Introduction

Increasingly, financial institutions are focusing on possible opportunities presented by electronic services, the Internet, and the World Wide Web. Institutions are exploring these electronic areas to remain competitive, improve customer service, and reduce their operating costs. Consequently, the electronic environment and technology employed by financial institutions to conduct activities is continually evolving.

Sophisticated phone systems and direct dial-up or Internet computer programs facilitate added access. Traditional products and services can be offered through new delivery channels and entirely new products and services may be developed. For example, in addition to promotional, lending, and deposit-gathering activities, institutions can offer bill payment programs, non-deposit sales activities such as mutual funds, and cash management services.

With the increased focus of institutions on the use of electronic channels to perform their daily operations and offer new products and services, safety and soundness examiners play a more important role in evaluating an institution's risks in the use of information technology. Whether the institution's deployment of technology is limited to the staff's use of stand-alone personal computers (PCs) or includes more sophisticated applications such as telephone or PC banking programs for customers, the rapid pace of change in the electronic networked environment calls for a risk-based approach to examinations of institutions.

An institution's effectiveness in controlling the risks inherent in the use of evolving technologies is directly related to its overall safe and sound operation. Institutions that engage information technology should create a safe, sound, and secure infrastructure that is adequate to evaluate and mitigate risks associated with such activities.

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 reliability. For instance, an information-only World Wide Web site used for advertising purposes may be inappropriately altered by unauthorized parties. Electronic mail containing confidential or proprietary information may be distributed in error. Networked systems that are directly connected to an institution's main operations database might be accessed by unauthorized parties, revealing sensitive data.

The use of an electronic channel to deliver products and services introduces unique risks for an institution due to the increased speed at which systems operate and the broad access in terms of geography, user group, applications, databases, and peripheral systems. In addition to the unique risks, traditional risks that are similar to those in customary banking activities are also present. For example, if an institution conducts lending or deposit-gathering activities over an electronic channel, credit and liquidity risks must be considered in the context of the high-speed, wide-access electronic environment.

This Section describes a safety and soundness examination program to evaluate such risks. If these risks are not detected and adequately addressed, problems such as unauthorized access to records, data integrity deficiencies, inadequate disaster contingency planning, interruption of customer service, lack of internal controls, and fraud can cause significant losses for an institution. This examination program can be used to determine if an institution's planning, deployment and operation, and audit processes are adequate to ensure a safe, sound, and secure infrastructure for use of information technology.

This program is intended to supplement Section 340, Internal Controls, of the Thrift Activities Handbook to ensure that risks of evolving technologies are periodically evaluated in all institutions and that appropriate controls are in place to mitigate such risks.

Information Technology and Electronic Banking in Financial Institutions

The volume, speed, and complexity of transactions in the financial industry generally require institutions to use software and computers to support their daily operations. Institutions can achieve significant efficiencies when they use technology to perform functions such as accounting, financial analysis, recordkeeping, wordprocessing, and financial and management reporting. Many institutions use a general ledger software or other types of financial software to process large volumes of data quickly and efficiently. Other institutions also use management information systems, database, word processing and spreadsheet software to track and report on the performance of the institution.

Similarly, institutions are challenged to find ways to improve customer services. Therefore, as discussed previously, institutions are focusing on possible opportunities presented by electronic services, the Internet, and the World Wide Web. Consequently, electronic banking is a primary component of many institutions' business plans.

Electronic banking is the delivery of information, products and services between a consumer and a financial institution using electronic access devices such as telephones, automated teller machines, automated clearing houses, and personal computers. Typically, these devices are connected through a communication line such as a telecommunication line, private network, or the Internet. Some electronic banking activities can be conducted outside of the communication network. For example, debit cards and stored value cards are potential electronic banking channels that can be used by consumers without the need for a direct link to a communication network.

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

- Personal computers, and local and wide area networks;
- In-house computer center and client server systems; and
- Outsourced vendors.

An institution'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 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 (PC) has become a prominent tool in today's business environment. The power of the PC has helped information processing to evolve well beyond the traditional central environment to decentralized or distributed networked operations. In addition to its use as a word processor and terminal access device to other computers, the PC can also operate for staff and customers as a powerful stand-alone computer or within a network of computers.

Local and wide area networks of PCs have offered substantial benefits in productivity and information access. Institutions' growing use of PCs and software to deploy new technology is dependent on a network environment. The electronic network facilitates interaction between the institution and the users (staff and customers). Telephone banking, PC banking, automated teller machines, automatic bill payments, automated clearing house systems for direct deposit or payment are familiar examples of existing and evolving services that institutions 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, and local and wide area network activities, 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 exposures and the demands for expanded information processing controls has lagged.

While each PC or network requires certain operational type controls such as physical security (e.g., lock and key), logical security (e.g., 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 computer. This may involve the original creation of a software program or the customization of existing routines from a 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 PC-related functions separate from the centralized operating controls. For example, users can download and manipulate information from main databases. The PC user

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 developed internally or purchased or licensed from outside vendors.

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 an institution 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 institutions may determine that their use 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 institution's 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 institution and 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.

Facilities Management Arrangements

Institutions that have an in-house computer center can contract with a facilities management company to take over the management and operations of the institution's computer center. The facilities management company provides the systems and programming support and computer operations personnel to manage the computer center.

Employing facilities management is not without limitations and risks. An institution may be exposed to excessive operating costs, poor outsourcing contracts that do not protect the institution in case of termination of service, loss of customer data, lack of data communications security, and lack of contingency planning.

Service Bureau

Service bureaus provide standardized information system services to multiple institutions. They are common among smaller institutions 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 institutions also find service bureaus a cost-effective alternative. Service bureaus provide the institution with experience, proven software, and reliable hardware.

Typically, data is forwarded to the service bureau computer center via on-line data entry terminals or transported by courier. Output reports are returned to the institution via on-line terminals, remote printing at the institution, or the shipment of paper and microfiche reports by courier.

Risks involving service bureaus are similar to facilities management arrangement since management has turned over control of the information technology function to an outside company.

Contracts

When employing the services of an outside vendor, management should carefully review any proposed service contracts or agreements to minimize the institution's exposure to risk. The guidelines listed below should be followed when executing any con-

tract with an outside vendor. In addition, the institution's legal counsel should review the draft contract to determine that the interests of the institution are adequately protected.

Typical contract guidelines require an institution to:

1. 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; and
   - Quality of the service provided.

2. Ensure that any contract specifies the duties and responsibilities of the institution and the service provider.

3. Review the contract's penalty provisions for reasonableness in the areas of: contract length, fees, compensation of the servicer for loss of income, etc.

4. 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 institution'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 with a copy of the:

     – current third-party review report when a review has been performed; and
     – service provider's current audited financial statements.

   - The service provider agrees to release the information necessary to allow the institution to develop a contingency plan that will work in concert with the service provider's plan.

In addition, institutions should be aware of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) restrictions on contracts. Title II, Section 225 of FIRREA states:

"An (FDIC) insured depository institution may not enter into a written or oral contract with any person to provide goods, products or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety and soundness of the institution."

Accordingly, when negotiating contracts, an institution must ensure that the service provider can provide a level of service that meets the needs of the institution over the life of the contract. The institution is also responsible to ensure that contracts are accounted for in accordance with generally accepted accounting principles (GAAP).

In addition, some service contracts improperly offer inducements that allow an institution to retain or increase capital by deferring losses on the disposition of assets or avoiding expense recognition for current charges. Institutions experiencing earnings and capital problems are particularly attracted to these inducements.

Examples of such inducements include:

- The service provider purchasing assets (e.g., computer equipment or foreclosed real estate) at book value, which exceeds current market value;
- The servicer providing capital by purchasing stock from the institution;
- The servicer providing cash bonuses to the institution once the conversion process is complete; and
- The institution deferring expenses for conversion costs or processing fees under the terms of a lease or licensing contract.

These inducements offer a short-term benefit to the institution. However, the servicer usually recoups its costs by charging a premium for the data processing services it provides. These excessive data processing

fees can adversely affect an institution's financial condition over the long term. In addition, the institution's accounting for such inducements typically is inconsistent with GAAP.

Contracting for excessive servicing fees or failing to properly account for such transactions is considered an unsafe and unsound practice. Service agreements that include contract provisions and inducements similar to those discussed above should be closely reviewed by the institution. Institutions must ensure that accounting under such agreements reflects the "substance" of the transaction, not merely the "form."

While the provisions of a service provider contract are not standardized across the industry, a number of items are included in most contracts. Appendix A to this Section provides additional guidance for institutions initiating, renewing, or revising a service provider contract or agreement and lists the various provisions usually incorporated in such contracts.

Management Controls for Evaluating and Controlling Risks

Institutions should adopt a risk management program to address unique aspects of an electronic environment. Factors such as transaction speed, geographic reach, and user anonymity introduce new challenges for risk management controls designed to monitor activities or trends. Without properly focused control procedures, questionable activities conducted over an electronic channel might not be discovered by traditional review and audit procedures. Management may need to consider multiple changes throughout its operations. Specifically, management should consider whether:

- New computer hardware and software is needed to control security threats;
- Existing audit procedures require expansion to incorporate the new electronic activities; and
- Outsourcing contracts should be modified to adequately protect the institution's interests.

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

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 and customer service, and operations.

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

Institutions should evaluate the risks associated with an electronic environment and implement sound controls. Management and the Board should implement a comprehensive program to manage the inherent risks prior to implementing new systems or technology. Representatives of all functional areas (e.g., audit, finance, information systems, legal, lending, and marketing) should be involved from the beginning of this process to collectively assess the overall effect on the institution.

Ineffective controls limit or distort the quality of information upon which management relies to make effective decisions. To assess management's awareness of the risks associated with the use of information systems and technology and its effectiveness at managing such risks, examiners should evaluate the adequacy of the institution's controls for planning, deploying and operating, and auditing their use of new technology.

Examiners should exercise discretion in determining the scope of the information systems and technology review based on the level of the institution's activities in this area and the adequacy of internal controls.

Strategic Planning

Information technology facilitates broad access to confidential or proprietary information. Therefore, it is imperative that management (including the board, senior management, and line officers) is fully informed of the significant investment, opportunities, and risks involved in deploying such technology. Deficiencies in planning and deployment significantly increase the risk posed to an institution and decrease its ability to respond in a satisfactory manner. There is a growing trend among the smallest institutions to plan for the use of information technology. Regardless of size, institutions should have an appropriate information technology plan that establishes the framework for their deployment and operation of technology. The substance and form of any formal plan will vary significantly, depending on the complexity of the institution's information systems and technology. Therefore, the key element for examiners to consider is whether the plan meets the institution's needs.

Institutions should annually update their information technology plan. The plan should coordinate technology initiatives and activities to the business planning process. The strategy may include a combination of internal and outsourcing activities that support the delivery of competitive products and services.

Before an institution deploys new information technology, management and the users should have a clear understanding of the specific needs being addressed by the proposed technology. Alternatives should be reviewed by management and the users to ensure that the best solution is selected. When developing or purchasing a new system, the institution should aim to produce or acquire a system that is easily modified and maintained by someone other than the original developer. Finally, the completed system should be subject to rigorous testing to provide assurance that the results produced are valid and reliable.

Deployment and Operation

As part of the institution's decision to deploy or outsource for technology to support a new product, service, or delivery channel, it should determine which operational areas are affected. The policies and procedures in each affected area should be reviewed and appropriate changes made to reflect the new electronic activities.

When deploying a new information system or technological capability, institutions must meet all regulatory requirements and resolve all legal issues for each activity that will be conducted. Institutions should determine that each new activity meets minimum standards for initiating, completing, and enforcing legal documents and financial transactions to protect the value and efficiencies of the systems and technology deployed. If an institution fails to review the regulatory standards and legal foundations, it heightens the risk of direct financial loss, regulatory action, or contingent liabilities resulting from civil actions.

Whether the institution deploys a new advertising medium or a transactional facility, all systems and technology must also be reviewed for compliance with consumer protection requirements. Although consumer protection and trust activities are addressed through separate examination programs, the institution's plans to deploy information technology must consider the full range of implications. To do otherwise may affect the institution's compliance posture, and possibly result in consumer complaints.

When deploying technology, management should:

- evaluate the associated risk with its information technology;
- establish clear responsibilities for the acquisition, implementation, and support;
- establish adequate insurance coverage;
- educate all users on the need to adhere to the control standards. This educational effort should also address the risks of not adhering to the standards; and
- incorporate control practices and responsibilities to manage these activities into an overall corporate information security policy and infrastructure.

Institutions should establish adequate controls to operate an in-house computer center, in addition to adequate control practices for PCs and local and wide area networks. Institutions that fail to establish such controls will be exposed to numerous risks such as inadequate hardware and software systems, excessive development and operating costs, unauthorized access to records, data integrity deficiencies, inadequate contingency planning, interruption of customer service, lack of internal controls, and fraud.

Generally, effective information systems and technology are subject to frequent changes to reflect new or improved technology and capabilities. Therefore, once the initial policies and procedures are established, each operational area should periodically review policies and procedures to stay current with the new activities. Any deficiencies should be documented for appropriate action.

When planning the deployment of any new system, whether developed internally or acquired through a service provider, the institution has an obligation to establish and maintain minimum standards for controls, operation, and user acceptance. Some basic control standards that should be implemented with information technology are:

- change-control management;
- data input and output controls;
- information security;
- contingency planning;
- conversion project management; and
- training.

Change-Control Management

An institution must be prepared to adapt its activities and information technology to meet changing requirements and circumstances. Modified technology should be subject to many of the same controls as newly developed systems. Most important among these is the requirement that there be thorough testing of any changes. In addition, accurate records should be maintained describing the change, reasons for the change, and person(s) responsible for making the change.

Input and Output Controls

An institution should require additional data controls for technology that is used to process information that has a direct monetary effect on the institution or its 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. In more sensitive situations with a significant dollar effect, institutions should require that certain functions be performed under dual control. Appropriate controls should be established in the early stages of development and deployment and described in detail in the institution's operating policies and procedures.

The institution 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 institution 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 delineated in this Section are generally applicable, 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 the intended person receives accurate information, and prevent eavesdropping by others. In addition, undeniable proof 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, monitor, control, and prevent potential risks. Although not all-inclusive, the following potential risks and respective 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 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 alpha-numeric 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 only 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 institution's computer system from unauthorized entry.

- Authentication - Authentication controls are used to verify and recognize the identity of parties to a transaction. It is the primary component of non-repudiation. 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 comprised from unauthorized fabrication, errors introduced in the system, or corruption. Institutions should utilize authentication controls to preserve the integrity of data.

- Acknowledgment - Acknowledgment controls, such as batch totaling, sequential numbering, and one-for-one checking against a control file 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, institutions should install anti-virus software to prevent corruption of data or systems.

Contingency Planning

When data is lost or systems are damaged, the institution should have contingency plans 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 institution's board of directors and senior management are responsible for establishing policies, procedures, and responsibilities for comprehensive planning, review, testing, and approval of the institution's contingency plans annually, and documenting such reviews in board minutes.

If the institution has contracted with a service provider, management also must evaluate the adequacy of contingency plans for its service provider and ensure that the institution'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 financial institution's processing and delivery systems. The loss or extended disruption of the institution's business operations poses substantial risk of financial loss and could lead to the failure of the institution. Therefore, contingency planning requires an institution-wide emphasis, as opposed to focusing only on the centralized computer operations.

In developing a contingency plan, decisions should be guided by management's best judgment. The beginning point is to assess the risks posed by each system deployed, identify the principal departments, resources, activities, and constituencies potentially affected by a problem. This includes assessing the response capability of key disaster recovery service vendors (e.g., the vendor(s) providing alternative processing sites; 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.

Appendix B to this Section provides an example of a process that management may consider in developing contingency plans. It is an outline and is not all encompassing. Each institution should assess its own risks and develop strategies accordingly.

The institution'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 in the event of a problem situation. Although the degree of sophistication will vary depending on the risks inherent in each system deployed, 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.

Conversion Project Management

Any institution that engages in the use of technology to perform its operations or provide services must make a commitment to continuously update its activities to keep current with technology and remain competitive. For example, if an institution experiences a corporate merger or acquisition, wants to control costs, or desires to offer new products or services, it must plan accordingly to convert its operations and computer systems to accommodate the change(s).

In today's technologically competitive environment, it is likely that institutions will experience one or more system conversions. A system conversion is the process of replacing existing applications with new ones developed internally, or with vendor software, either through a leasing or outsourcing agreement.

Typical reasons for a system conversion:

- Improve operating efficiencies and reduce costs;
- Merger or acquisitions of institutions;
- Inability of a service bureau to meet the institution's demands; or
- The service bureau upgrades its systems and no longer supports the current system.

The institution's planning, testing, and monitoring of new activities should be conducted as part of their system development project management and risk management process.

Without adequate project management controls, a conversion can present significant risks of loss to the institution. Flawed or failed conversions can be very costly and can compromise the integrity and reliability of books and records, causing unsafe and unsound conditions in the institution. For example, because of a flawed check processing conversion, a well-run institution was forced to charge off unresolved bookkeeping differences equivalent to one-year's net income. In another institution, a conversion that affected deposit accounting caused management to lose track of 10 percent of all deposits and remained unreconciled for 30 days, resulting in significant losses of time and money.

The board of directors should monitor the progress of major conversions and hold senior management accountable for their success. Management should develop and oversee the successful completion of key tasks and milestones by both the vendor and responsible institution personnel. User acceptance testing and debugging as well as adequate training for staff and customers must occur before a system is implemented or converted.

Training

Institutions must properly supply education and support to achieve user acceptance and confidence. Participants should be trained to properly use applications and respond to problem situations. If an institution fails to provide reasonable training and support for customers and staff, the users' commitment to the system is weakened, administrative expenses increase, and avoidable errors occur. These deficiencies raise the risk of data integrity problems, complaints, and possible legal actions. Risk also increases when an institution fails to educate users on proper security precautions such as locking personal computers and confidentiality of passwords.

Support staff, such as a help-line or customer service representatives, should also be kept informed of any changes or updates to systems. They should also be trained on how to execute the disaster recovery plan. If the institution contracts for outside resources, qualifications of external personnel should be evaluated prior to signing with the vendor. Management should also provide backup training for key job

functions so that human emergencies will not disrupt service.

When planning and deploying an electronic activity or new technology, management should establish prudent guidelines for change-control management, data input and output, security, contingency planning, project management, and training. Once deployed, the operation of each system must be subject to ongoing reviews to evaluate performance against current strategic plans and objectives, technological developments, and operating policies and procedures.

Audit

Sound management practices dictate that the board of directors and management establish appropriate policies, procedures, and operating controls for the use of information technology. They should also establish monitoring systems to ensure that controls are maintained. All large institutions and those with complex operations should have an internal audit department to supplement the annual audit. Regardless of size, institutions should have appropriate internal audit functions. In fulfilling these functions, an institution's priority is to ensure the accurate processing of information, privacy of financial and customer records, and continuation of service in case of business interruptions.

Audit procedures are most effective when designed into each system during the development phase. When coupled with a strong risk management control program, a comprehensive, ongoing audit program allows the institution to protect its interests as well as those of its customers and other participants. In developing audit programs, the institution must consider the full scope of each application to protect financial and informational assets, system reliability, and user confidence.

An effective audit function will maintain independence in reviewing institution activities and be accountable to the Board and senior management. The audit function should have competent staff to provide adequate audit coverage. The institution should have Board approved audit procedures and the audit function should document and report findings and recommendations, with management responses, to the Board. All audit findings should require management follow-up with appropriate action.

Generally, an audit will:

- evaluate the quality of management through a review of policies, standards, and procedures;
- evaluate the efficiency of operations, and adequacy of procedures and controls;
- determine if controls are being applied in a manner consistent with management policies and procedures; and
- substantiate the integrity of actual activities (e.g., employee activities, operating system controls, and access levels).

The scope of an examination will be significantly influenced by the:

- adequacy of the audit function; and
- extent to which the institution has adequate policies, procedures, and controls in place.

Examiners should refer to the Thrift Activities Regulatory Handbook Section 355, Internal Audit, for detailed guidance in evaluating internal audit work.

Examination Comments and Rating

Examination findings will generally be incorporated into the Management section of the safety and soundness report. Unless otherwise instructed, findings should be addressed collectively as "information technology." If the institution is engaged in the use of information technology, at a minimum, a brief summary comment describing the institution's use of information technology should be included. Significant findings should be described in sufficient detail to identify specific conditions that warrant corrective action by the institution. A summary of such findings should also be carried forward to the Examination Conclusions and Comments page.

In reviewing the institution's use of information technology and determining its effect on the overall management rating, the examiner should consider:

- specific issues in relation to the volume and trends in transactions, dollars, and customers;
- apparent risk to the institution's financial and informational assets, including customer data, regardless of the volume and trends in activity;
- anticipated growth in volume, whether dollars, transactions, or customers; and
- anticipated expansion of products, services, or platforms.

Generally, if the safety and soundness examiner identifies serious deficiencies with the controls, such findings should be reflected in the management rating.

Distinction Between Information Systems and Safety and Soundness Examinations

Information systems examiners will continue to examine institutions 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, information systems 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.

The growing use of on-line systems, personal computers, and local and wide area networks to develop and deliver financial products and services, however, also requires appropriate examination guidance for the safety and soundness examiner. Safety and soundness examiners will examine the information systems and technology controls of institutions that have their information systems 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. In addition to these safety and soundness procedures, examiners can refer to the FFIEC Information Systems Handbook as a source of useful information.

For those institutions that are developing in-house technology and continue to outsource a significant part of their technology needs, appropriate examination requirements may not be clear. In such situations, regional management should consider the most recently available information concerning the institution's information technology and determine if these safety and soundness procedures are sufficient to evaluate the infrastructure of the institution or if a more detailed information systems examination is required.

Examiners are reminded that the 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 an institution's central operations or databases. In other words, an institution can be exposed to significant risk even if activity volume is nominal. Therefore, consultation between the safety and soundness and information systems examiners may be necessary to comprehensively evaluate an institution's electronic environment. Safety and soundness examiners should consult with a regional information systems examiner for assistance, as appropriate.

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

- The institution has a web site that is directly connected to the institution's operating system.
- The institution has the capability for customers to access and transfer data, files, or messages.
- The institution has the capability to enable users to direct or process financial transactions (e.g., transactional web site, PC on-line banking, or stored value system).
- Any situation where significant deficiencies or weaknesses are noted.

An expanded analysis should be performed in situations where systems are more sophisticated or when significant deficiencies are observed. The expanded analysis will involve technical procedures that will be performed by information systems examiners.

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

Examination Objectives

To determine if management analyzed the investment, opportunities, and risk involved with deploying electronic capabilities.

To determine if management policies, procedures, and internal controls are adequate to monitor and control information technology risk.

To assess the adequacy of security controls over computer and microcomputer terminals used for information technology services.

To assess management's guidelines for selecting, evaluating, and monitoring service bureau performance.

To assess the adequacy of internal audit review of related information technology.

To determine compliance with information technology related regulations.

To recommend corrective action when internal controls, policies, procedures, and practices are deficient.

Examination Procedures

While systems will generally be reviewed individually, examiners should consider the degree of integration. Examiners should use judgment to identify common review points. These procedures are intended to compliment traditional examination procedures in the evaluation of specific activities, such as lending, deposit-gathering, and non-deposit activities. Although the primary objective of this program is to evaluate the adequacy and effectiveness of the institution's information technology controls, efforts should be made to coordinate reviews of written policies, internal controls, and other related functions.

Contact with examiners in other examination areas may be necessary to comprehensively evaluate an institution's activities. Referrals to information systems, compliance, and other examiners should be considered with respect to the institution's activities and the nature of examination findings.

Level I

1. Obtain and review the following material for information relating to the condition of the institution's information technology controls:

    - Most recent financial statements of the institution.
    - Information technology comments contained in the institution's latest ROE.
    - Most recent service provider information systems ROE and any subsequent correspondence, if available.
    - Current Regulatory Plan.
    - Summary of the most recent service provider external audit or third-party-review reports, if available.
    - Internal or external audit reviews of data security, end-user applications, data communications, ATMs, balancing and reconciling accounts, etc.

2. If the institution has a web site, examiners should review it to determine the extent and complexity of potential Internet activities. In addition, search the Internet for the institution's name to determine if any relevant information was published about the institution.

3. Review the information contained in the Information Systems PERK 005 to identify the institution's service bureau(s) and in-house information systems applications. This information should include:

    - Information systems contact person.
    - Name/address of servicer(s) and applications processed.
    - Any affiliated relationships with thrifts or data processing vendors.
    - Any in-house PC, local area network (LAN), wide area network (WAN) computer systems used for processing primary or special applications.
    - Future information systems plans/conversions and target dates. (This information should also be forwarded to the regional information systems examination manager.)

4. Obtain and review the following documentation to assist in evaluating the adequacy of controls:

    - Board minutes and audit committee minutes relating to information systems matters (see Handbook Section 330, Management Assessment).
    - Current data processing contracts with servicer.
    - Insurance policies relating to information systems.
    - Copies of the policies, standards, and procedures relating to data security, information systems operations, contingency plans, data communications, and microcomputer controls.
    - For in-house PC/LAN/WAN systems:

        – software utilized and the functions performed by that software; and
        – spreadsheets used for loan analysis and board reports.

5. Determine if the institution has assessed the importance and sensitivity (i.e., high, medium, low) of the information processed in each system.

6. Determine whether each system was reviewed by the institution's internal or external auditors. Verify that major findings were adequately addressed.

7. Verify that the institution's internal and external audit programs were updated to specifically address the institution's use of information technology.

8. Verify that an internal auditor, external auditor, or member of management, not directly involved in information systems activities, has been assigned the responsibility for auditing the information systems function and activities. Determine whether this individual has any specialized audit or information systems training.

9. Determine whether the scope of the audit program is commensurate with the extent of information systems activities in the areas such as contract administration, insurance, operational controls, on-line access controls, contingency planning, ATM activities, and PC/LAN/WAN controls.

10. Verify that there are written audit procedures that require:

    - review of all critical automated applications and systems;
    - issuance of formal audit reports;
    - formal management responses;
    - periodic review of audit reports by the board of directors; and
    - preparation and maintenance of audit work papers.

11. Determine whether the person responsible for the audit function does the following:

    - Tests balancing procedures of automated applications including the disposition of rejected and unposted items.
    - Periodically samples customer record files (master files) to verify them against source documents for accuracy and authorization.
    - Spot-checks computer calculations, such as interest on deposits, loans, securities, loan rebates, ARM calculations, service charges, and past-due loans.
    - Verifies output report totals.
    - Checks accuracy of exception reports.
    - Traces transactions to final disposition to determine adequacy of audit trails.
    - Performs customer confirmations.

12. Determine whether the audit procedures cover the flow of critical data through interrelated systems (i.e., from point of origin to point of destination within the set of systems).

13. Determine whether the institution obtained and reviewed the servicer's third-party-review report. (If so, list exceptions and corrective action from the report).

14. If the examiner determines that the institution's audit function is adequate and the institution's audit work papers may be relied upon, the audit work papers should be referenced in lieu of completing the remaining Information Technologies procedures. If the internal audit work does not adequately address controls, the examiner should review Level II procedures and perform those necessary to test, support, and present conclusions from performance of Level I procedures.

Level II

Select one or two departments using information systems and technology (e.g., loans and savings) to determine the adequacy of the institution's operational controls. If the initial findings indicate serious deficiencies, other departments should be reviewed to validate the findings.

Strategic Planning

1. Determine whether the board or an appropriate committee approves each system deployment based on a written strategic plan and risk analysis commensurate with the activity. Such analysis should prompt management to ensure that strategic and operating plans were updated to incorporate electronic delivery channels and that the identified risks associated with each deployment were addressed.

2. Determine whether management maintains and updates annually the institution's information systems plan to coordinate with business plan objectives and requirements.

3. Determine whether management reviewed the institution's defined trade area.[1] Determine whether guidelines for accepting account applications and other relevant policies and procedures were updated to address activities beyond the traditional trade area.

4. Determine whether a study of alternatives was completed or obtained for each system deployed. Determine whether the study considered "worst case" scenarios. Verify that the study was reviewed by senior management and the board. Verify that major findings were adequately addressed.

5. As applicable, determine whether each system was reviewed by the institution's compliance officer in regards to content, required disclosures, and any other relevant issues. Verify that major findings were properly addressed.

6. As applicable, determine whether each system was reviewed by the institution's legal counsel. Verify that major findings were adequately addressed.

7. Determine whether the institution offers any guaranty or similar pledge in relation to any payment or delivery system. Verify that such guarantees were reviewed by the institution's legal counsel, as applicable.

8. Determine the extent of any lawsuits or complaints filed against the institution or its vendors. Determine the status of resolution and existence of any contingent liabilities.

9. Verify that the underlying customer, vendor, and merchant agreements fully address the rights, responsibilities, and liability for each party. Determine whether the documents address the institution's authority to monitor, store, and retrieve electronic transmissions (including messages and data) between the institution and its customers.

10. Verify that appropriate procedures were established to ensure compliance with Financial Recordkeeping and Institution Secrecy Act. Verify that procedures were established to identify potentially structured transactions.

11. Determine whether each system was adequately tested, including volume stress testing (to ensure system capacity) and screen testing (to review content). Determine whether a pilot program was conducted. Verify that major findings were properly addressed.

12. Determine if management verified the accuracy and content of financial planning software, calculators, and other interactive programs (between internal and external users) available through the deployed systems.

Outsourcing

1. Determine whether outsourcing arrangements with vendors and subcontractors are included in the institution's consumer protection and legal reviews.

2. Determine whether, before selecting a service provider, management investigated and documented the following:

   - Alternative services.
   - Pricing of services, including special charges for forms, equipment, etc.
   - Quality of reports and user documentation.
   - Financial stability of the servicer.
   - Contingency planning if servicer is down.
   - The ability of the servicer to handle future processing requirements.
   - Requirements for termination of service.
   - Insurance requirements.

3. Determine whether the expiration dates for interrelated service contracts coincide.

4. Determine whether the institution is satisfied with the service provider's performance and output reports. If not, explain.

5. Determine whether the servicer provides the institution with current, understandable user instruction manuals for each application and whether they are used by the employees.

6. Verify that there is a written contract(s) between the institution and service bureau and the contract(s) has been reviewed by the institution's legal department.

[1] In the context of these procedures, the institution's defined trade area is viewed strategically and should not be confused with their assessment area for Community Reinvestment Act purposes.

7. Determine whether the service contract(s) provisions include:

   - Description of work performed and time schedules for processing and delivery of work.
   - Fee schedules and other charges.
   - On-line communication access and security.
   - Audit responsibility.
   - Opportunities for the institution to review independent annual audits and similar reports.
   - Provisions for contingency backup processing and record protection.
   - Notice required (both parties) for termination of service and the return of customer records in machine-readable form.
   - Confidentiality of institution data files and programs.
   - Insurance carried by the servicer.
   - Liability for documents damaged or lost in transit.

8. Determine whether the institution has maintenance contracts on computer equipment and software furnished to or purchased by the institution.

9. Verify that appropriate contract administration policies and procedures have been established.

10. Determine whether the contract administration policies and procedures provide for monitoring and management of the information systems service provider's performance in areas such as:

    - Service level performance and service charges
    - Financial condition
    - Ability to meet future needs
    - Performance reports by information systems service provider

11. Review minutes of the board of directors meetings to determine if the board has reviewed the annual servicer evaluation.

12. Verify that the institution has established policies and procedures that control third-party servicers' (e.g., electronic system providers, data processors, etc.) ability to access or monitor electronic transmissions between the institution and any of its customers. Verify that the guidelines were included as part of the contracts and agreements covering the service arrangements.

Insurance

1. Determine whether the institution's insurance provides adequate coverage for:

   - employee fidelity;
   - information systems equipment and supplies;
   - reconstruction of lost or damaged paper, digitized records, or microfilm media;
   - loss resulting from business interruption;
   - errors and omissions;
   - checks and other documents transported by air or ground courier to the data center; and
   - extended blanket bond fidelity coverage to employees of the servicer (563.190(c)).

   Confirm that any gaps in coverage were addressed appropriately.

2. Determine whether there is a formal review process for periodic assessment of the institution's information systems insurance needs by qualified employees.

Operating Controls

1. Review all relevant operating policies and procedures to determine if they were updated for the unique character and principal risks associated with alternative delivery channels.

2. Verify that policies and procedures governing access to, and the disclosure of, customers' confidential information were updated for electronic capabilities. Verify that the policies also address the information that should be shared with third parties (e.g., non-deposit product representatives, discount brokerage services, etc.). Confirm that guidelines pertaining to confidential information were included as part of the contracts and agreements covering third-party arrangements.

3. Verify that there are written policies and procedures for the acquisition, use, and maintenance of PC software and equipment.

4. Verify that reasonable requirements were adopted for periodic due diligence reviews of third-party providers, including contractors, subcontractors, support vendors, and other parties.

5. Determine whether appropriate measures were implemented to protect against violating licensing agreements in distributing software.

6. Determine whether appropriate operating policies and procedures were established or updated to address:

   - fund transfers;
   - dollar limits per transaction and relationship;
   - minimum credit standards for participants, as appropriate;
   - settlement guidelines; and
   - daylight overdrafts.

7. Determine whether control procedures exist for:

   - Source document preparation and data entry.
   - Preparation of rejects for reentry.
   - Reconcilement of output reports to input for batch systems.
   - Reconcilement of output reports of subsidiary ledger systems to the general ledger control account totals.
   - Posting entries to the general ledger.
   - Customer statement preparation and mailing.

8. Verify that procedures are in place to control customer transfers of uncollected funds from each access point. Confirm that safeguards are in place to detect and prevent duplicate transactions within each system deployed.

9. Determine whether policies and procedures were adopted to address the institution's use of electronic mail. Verify that the policies and procedures:

   - address transmissions among all user groups, including customers, officers, and employees; and
   - define permissible content to minimize risk from improper disclosure.

10. Verify that automated entries from one application to another are balanced for correctness (e.g., CD interest to DDA or Savings).

11. Verify that file maintenance changes to customer accounts record files (master files) are:

    - requested in writing (Note: In on-line systems, this procedure is handled as part of the system access controls and supervisory override feature.);
    - reviewed by staff and, when appropriate, a supervisor; and
    - verified for correctness after processing.

12. Determine whether customers are required to submit a signed authorization for each payee included in bill payment, funds transfer, and similar programs. Determine how the institution verifies the legitimacy of each payee, and whether the institution has adopted reasonable guidelines for adding payees.

13. Verify that the institution maintains control over changes to application processing parameters (e.g., CD interest rates, ARM index).

14. Determine whether transaction and exception reports are produced for user departments, and reviewed by staff and supervisory personnel. Verify that supervisory action is documented for:

    - unposted and rejected items;
    - customer account changes;
    - supervisory override transactions;
    - dormant account activity; and
    - adjusting entries to customer accounts.

15. Determine whether control procedures are in place to ensure that all reports are produced and delivered to user departments.(Note: Computer reports are frequently available on-line and are not printed on a regular basis.)

16. Determine whether microfilm, digitized records, or paper copies of checks and data entry source documents are retained before the computer work leaves the premises. If so, verify that:

    - documents and microfilm/microfiche are stored on- or off-site in a secure location with limited access;
    - an inventory or usage log is maintained at the storage site location; and
    - the quality of the microfilm is checked periodically.

17. Determine whether the institution uses standalone PCs, LANs, or WANs to process signifi-

cant data for accounting operations, management information systems, or recordkeeping functions. If so, verify that there is an adequate procedure for backing up critical files. Determine whether it is being followed. Determine whether diskettes containing significant or critical information are labeled and stored in a secure location (i.e., on- or off-site).

18. Determine whether the institution has procedures and a training program to promote awareness on the use and care of PCs.

19. Determine whether user departments processing significant applications on a PC reconcile the input and output for accuracy.

20. Determine whether there is a security policy that contains minimum control standards for PCs as described in Thrift Bulletin 29, End-User Computing.

21. Determine whether there is an established program for ongoing review of each system deployed for content, continued appropriateness, accuracy and integrity, security and controls, system updates and obsolescence, system capacity, and strategic direction.

22. Determine whether appropriate procedures exist for maintaining links with other Web sites, including both external and internal (i.e., Intranet) sites. Determine whether management regularly monitors these linked sites for continued appropriateness and accuracy of the site addresses.

23. For systems that permit access to credit lines, verify that draws or credit extensions are adequately controlled.

24. Determine whether:

    - A person(s) is designated to handle liaison with the service bureau(s).
    - Employee duties are periodically rotated for control and training purposes.
    - Employees are required to be absent from their duties by vacation or job rotation for a minimum of five consecutive days.
    - The institution's employee duties are adequately separated so that no one individual can initiate, authorize, and execute transactions.

25. Determine whether the institution's policies regarding separation of duties were updated to recognize the access afforded by electronic capabilities.

26. Determine whether user departments:

    - Establish batch controls on monetary and non-monetary data entry source documents (e.g., dollar totals or item counts) before they are sent to the service bureau for processing. (Note: On-line input processing systems now perform automated input to output balancing procedures.)
    - Receive and review output reports to check batch totals, rejected transactions, and errors.
    - Receive all scheduled output reports even when the report contains no activity.
    - Balance application totals to the general ledger.
    - Balance and reconcile suspense accounts.

27. Verify that the servicer provides:

    - Testing of new and revised programs.
    - Backup service for on-line systems.
    - Periodic testing of backup capabilities.

Information Security

1. For each system that interacts with any of the institution's other systems or databases, determine whether management required a review of the interactive components and processes to ensure compatibility and security. Verify that major issues were appropriately addressed.

2. Verify that senior management has established appropriate levels of access to information and applications for officers, employees, system vendors, customers, and other users. Verify that the access levels are formally established, reviewed on a regular basis, and enforced.

3. Determine whether appropriate procedures were established to monitor for unauthorized attempts to access the institution's system. Verify that the institution's policies require formal reporting in the event of attempted or actual attacks against any of the institution's systems. Review all known incidents. If any incidents were not reported, determine why.

4. Verify that terminals with service provider access are controlled by:

   - user logon codes;
   - passwords known only to individuals;
   - encryption, when necessary;
   - physical keys; and
   - physical configuration.

5. Verify that users with terminal access are controlled by unique user log-on codes, passwords known only to the user, or other (explain).

6. Verify that access to PCs is restricted due to physical security (e.g., keyboard locks, secure rooms) and software security (i.e., passwords) and enforced.

7. Determine whether PCs are linked to a LAN or WAN. If so, verify that:

   - passwords are used to grant access and functional authorization on the system;
   - passwords are changed periodically; and
   - each user has a unique user identification code and password.

8. Verify that periodic changes are made to user log-on codes, passwords, and supervisory override passwords. Verify that they are adequately controlled with regard to:

   - personnel authorized to make changes;
   - security of documentation; and
   - monitoring and reporting of violations.

9. Determine whether users or terminals are controlled as to:

   - the applications they can access;
   - the transactions they can initiate;
   - specific hours of operation; and
   - sign-off procedures or automatic sign-off after period of inactivity.

10. Verify that controls over restricted transactions include limited logical access, supervisory approval, and periodic management review.

11. Verify that security passwords and user identification codes are suppressed on all video and printed output displays.

12. Determine whether the institution has any direct connection between its internal operating system(s) and the system that hosts the external electronic service or activity (for example, a Web site). If the institution does have a direct connection, an information systems examiner should be consulted.

13. Determine how the institution establishes the legitimacy of each party requesting an account action or submitting related instructions or data.

14. Verify that appropriate exception reports are generated and reviewed on a periodic basis. In addition, determine whether there are reports that indicate:

    - all transactions made at a terminal by an operator;
    - restricted transactions;
    - correcting and reversing entries;
    - dates and times of transactions;
    - unsuccessful attempts to access the system and restricted information; and
    - unusual activity.

15. Determine what reporting mechanisms are employed to track the nature, volume, and trends in activity for each system deployed. Determine whether these reports include current and historical data (such as flow of funds), and provide a comparison of performance to projections.

16. Verify that the measurements above are incorporated into strategic and operating plans, budgets, and other analyses. Verify that the measurements are incorporated into relevant operating policies and procedures, such as funds management, liquidity, and interest-rate risk.

Contingency Planning

1. Verify that a backup system or method was established for users to conduct normal activity in the event the system is not available for an extended period of time. Verify that support materials (e.g., instruction guides) address the backup system or method. Verify that the institution has established a reasonable procedure to notify users in the event of a problem.

2. Determine whether an incident response team was designated to respond to problem situa-

tions. In the event a team was established, verify that the board has approved a written delegation of the team's responsibilities and authority.

3. Determine whether the institution has a contingency plan that:

   - is in accordance with CEO Memorandum 72;
   - is compatible with the service bureau;
   - identifies all critical resources, including data communication networks;
   - provides for in-house LANs and WANs;
   - provides for in-house communication hubs;
   - is tested annually;
   - is approved by the board of directors; and
   - requires participation in service bureau disaster recovery tests.

Training

1. Determine whether adequate training was provided for all officers and staff affected by the deployments (including those responsible for products, services, information systems, audit, compliance, and legal). Determine whether management has established a program for ongoing training.

2. Determine whether appropriate programs were established for customer service, support, and education. Verify that:

   - service and support functions are available during reasonably appropriate hours;
   - appropriate educational and reference materials are made available to customers regarding system security, controls, and liability; and
   - the institution has established a reasonable program to address recurring problems in a timely manner.

Conclusions

1. Discuss the adequacy of the institution's information systems with other examiners. Identify any significant problems examiners have noted, such as late reports, inaccuracy of calculations, and poor report formats.

2. Evaluate the examination findings for significant concerns and to determine if referral to an information systems or compliance examiner is necessary. Negative responses to the following questions may not require a referral. Conversely, positive responses do not preclude examiners from referring specific findings to an information systems or compliance examiner, if deemed appropriate:

   - Is an effective risk management program in place?
   - Are adequate policies and procedures in effect and enforced?
   - Do accounting and reconcilement procedures adequately address electronic capabilities?
   - Does the audit program adequately address stand-alone, interrelated, and integrated systems?
   - Are important matters referred to the institution's legal counsel?
   - Are the institution's operations consistent with regulatory requirements?
   - Is program administration and oversight adequate?
   - Is an effective vendor oversight program in effect?

If the review identifies major deficiencies and weaknesses that require additional information systems expertise to evaluate, the EIC should notify the information systems examiner to determine further action. Further review by an information systems examiner may also be required if the institution processes critical applications (e.g., general ledger) on internal information systems (e.g., PCs, LANs, or WANs).

References

Code of Federal Regulations (12 CFR)

§ 545.138	Data Processing Services
§ 545.141	Remote Service Units (RSUs)
§ 545.142	Home Banking Services
§ 563.170	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 563.190(c)	Bonds for Directors, Officers, Employees, and Agents
§ 568	Security Procedures

Office of Thrift Supervision Bulletins and Memoranda

TB 11	Interagency Supervisory Policy on Large–Scale Integrated Financial Software Systems (LSIS)
TB 11–1	Purchased Software Evaluation Guidelines
TB 29	End–User Computing
TB 44	Interagency Statement on EDP Service Contracts
TB 46	Contracting for Data Processing Services or Systems
TB 59	Interagency Supervisory Statement on EFT Switches and Network Services
CEO Memo 72	Revised FFIEC Policy Statement: Corporate Business Resumption and Contingency Planning

Other References

Federal Financial Institutions Examination Council IS Examination Handbook, 1996.

Regulation (E) Electronic Funds Transfers

OTS Web Site, Electronic Banking Page, www.ots.treas.gov

APPENDIX A: Outsourcing Contracts

While the provisions in a service contract are not standardized across the industry, a number of items are included in most contracts. This attachment contains a list of various provisions that are usually incorporated in service provider contracts. Neither the significant deviation from, nor inclusion of, these items will render a contract unacceptable or acceptable. This is an outline and is not meant to be all inclusive.

Provisions contained in such contracts should include:

- A detailed description of the specific work to be performed by the servicer, and the frequency and general content of the related reports.
- A fee schedule that outlines development, conversion and processing costs, as well as charges for special requests.
- An outline of the training to be provided for institution personnel, including the type, number of employees to be trained, and the associated cost.
- Established time schedules for receipt and delivery of work.
- The availability of on-line communications, security over accesses and transmissions, and alternate data entry considerations.
- Audit responsibility, including the right of financial institution representatives to perform an audit.
- A definition of backup, contingency, and record protection provisions (equipment, software and data files) to ensure timely processing by the service center in the event of an emergency.
- A detailed description of liability for source documents while in transit to and from the service center. The responsible party should maintain adequate insurance coverage for such liabilities.
- Maintenance of adequate insurance for fidelity and fire liability, reconstruction of physical properties, data reconstruction, and resumption of normal operations, as well as for data losses from errors and omissions.
- Confidentiality of records.
- Ownership of software 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.
- Processing priorities for both normal and emergency situations.
- Mandatory notification by the servicer of all system changes that affect the institution.
- A requirement that the vendor be responsible for keeping the software current by incorporating regulatory changes and updates.
- Access to vendor's source code and maintenance of documentation via escrow agreements for turnkey operations.
- A guarantee that the servicer will provide necessary levels of transition assistance if the institution decides to convert to other automation alternatives.
- Cancellation, termination, and bankruptcy clauses.
- A requirement that the EFT facility provide for contingencies, integrity, security, and confidentiality of data.
- Financial information (audited) to be provided annually by the servicer to the financial institution.
- A detailed description of the disaster recovery contingency test results to be provided annually by the servicer to the financial institution.
- A prohibition against the assignment of the contract by either party without the consent of the other.

OTS Thrift Bulletin (TB) 44, Interagency Statement on EDP Service Contracts, and TB 46, Contracting for Data Processing Services or Systems, offer additional guidance related to contracting for such services.

APPENDIX B: Corporate Business Resumption and Contingency Planning Process

This outline provides an example of a process that management may consider in developing contingency plans. It is an outline and is not all encompassing. Each institution should assess its own risks and develop strategies accordingly.

I. Obtain a commitment from senior management to develop the plan.

II. Establish a management group to oversee development and implementation of the plan.

III. Perform a risk assessment.
- A. Consider possible threats such as:
  1. Natural – fires, flood, earthquakes, etc.
  2. Technical – hardware and software failures, power disruption, communications interference, etc.
  3. Human – riots, strikes, disgruntled employee, etc.
- B. Assess the affects from loss of information and services.
  1. Financial condition
  2. Competitive position
  3. Customer confidence
  4. Legal / regulatory requirements
- C. Analyze costs to minimize exposures.

IV. Evaluate critical needs.
- A. Functional operations
- B. Key personnel
- C. Information
- D. Processing systems
- E. Documentation
- F. Vital records
- G. Policies and procedures

V. Establish priorities for recovery based on critical needs.

VI. Determine strategies to recover.
- A. Facilities
- B. Hardware
- C. Software
- D. Communications
- E. Data files
- F. Customer services
- G. User operations
- H. Management information systems
- I. End-user systems
- J. Other operations

VII. Obtain written back-up agreements and contracts.
- A. Facilities
- B. Hardware
- C. Software
- D. Vendors
- E. Suppliers
- F. Disaster recover services
- G. Reciprocal agreements

VIII. Organize and document a written plan.
- A. Assign responsibilities
  1. Management
  2. Personnel
  3. Teams
  4. Vendors
- B. Document strategies and procedures to recover.
  1. Procedures to execute the plan
  2. Priorities for critical vs. non-critical functions
  3. Site relocation (short-term)
  4. Site relocation (long-term)
  5. Required resources
     a) Human
     b) Financial
     c) Technical (hardware and software)
     d) Data
     e) Facilities
     f) Administrative
     g) Vendor support

IX. Establish criteria for testing and maintenance of plans.
- A. Determine conditions and frequency for testing.
  1. Batch systems
  2. On-line systems
  3. Communication networks
  4. User Operations
  5. End-user systems
- B. Evaluate results of the tests.
- C. Establish procedures to revise and maintain the plan.
- D. Provide training for personnel involved in the plan's execution.

X. Present the contingency plan to senior management and the Board for review and approval.

Additional guidance is available in Chapter 10 of the FFIEC IS Examination Handbook. Also, many materials on contingency and disaster recovery planning have been published by trade associations, accounting firms, and the disaster recovery industry. These can be valuable guides to comprehensive contingency planning.