactions are properly completed. For example, if an electronic transmission is interrupted, the institution should have controls to notify the sender of the incomplete transaction and prevent duplication of data during the retransmission. In addition, savings associations should install anti-virus software to prevent corruption of data or systems.

Evaluating Information Technology

The trust and asset management examiner should focus on the systems and issues that are considered critical to the performance of the institution's trust and asset management responsibilities. There are five basic IT elements to be considered in the discussion of the risks associated with information technology. While trust and asset management examiners will defer to the OTS information technology examination staff for a more technical review of these elements, the trust and asset management examiner should discuss them with management to ascertain whether the appropriate risk controls have been established. The five information technology elements are:

Management Processes: Management processes encompass planning, investment, development, execution and staffing of information technology from a corporate-wide and business-specific perspective. Management processes relating to information technology are effective when they are aligned with, and supportive of, the institution's mission and business objectives. Management processes include strategic planning, management and reporting hierarchy and a regular independent review function.

Architecture: Architecture refers to the underlying design of an automated information system and its individual components. The underlying design encompasses both physical and logical architecture, including operating environments and the organization of data. The individual components refer to network communications, hardware, operating systems software, communications software, database management systems, programming languages and desktop software. Effective architecture meets current and long-term organizational objectives and addresses capacity requirements to ensure that systems allow users to easily enter data at both normal and peak processing times. It also provides satisfactory solutions to problems that arise when information is stored and processed in two or more systems that cannot be connected electronically.

Integrity: Integrity refers to the reliability, accuracy and completeness of information delivered to the end-user. An information technology system has an effective level of integrity when the resulting information flows are accurate and complete. Lack of integrity in an institution's systems will adversely affect day-to-day reliability, processing performance, input and output accuracy and ease of use of critical information.

Security: Security refers to the safety afforded to information and its data processing environments, using both physical and logical controls to achieve a level of protection commensurate with the value of the information. Information technology has effective security when controls prevent unauthorized access, modification, destruction or disclosure of information during its creation, transmission, processing, maintenance or storage.

Availability: Availability refers to the delivery of information to end-users. Information technology is effective only when information is consistently delivered on a timely basis to support business and decision-making processes. In assessing the adequacy of availability, examiners should consider the capability of information technology to provide information to the end-users from either primary or secondary sources, including contingency plans to mitigate business disruption. Contingency plans should set out a process for restoring or replacing its information processing resources, reconstructing its information assets and resuming its business activity when disruption occurs. Disruption may be caused by human error or intervention, natural disaster or infrastructure failure (such as loss of utilities or communication lines) or operational failure of hardware, software or network communications.

Contingency Planning

All institutions should have written contingency plans established in the event that data is lost or systems are damaged. The contingency plans should address processes to restore data and systems from off-site backup. Contingency planning, also known as business resumption planning, is a process of reviewing an institution’s departments or functions and assessing each area’s importance to the viability of the organization. This planning process should address each critical system and operation, whether performed on-site or by a service provider.

The savings association’s board of directors and senior management are responsible for the comprehensive planning, review, testing and approval of the institution’s contingency plans. These plans should be reviewed annually and documented in board minutes.

If the savings association has contracted with a service provider, management also must evaluate the adequacy of contingency plans for its service provider and ensure that the savings association’s contingency plan is compatible with its service provider’s plan.

Contingency plans can minimize business disruptions caused by problems that impair or destroy the institution’s processing and delivery systems. The loss or extended disruption of business operations poses substantial risk of financial loss and could lead to the failure of the institution. Therefore, contingency planning requires a department-specific, as well as an institution-wide emphasis, as opposed to focusing only on the centralized computer operations.

The beginning point in establishing a contingency plan is to assess the risks posed by each processing system, identifying the principal departments, resources, activities and constituencies potentially affected. This includes assessing the response capability of service vendors that provide disaster recovery services. The vendor should provide alternative processing sites as well as storage and transportation of back-up media between the storage vendor, alternate processing site and the institution). Management should also formally appoint and empower individual(s) with the latitude and authority to respond during an incident.

The savings association’s contingency plan should also include an incident response team. Generally, the team consists of the officers and employees who represent key departments and functions and who collectively provide the expertise necessary to respond quickly and decisively to problems. A preparedness plan should also be established that defines the roles and responsibilities for each team member. Although the degree of sophistication will vary depending on the risks inherent in each system, establishing an incident response team and preparedness plan also provides a platform from which an institution can respond to a problem situation. The composition of a response team or extent of a preparedness plan will depend upon the level and complexity of information technology and the institution’s available resources.

Distinction Between Information Technology and Trust and Asset Management Examiner Review

Information technology examiners will continue to examine savings associations that operate their own computer center or have sensitive and complex internal information systems operated on personal computers or local or wide area networks. Additionally, IT examiners will continue to examine national, regional and local service bureaus. All information systems examinations (institution and service bureau) are conducted according to the policies and procedures in the Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook.

Trust and asset management examiners will examine the information systems and technology controls of savings associations that have information system services provided primarily by a service bureau but are increasingly using internal information systems and technology to perform daily operations and provide products and services. During the course of a trust and asset management examination, examiners should specifically review the adequacy of authority level controls and access to Fedline operations in the trust department.

In addition to these procedures and those found in Section 341 of the Thrift Activities Handbook, examiners should become familiar with the FFIEC Information Systems Handbook as a source of useful information.

Examiners are reminded that access and speed capabilities can magnify risk in an electronic environment. This is particularly true if risk management control programs are ineffective or if a system is linked to a savings association's central operations or databases. In other words, a savings association can be exposed to significant risk even if activity volume is nominal. Therefore, consultation between the trust and asset management and IT examiners may be necessary to comprehensively evaluate a savings association's electronic environment. Trust and asset management examiners should consult with a regional IT examiner for assistance, as necessary.

Generally, the need for services of an IT examiner may include instances where:

- The savings association has a web site that is directly connected to its operating system
- The savings association has the capability for customers to access and transfer data, files or messages
- The savings association has the capability to enable users to direct or process financial transactions (e.g., transactional web site or stored value system)
- Significant deficiencies or weaknesses are noted
- Systems are unusually sophisticated

Depending on the extent of internal control weaknesses, the examiner in charge (EIC), the trust and asset management examination manager, and the IT examinations manager will determine if follow-up by the IT examination staff is required as part of the current or future examinations.