Rescinded 4/20/06 by RB 37-15. Click HERE to link to RB 37-15.

Department of the Treasury

Regulatory Bulletin

RB 32-21

RESCINDED

Handbook: **Thrift Activities**
Subject: **Management** **Section: 341**

Thrift Activities Regulatory Handbook Update

Summary: This bulletin provides an update to Thrift Activities Regulatory Handbook Section 341, Technology Risk Controls. Please replace existing Handbook Section 341, Information Technology, with the enclosed revised section. This bulletin rescinds RB 32-6 dated October 15, 1997.

For Further Information Contact: Your Office of Thrift Supervision (OTS) Regional Office or the Supervision Policy Division of the OTS, Washington, DC. You may access this bulletin at our web site: www.ots.treas.gov. If you wish to purchase a handbook and a subscription to the updates, please contact the OTS Order Department at (301) 645-6264.

Regulatory Bulletin 32-21

SUMMARY OF CHANGES

OTS is issuing an update to Thrift Activities Handbook Section 341. We provide a summary of all substantive changes below. Section 341 is in plain language as part of OTS's continuing effort to convert all guidance to plain language.

341 Technology Risk Controls

We changed the name of this section from Information Technology to Technology Risk Controls and made the following revisions to the narrative:

- Added a discussion of the trend towards greater reliance on local area networks (LANS) and wide area network (WANS), and the need to ensure appropriate security controls related to these systems.
- Highlighted the increased use of the Internet and the types of controls that should be in place to protect the integrity of information and avoid unauthorized access.
- Provided detail on how technology risk controls impact all areas of the institution and emphasized that the adequacy of controls should be assessed in all examination reviews.
- Added a section regarding requirements set forth in the Gramm-Leach-Bliley Act to cover protection of consumer information.
- Added a discussion of CEO memo No. 109, which requires notice to OTS prior to the implementation of a transactional website.

- In addition to background information on technology risk, we also provided guidance relating to each broad section of the revised examination procedures, such as information integrity, business continuity, vendor management, and management oversight.

The examiners should perform the procedures in the Technology Risk Controls Program as a part of each safety and soundness examination unless the institution is to receive an IT examination. We revised the procedures to allow for greater flexibility with regard to the depth of review. The procedures prompt examiners to focus on the institution's management of technology. The board of directors and management should take responsibility for managing the use of technology and should establish a control environment appropriate to the level of technological complexity and risk. Level I procedures outline the minimum review required to adequately assess the technology risk of each institution. In addition, examiners may eliminate some Level I procedures if there is adequate internal or external audit reviews of a particular activity or risk.

We modified PERK 005 to account for the changes in the examination program.

—Scott M. Albinson

Managing Director, Supervision

INTRODUCTION

Financial institutions operate in a technology-intensive industry. Almost all aspects of operations are automated and most business transactions are consummated without the exchange of currency. Instead, transactions are stored, processed, and transported electronically using information systems and technology.

Financial institutions have long stored information in electronic form. Historically, however, transaction entry remained largely a manual process, providing a traditional paper trail through which the accuracy of electronically produced output reports could be verified. Today, advancements in communication technology are increasingly replacing institution-controlled, paper-documented transactions with electronic entries initiated by customers, by telephone or PC, by merchants, through automated bill payment, etc. Financial institutions need new methods to control transaction input, to ensure its accuracy.

Institutions are also becoming more dependent on electronic information to make strategic and daily management decisions. Institutions use computer models to:

- Develop budget projections and business plans.
- To underwrite loans.
- To measure interest rate risk.
- To manage assets.
- To track trust accounts.
- To produce loan documents and consumer protection disclosures.
- To measure management performance.
- Manage virtually every other aspect of financial institution activities.

Increasingly, institutions download electronic data from third parties, such as credit bureaus, and run that data through a variety of internal electronic decision models. Institutions use the results to determine:

- Where to market their products.
- How to price them.
- Who to grant loans to.
- What the terms should be.
- When to cross-market other products.
- When to adjust credit limits or interest rates on individual accounts and by how much.
- To determine the most effective collection strategy.

As this dependence on electronic information grows, it is increasingly important to take appropriate measures to ensure the integrity of the input, to protect against corruption of the data or the programming, and to test the accuracy of the output.

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. Unauthorized parties may inappropriately alter Web sites or hackers may initiate denial of service attacks to prevent customers from transacting business. Electronic mail containing confidential or proprietary information may be distributed in error. Unauthorized parties might access networked systems that are directly connected to an institution's main operations database, revealing sensitive data.

At the same time, traditional information integrity and availability responsibilities and risks continue to be present. Management's responsibility to protect records from fires and natural disasters predates what we call technology, but the responsibility to safeguard the confidentiality of customers' records is the same whether that means physically restricting access to ledger cards and file vaults or establishing and maintaining logical access controls such as strong password and log-on practices to protect information stored in electronic form.

Institutions increasingly are seeking control enhancements to mitigate risks that impact data integrity and data availability, and provide new opportunities to remain competitive, enhance profitability, and improve customer service. Recent lessons learned from Year 2000 renovation work, use of the Internet as an alternate delivery channel, and regulators' emphasis on risk management processes are prompting institutions to give greater attention to planning for use and control of information technology.

The Year 2000 project was one of the most expensive and resource-intensive information technology challenges ever faced by the financial services industry. The project posed a technology-based problem that had to be managed on an enterprise-wide basis by more than technology experts. It transcended corporate boundaries and hierarchies and required organizations to work together to review information technology (IT) systems and business practices and develop a comprehensive strategy to address technology related risks and business continuity plans.

The financial institutions best prepared for Year 2000 shared common characteristics. Typically, these institutions:

- Had senior managers and directors who were committed to and involved in the project.
- Used interdisciplinary teams.
- Developed comprehensive IT inventories.
- Improved their vendor management practices.
- Prepared and tested detailed contingency plans.
- Strengthened internal controls and security.

These practices are also essential to the ongoing prudent management of information technology.

This handbook section, which supplements Section 340, Internal Control, describes a safety and soundness examination program to evaluate technology risk controls. If management does not identify and address technology risks, 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 the institution. You can use this examination program to determine if an institution's controls are adequate to reasonably ensure a safe, sound, and secure infrastructure for use of information technology. We generally refer to "you" as the safety and soundness examiner. When necessary, we make the distinction between Safety and Soundness (S&S) and Information Technology (IT) examiners.

INFORMATION TECHNOLOGY IN THRIFT INSTITUTIONS

Financial institutions have a number of choices available to meet their information systems and technology needs. Most OTS-regulated thrifts outsource most of their data processing functions to one or more third-party service providers; these are sometimes called "serviced thrifts." A much smaller portion of thrifts maintain internal data centers to run software licensed from vendors or developed in-house. Mixes or hybrids of these basic approaches are common. A thrift might contract with one service provider for its general ledger and deposit systems, with a second service provider for loans, and with a third for its web site. The same thrift might use licensed software for certain investments and interest rate risk analysis and might use complex spreadsheets developed in-house for some asset quality and board reports.

In addition to doing business with the primary and secondary service providers, most thrifts are interconnected with various other entities, such as ATM networks and automated clearing houses (ACHs), to process daily business. And, most thrifts now maintain one or more internal networks known as Local Area Networks (LANs) or Wide Area Networks (WANs). More and more of the internal networks are configured in a client-server environment.

Each of these arrangements requires a different type and level of management involvement with regard to data integrity controls, security measures, and business continuity plans.

Outsourcing

Almost all thrift institutions, including large entities, use outsourcing to some extent.

Contracts with service providers typically provide for a standard package of routine and standardized services and reports and allow for some special reports. Additional costs may be incurred for certain special reports or for nonstandard processing of standard reports.

Client institutions may request services and products beyond those provided for in the contract, for example, for a new deposit or loan product. Clients generally must pay extra for unique software requirements that are not enhancement priorities to the provider/ vendor and client-base at large. In these situations, institutions frequently build their own supplemental systems (for example, using PC-based applications) to augment outside products and services.

The delegation of data processing or other technological functions to a third party requires reasonable due diligence in selecting and contracting with service providers and vendors, and in monitoring performance. Conditions, rights, and responsibilities of the institution and the third-party service provider or 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.

Independent Service Providers

Contracting with independent service providers is common at thrifts of all sizes. An independent service provider can provide experienced staff, proven software, and reliable hardware that might otherwise be difficult if not cost-prohibitive for an individual thrift to maintain. However, the selection of an independent service provider is important. Most contracts are long-term, and it is important that the institution ensure that the service provider can deliver the appropriate type and quality of service that the institution will need over the life of the contract. If the service provider does not provide the needed services, or cannot promptly add services the institution needs later to meet market conditions, it may constrain the institution's operations. For example, its choice of loan products may be more limited than what changing competitive factors might otherwise dictate.

Similarly, dissatisfaction with a service provider will typically lead to a conversion from one data service provider to another. While converting to a service provider that better meets the institution's needs is a business decision, and not automatically a regulatory concern, conversions can be disruptive to the normal flow of business. Fees or penalties for early contract termination can be considerable. Appropriate upfront due diligence and planning should help institutions avoid unnecessary conversions.

Most serviced thrifts have one primary service provider and one or more secondary service providers. Typically, the primary service provider is responsible for (and paid for) ensuring compatible setups, connections and data transmissions with the secondary service providers as well as with other companies and entities included under the technology umbrella (for example, the ATM network).

Data is forwarded to the service provider's computer center, usually via on-line data entry terminals. Output reports are available at the institution's on-line terminals and printers, or in some cases, or for certain reports, hardcopy or microfiche reports may be delivered.

Client institutions are responsible for establishing and maintaining appropriate controls over those portions of the serviced systems that are under their control. For example, institutions should permit only tellers and other authorized personnel to use teller terminals. Other common controls that clients, rather than service providers, are responsible for include certain balancing and reconciling activities. Client responsibilities should be addressed in the contract and may be discussed in greater detail in other documentation from the service providers or independent auditors conducting third-party reviews (discussed later).

Thrift management is also responsible for ensuring that employees are properly trained on the systems they use and related control steps.

Affiliated Service Providers

Thrifts that are part of a holding company structure may have an affiliated company handle their technological needs. This may be a department of the holding company or a separate affiliated company. This frequently happens where there are several financial institutions with common ownership. The related institutions can eliminate some duplication of efforts and equipment and realize economies of scale.

Where there are such contracts or arrangements, Transactions with Affiliates provisions may apply. For additional information, see Section 380 of this Handbook.

In-House Computer Centers

In-house computer centers vary in size and complexity. Computer equipment may vary in size from large "mainframe" to smaller microcomputer systems. Also, the level of responsibility assumed by the institution can vary. Under the traditional in-house computer arrangement, the thrift would own the hardware and would be responsible for developing, maintaining, and operating the program. However, most banks and thrifts have implemented a hybrid arrangement, where they outsource some of the responsibilities traditionally associated with in-house systems.

One type of hybrid arrangement is often referred to as a turnkey operation. Under this type of set up, thrifts will acquire software from a third party, and run the software on equipment owned and operated by the thrift. One variation of a turnkey operation is when a thrift enhances the standard software to better suit their information needs. The additional programming is referred to as "surround code."

Facilities management is another type of IT environment occasionally seen in financial institutions. In these cases, the financial institution has an in-house data center, but employees of a service provider provide the programming and operate the systems.

Other "Internal" Technologies

Whether the institution's main data processing functions are handled internally or outsourced, some technologies common to most financial institutions have emerged in recent years.

End-User Computing

With the advent of PCs, thrift officers and employees began creating applications to supplement those provided by service providers or internal data centers. As PCs and software applications simultaneously became more powerful and easy to use, and downloading information from service providers and in-house data centers became more feasible, these business users, as opposed to IT professionals, created yet more complex "end-user" applications.

These business users may create new software programs or miniprograms or customize existing routines from vendor software. PC users originate data, download and manipulate information from main databases, and upload data to secure databases. Each of these activities can create information that management may use to make decisions that affect corporate strategies, customer relationships, and governmental reporting.

Management should take steps to implement and maintain control techniques for the programming, testing and documentation of end-user applications to ensure the integrity of the software and the production of accurate reports. TB 29, End-User Computing, contains more detailed guidance on basic controls that should be implemented and maintained in this area.

Computer Networks

The power of PCs also helped information processing to evolve well beyond the traditional central environment to decentralized or distributed networked operations. Most OTS-regulated thrifts have at least one internal network of PCs, whether the thrift is serviced or operates an in-house data center.

Computer networks offer substantial benefits in productivity and information access. A Local Area Network or LAN refers to a network that interconnects systems within a small geographic area such as a building, or even just a floor or portion of a building. Through PCs or other terminals, users have access to common systems, databases and software; communicate via electronic mail (email), and share peripherals such as printers. A Wide Area Network or WAN is a wider network that connects users in other locations. A thrift might have a LAN within its headquarters building and a WAN for its branches to communicate with each other and the home office. Other types of computer networks include MANs (Metropolitan Area Networks) and VPNs (Virtual Private Networks).

These networks provide high-speed interconnection and data exchange and facilitate communications within the institution and between the institution and the users (staff and customers). Some familiar on-line customer delivery application systems that are available to network users include telephone banking, PC banking, ATMs, automatic bill payments, and automated clearinghouse (ACH) systems for direct deposit or payment.

Institutions using LANs, WANs, or other types of computer networks need to have policies and procedures that govern the purchase and maintenance of hardware and software. They must also establish and maintain sound controls that allow reasonable access to data but also protect data's confidentiality and integrity.

For more detailed guidance, see CEO Memorandum No. 59, Risk Management of Client/Server Systems, which forwarded the interagency statement on this topic.

Electronic Banking and Internet Activities

Electronic banking encompasses customer services such as telephone banking and PC banking, whether the latter is conducted through a direct connection or over the Internet. General Internet activity refers to activity by thrift employees including browsing, downloading, or other Internet activity, using institution resources for purposes not related to the institution's Internet banking products.

Institutions that have any sort of electronic banking or Internet activities should be prepared to deal with unique information security matters through the advice and support of qualified employees or outside consultants. Institutions that provide retail electronic banking may refer to CEO Memo No. 70, Statement on Retail On-Line Personal Computer Banking, which alerts boards and management to risks and concerns in that area. The memorandum discusses strategic risk, legal/regulatory risk and operational risk as well as security and operations procedures. The memorandum also briefly addresses planning, testing, and monitoring.

As the industry has migrated from direct connect PC banking to Internet banking, the focus of this program (341) is on Internet banking or related activity that involves sending or receiving data using the Internet.

Internet Banking

Internet banking refers to the systems that enable financial institution customers to access accounts and general information on an institution's products and services through a PC or other intelligent device (for example, Internet-enabled wireless phones) in communication with a financial institution's Internet website.

An **Informational Website** provides general information about the financial institution's products and services, and is usually located on a separate server. Informational websites often highlight deposit and loan programs, list branch locations and hours, and provide "email" addresses for customers or the public to contact the thrift. Some informational web sites provide links to other web sites deemed of interest to their community.

For OTS's regulatory purposes, a **Transactional Website** is defined as one that allows customers to do one or more of the following activities:

- Access an account
- Obtain an account balance

- Transfer funds
- Process bill payments
- Open an account
- Apply for or obtain a loan
- Purchase other authorized products or services.

An **Internet-only Bank** represents a special case where the thrift's business strategy rejects the traditional bricks and mortar approach to banking. All or almost all transactions are conducted via the Internet or other electronic networks such at ATMs.

GRAMM-LEACH-BLILEY ACT, PROTECTION OF CUSTOMER INFORMATION

Section V of the Gramm-Leach-Bliley Act of 1999 governs privacy in the context of financial institutions. Subtitle A of that section, titled Disclosure of Nonpublic Personal Information, includes a "Privacy Obligation Policy" and addresses "Financial Institution Safeguards." More specifically, Section 501(a) states, "it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic information." Section 501(b) directs federal banking agencies such as OTS to "establish appropriate standards for the financial institutions subject to their jurisdictions relating to administrative, technical, and physical safeguards–

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to use of such records or information which could result in substantial harm or inconvenience to any customer."

On February 1, 2001, OTS amended 12 CFR Part 570 Appendix B in order to establish the standards required by Section V of the Gramm-Leach-Bliley Act. Appendix B to Part 570 outlines the Agency's expectations for the creation, implementation, and maintenance of an information security program. This program must include administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. The guidelines describe the oversight role of the board of directors in this process and management's continuing duty to evaluate and report to the board on the overall status of this program.

The four steps in this process require an institution to:

- Identify and assess the risks that may threaten customer information.
- Develop a written plan containing policies and procedures to manage and control these risks.
- Implement and test the plan.
- Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.

The guidelines also set forth an institution's responsibility for overseeing outsourcing arrangements.

OTS examination procedures include review activities to determine an institution's level of compliance with the recently enacted regulatory guidelines.

TECHNOLOGY RISK CONTROL ACTIVITIES

The level of technical knowledge required by boards of directors and senior managers varies depending on the size and nature of its operations, and by the degree of complexities within its technology environment. Nonetheless, directors and senior officers should have a clear understanding of the risks posed by technology, provide clear guidance on risk management practices, and take an active oversight role in monitoring risk mitigation activities.

Institutions must establish and maintain adequate functional control systems so management can identify, measure, monitor, and control information technology risks that could adversely affect performance or pose safety and soundness concerns. Similar to basic internal controls, institutions should design technology risk controls to prevent errors and problems that realistically can be prevented and to promptly detect and address those problems that do occur.

Risks, previously alluded to, may be grouped as following:

- Information Integrity Risk
- Business Continuity Risk
- Vendor Management Risk.

Although the volume and mix of risks will vary depending on the institution's technology environment, each of these types of risk is present at all thrifts. The board of directors and senior management must take steps to prevent, to the extent feasible, the exploitation of any of these risks and to quickly detect and resolve weaknesses and breaches.

Management Oversight

In addition to control activities already discussed, management and board of director oversight responsibilities includes:

- Planning for use of information technology.
- Establishing general control systems.
- Verifying (or auditing) those controls.
- Educating and supporting information technology users, including both staff and customers.

Planning and Implementing Information Technology

Technology is ever changing. From time to time, management will determine to upgrade various parts of its technology environment. This may entail adopting new technologies; upgrading hardware or software; or converting its "environment" (e.g., outsourcing systems previously operated internally or vice versa, or switching from one service provider to another).

Institutions should have an information technology plan that establishes the framework for the deployment and operation of technology. Management should update the plan annually to coordinate technology initiatives and activities to the business planning process. Technologies in place should be subject to periodic review to evaluate performance against current strategic plans and objectives, technological developments, and operating policies and procedures.

The substance and form of any formal plan will vary significantly, depending on the complexity of the institution's information systems and technology. The key element for you to consider is whether the information plan meets the institution's needs.

Management should also ensure that appropriate resources, including the correct mix of staff and a realistic amount of time, are brought to bear on program development or upgrade. A common misunderstanding is that limitations of the computer systems inhibit the development of high quality management information systems. In reality, management has sufficient flexibility under most computer systems to design a management information system that meets the needs of the institution. Therefore, business managers should play a significant role in the development and ongoing assessment of information systems.

General Controls

An institution should require additional data controls for technology that is used to process information. At a minimum, these data input and output controls should provide for accurate data preparation before data input procedures, and segregation of duties between the input of information and the review of that information after it is processed. Such controls generally require the reviewer to reconcile the processed information. In situations involving large-dollar transactions, institutions should require that certain functions be performed under dual control. Management should establish appropriate controls in the early stages of development and deploy-

ment and the institution's operating policies and procedures should describe them in detail.

Certain types of input data do not readily lend themselves to robust verification for accuracy and completeness by means of automated edits. Common examples are data from mortgage loan notes, new-account input forms, and PC-prepared spreadsheets. However, verification procedures may still be warranted, depending on the sensitivity or significance of the data or resulting output. Verification could consist of manually comparing the system output with the source document, or reviewing the data for reasonableness.

Information Integrity Risk

Information is one of an institution's most treasured intangible assets. A major performance factor for institutions is their ability to manage, safeguard, and optimize the use of customer and corporate data.

Information must be:

- Available
- Accurate
- Complete
- Valid
- Secure.

Information integrity concerns are sometimes expressed in the following terms:

Transactional Risk: This is the risk that weaknesses will cause errors to occur in transactions or will prevent a thrift from completing a transaction (or delivering products or services). Individuals may exploit weaknesses to perpetrate fraud via unauthorized transactions.

Reputational Risk: This is the risk that real and perceived errors and lapses in information technology compromise the customer's trust in the accuracy of their account records or the thrift's ability to safeguard the confidentiality of those records.

Compliance Risk: This is the risk that information technology weaknesses will manifest themselves in errors and omissions that cause the institution to be out-of-compliance with laws and regulations.

The weaknesses may or may not be strictly technological. For example, an interest rate risk model might create invalid results due to either faulty programming or inappropriate assumptions. Inaccurate information leads to bad management decisions. Similarly, individuals who perpetrate fraud through technological tools sometimes also employ simple deception – also known as social engineering – to gain passwords from unsuspecting employees.

To combat information integrity risk, the institution should have an active corporate information security program that delineates policy, standards, and management responsibilities. In addition to the policy statement, the program should provide for incident response to security exceptions (for example, employee violations and external unauthorized access attempts), security awareness, and training.

To maintain information integrity and confidentiality, management should establish and enforce controls that safeguard information from unauthorized access and use of data, provide for timely detection and correction of erroneous transactions, and provide for complete audit trails of transaction activity. Management should develop methods to maintain confidentiality, ensure the intended person receives accurate information, and prevent eavesdropping by others. In addition, both the sender and the receiver in a transaction should create undeniable proof of participation.

The scope of information security should address all of the institution's information technology activities, including personal computer activities, Internet-based electronic banking services, and processing by the institution's information service providers.

Effective security does not rely on one solution. Management should use several types of controls to manage information integrity risk:

- User-ID controls.

- Password controls.
- System log-on and log-off controls.
- Virus protection controls.
- Other controls to limit "powerful user" access.
- In some situations the institution will also need to use firewalls and encryption.

User-ID controls, along with password controls, are intended to restrict system access and promote user accountability. For detailed guidance, see CEO Memo 143, Authentication in an Electronic Banking Environment.

User-ID controls include the following:

- Approval: Management-level staff should approve the issuance of user IDs.
- Uniqueness: Each user ID should be identified with only one user (sharing of user IDs should be prohibited).
- Number of IDs per User: In general, each user should only have one user ID, to promote activity monitoring efficiency and employee accountability. Multiple user IDs are sometimes justified (for example, for technical support reasons), but related approval and monitoring controls should be in place.
- Expired or Discontinued Use: User IDs of terminated employees or expired authorizations should be disabled immediately and deleted from the system based on institution policy.

Password controls include the following:

- Length: Experts recommend a minimum of six characters for passwords.
- Composition: Passwords may be alphabetic, alphanumeric, or other. Many experts recommend alphanumeric passwords and avoiding common words like "password" and the names of professional sports teams. Note, however, that complicated passwords may cause users to write them down, especially if the employee needs several passwords to access different systems or applications, and thus compromise the password's confidentiality.
- Expiration: Users should change passwords on a regular basis. The more sensitive the system being protected by the password, the more often the password should be changed. Highly sensitive systems should require password changes at least every 90 days.
- Reuse: The institution should restrict reuse of previous passwords (for example, disallow reuse of the last five passwords used).
- Suppression: All systems should suppress the display of user passwords in any form.
- Encryption: The institution should ensure encryption of password files (the vendor usually encrypts password files for outsourced systems).

Maintenance procedures should ensure that only the user has knowledge of his or her password. Procedures should allow users to change their own passwords.

Access to sensitive data or powerful processing capabilities should require the use of a password. Institution management should promptly reverse temporary privileges, for example, additional access given to an "acting" teller supervisor or branch manager, when no longer needed.

System log-on and log-off controls should limit the number of unsuccessful log-on attempts a user can make. An added enhancement would be to notify the user, upon successful log-on, of unsuccessful attempts since the last log-on interval. PCs and other terminals should automatically log off after a period of inactivity.

Virus-protection controls include policies and software. Policies should restrict employees from importing software from high-risk sources, such as bulletin boards or informally obtained floppy disks.

The institution should install virus-protection software on all PCs and servers. Such software should be updated regularly to protect against new viruses.

The institution should establish **controls to limit powerful user access to system resources**. For example, the institution should appropriately limit

"Security Administrator" access, usually to no more than two persons, and the Security Administrator should not have access to customer records.

User Access

Authorized managers grant employees access assignments, which are information retrieval and transaction-processing capabilities. Authorized managers may also grant access to nonemployees such as consultants, vendor systems-support personnel, and others. For purposes of these procedures, "users" are employees and nonemployees who have authorized system access.

For outsourced systems, service providers may set up generic access assignments for various banking job categories in their access control software. In many cases, thrifts accept and use the vendor-provided access assignments without reviewing or questioning them. This practice increases the risk of inappropriate user access assignments, which in turn weakens controls over user access to sensitive data fields and powerful transaction processing capabilities.

To help ensure that user access assignments are appropriate, institution managers should:

- Identify the system's sensitive customer-record fields (such as account activity status, social security number, and mother's maiden name) and powerful transaction processing features (such as account-linking capabilities and the ability to increase overdraft limits).
- Assign job responsibilities that provide for proper segregation of duties and dual control over sensitive fields and transactions. Institutions should require dual control when using the system's "supervisory override" capability (for example, when approving a transaction keyed-in by a supervisor).
- Assign user information retrieval and transaction processing capabilities according to employees' defined job responsibilities. This step produces user "access profiles."
- Authorize and forward the access profiles to the information security officer for implementation in the system.

If you find any inappropriate user access assignments, determine if the condition was caused by either of the following:

- Control deficiencies in the granting of user access assignments.
- Deficiencies in the system's security controls (system rules or software).

Common deficiencies in security software controls include:

- Deficiencies in implementing certain security software rules. A common example is the inappropriate grouping ("bundling") of transactions by information security officers who maintain the security software. In such cases, large numbers of transaction screens are inappropriately bundled to ease the burden of maintaining security access rules. However, bundling gives many users more system access than required by their job responsibilities.
- Deficiencies in the use of the system's supervisory override feature. In such cases, the dual control (supervisory override) capability of the software has not been properly invoked over certain sensitive fields (such as the dormant-account status field) or powerful transactions (such as the ability to increase an overdraft limit).
- Inherent security software deficiencies. For example, the security software cannot restrict access to certain fields within a record. That is, a user granted access to a record could view or update any field in the record. To alleviate this problem, some companies create additional programs to enhance the capabilities of the basic security software.

Management should determine the frequency of user access assignment reviews. These reviews should be performed at least annually. Management should document these reviews to evidence the performance of the review and approval of changes made.

Firewalls

Firewalls are a combination of hardware and software placed between two networks through which

which all traffic must pass, regardless of the direction of flow. They provide a gateway to guard against unauthorized individuals gaining access to an institution's network. Institutions should consider firewalls for any system connected to an outside network.

Nonetheless, a firewall does not ensure that a system is impenetrable. Firewalls must be configured for specific operating environments and the institution must review and update firewall rules regularly to ensure their effectiveness.

Encryption

Encryption is the scrambling of data so that it cannot be read without the proper codes for unscrambling the data. Confidential or sensitive data should always be encrypted when being sent over the Internet and the sender and receiver of the data are not behind the same firewall. This includes email containing confidential and/or sensitive information as well as Internet Banking transactions.

Management should perform a risk assessment to identify types of sensitive data requiring protection and determine the type and strength of encryption to use for various protected communications. The assessment should include databases and password files.

Other Controls

Other information controls that an institution may use to safeguard information integrity include:

- Secure data storage (sensitive data is encrypted; access is stringently controlled).
- Acknowledgement practices (batch totals, sequential numbering and one-for-one checking against a control file can be used to verify that a transaction is complete or has not been interrupted).
- Modem sweeps (efforts to locate and remove unauthorized modems).
- Physical controls (secure storage of hard copies of sensitive data; locks, alarms, etc.).
- Audit procedures (discussed later in this section).

In sum, management should periodically perform a thorough update of its information integrity risk profile and select the appropriate mix of controls to monitor and manage that risk.

Business Continuity Risk

Financial institutions need to be prepared to resume operations as quickly and efficiently as possible after a disaster or other adverse incident. In an Internet environment, these threats may include the loss of Internet access by the institution or loss of access to the institution via the Internet by its customers.

Business continuity risk for an institution relying on one or more service providers includes the risk that it will not be adequately prepared to execute its disaster recovery responsibilities in the event of a disaster affecting the service provider, thereby delaying complete recovery of the institution's financial records. (*Note*: The risks associated with routine service provider system outages are generally low and are not addressed in this handbook section.)

In the context of internally operated systems, business continuity risk is the possibility that the institution will not be adequately prepared to promptly recover from a disaster affecting the computer hardware and software it owns and operates, resulting in significant losses for the institution.

An institution-wide contingency plan provides for timely business continuity if there is disruption to the institution's information technology. 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 and risks to the viability of the organization. Institution management should establish and maintain disaster recovery plans that address all of its mission-critical systems whether those are operated internally or outsourced. Overall, the extent of a preparedness plan will depend upon the level and

complexity of information technology and the institution's available resources.

Management should establish requirements for all operating departments to establish disaster recovery plans for their respective areas of activity. The policy may describe the required components of an acceptable disaster recovery plan (for example, individual responsibilities, resources to be recovered, backup location, and time-line for recovery).

The contingency plan should cover the following areas:

- Define the roles and responsibilities for each team member in the event of a problem situation.
- Identify the risks posed by each system deployed.
- Detail strategies and procedures for recovery.
- Establish criteria for testing and maintenance of plan.
- Identify the principal departments, resources, activities, and constituencies potentially affected by a problem.
- Assess the response capability of key disaster recovery service.

Management should formally appoint and empower individual(s) with the latitude and authority to respond during an incident.

A full understanding of the recovery time line is essential. Full recovery, for example, is usually not achieved when the affected system(s) come "back up" or "back on-line." The institution may have to correct transactions that were in process when the disaster or other disruptive event occurred. In some cases, the institution may have to track down and re-enter the entire day's worth of business.

Management should periodically test and update the contingency plan as needed. Management may accomplish this testing through walk-throughs, tabletop simulations, or other exercises.

OTS's CEO Memorandum No. 72 forwarded the "Interagency Policy on Corporate Business Resumption and Contingency Planning." This package lists a 10-step process that institutions may find helpful in developing contingency plans. The FFIEC IS Examination Handbook (1996; Chapter 10) also discusses contingency planning.

Although management is responsible for institution-wide contingency planning, they should consider different factors depending on whether a particular system is outsourced or internally operated.

Outsourced Systems

Disaster recovery plans for outsourced systems should provide for the following:

- Recovery of lost data for re-submission to the service provider (i.e., day-of-disaster online input).
- Management-approved timeline for completion of recovery.

It is the service provider's responsibility to provide a recovery plan for its computer processing capabilities in the event of a disaster affecting its computer resources. Management should obtain and review (relevant portions of the) contingency plans of its service provider(s):

- To determine that the institution is reasonably protected.
- To ensure that the institution-wide contingency plan is compatible with its service providers' plans.
- To supplement the external contingency plans with appropriate steps the institution itself should take.

The institution's contingency plans for systems involving service providers should do the following:

- Identify all the categories and sources of data input into the service provider's systems by the thrift. Usually, these items are limited to branch and back-office online terminal input. Other items of input, such as automated teller

machine (ATM) transactions, automated clearinghouse (ACH) transactions, and in-clearings ("on us" checks negotiated outside of the institution), are usually the responsibility of vendors that provide the respective processing services.

- Describe the steps required to recover previously input data and prepare them for resubmission when requested by the service provider. (Institution management should realize that if the disaster takes place on a business day, online data entered on that day will not have been backed up offsite and will likely be lost.)
- Identify the persons or teams responsible for executing the recovery steps.
- Provide a management-approved time line showing key points, from the point of receipt of notification that the service provider has experienced a disaster to the completion of the preparation of input for resubmission.

Internally Operated Systems

The institution needs additional disaster recovery steps for internally operated systems, especially in the area of backup. The plans should provide for the recovery of key resources, including the infrastructure (computer and operating system software), application software, and data (previously backed up data and day-of-disaster data), as well as, one or more alternate work areas/locations.

Disaster recovery plans for internally operated systems should provide for the following:

- Recovery of lost data (for example, day-of-disaster online input).
- Replacement of damaged resources (such as hardware and software.
- An alternate processing location.
- A management-approved time line for completion of recovery.
- Testing and periodic updating of the plans.

"Recovery" is defined as the point at which application system records (for example, customer balances) have been brought to current status. The recovery time line should provide a breakdown of the various phases of recovery and corresponding elapsed time for each phase of the recovery process.

The institution should periodically copy and store certain data and software components of a system at a prudently distant or remote location to facilitate recovery efforts in the event of a disaster. The institution should perform periodic tests, and resolve within an appropriate time period, any problems the tests reveal. In particular, the tests should verify that the backup files are readable, that is, not corrupted by a record-writing problem. Management should document backup procedures and keep a current inventory of files maintained at the backup site(s).

Vendor Management Risk

Vendor management risk is the risk that the service provider will not perform the contract terms and conditions as specified, causing undesirable consequences for the institution's operations.

When employing the services of an outside service provider or software vendor, management should carefully review proposed service contracts or agreements or renewals thereof to minimize the institution's exposure to risk. Legal counsel should review the draft contract to determine if the interests of the institution are adequately protected.

Before entering into contracts, management should assess and review the following factors:

- Alternate vendors and related costs.
- Financial stability of the vendor.
- Capacity of vendor to stay current with industry developments.
- Requirements for contract termination.
- Contract provisions allowing examination of the vendor.

For detailed guidance, see CEO Memo 133, which details the FFIEC standards for Risk Management of Outsourced Technology Services, and TB 46,

Contracting for Data Processing Services and Systems.

After signing a contract for services, management should maintain close oversight of the institution's relationship with the vendor. The institution should establish a contract administration process to ensure that the vendor fulfills its contractual obligations.

Most IT-related contracts specify performance measures for the products or services provided by the vendor. Two common and important measures are online "up time" and "terminal response time." These performance measures generally have a high impact on the institution's business processes, customers, and employees.

Up time usually refers to the hours and days that online services will be available to the institution. For IT-related contracts, these hours are often the institution's branch operations hours plus two or three additional hours daily. IT contracts should stipulate the vendor's commitment to achieve a high, ongoing level of performance (for example, "99% up time").

Terminal response time usually refers to the standard elapsed time between a user request (for example, the moment when the user presses the Enter Key) and the delivery of information to the user's terminal screen. Current response time standards range from three to five seconds.

In addition, contracts often specify nonproduction-related "deliverables" (products or services) that may enhance the value of the contract for the client. Deliverables may include:

- Commitments to provide the institution with system performance reports.
- Audited financial information.
- Summaries of disaster recovery test results.
- Third-party operations audit reports.
- Other useful materials.

Management should monitor vendor performance. Performance level reports supplied by the service providers should be verified, at least occasionally. Receipt of special services should be verified and payment approved by the business unit receiving those services or the unit monitoring vendor performance. Delivery of nonproduction deliverables should also be monitored. Senior management should be informed promptly of significant deficiencies in vendor performance.

Audit

Institution management is responsible for design and maintenance of a sound system of internal controls that include information technology. The scope of the examiner's assessment of technology risk controls will vary depending on adequacy of the audit function to test and report on those controls. How formal the audit plan is and whether audit work is conducted internally or by external auditors will depend on a number of factors including the institution's size, operations, and technology environment. However, management must ensure that qualified independent (internal and/or external) individuals periodically assess basic technology controls.

The audit plan should provide for review of information technology risks in operations and management activities. This is consistent with an institution's priority to ensure the accurate processing of information, privacy of financial and customer records, and continuation of service in case of business interruptions. In developing audit programs, the institution must consider the full scope of each application to protect financial and information assets, system reliability, and user confidence.

The audit function should cover the flow of critical data through interrelated systems and should generally include the following:

- Tests of balancing procedures of automated applications, including the disposition of rejected and unposted items.
- Periodic samples of customer record files (master files) to verify them against source documents for accuracy and authorization.
- Spot-checks of computer calculations, such as interest on deposits, loans, securities, ARM calculations, service charges, and past-due loans.

Some of these audit functions will not be conducted separately as a "technology" audit but may be incorporated into audits of specific departments or lines of business.

Thrift clients of service providers should obtain "third-party reviews" and take appropriate action in response to control considerations or weaknesses addressed therein. A "third-party review" is a type of independent audit designed to meet the audit needs of financial institutions without overburdening the service provider. That is, without this vehicle a service provider that processes work for several financial institutions could be subject to redundant audits by audit firms for each of its clients. A qualified auditor who is independent of both the service provider and the serviced institutions conducts the third-party review.

The scope of the audit should be detailed enough to satisfy the audit objectives of the serviced institutions and the servicer. The American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) Number 70 provides guidance for external auditors auditing the servicer as well as for those auditing its financial institution clients. In general, the third-party review audits should determine the adequacy of controls in all areas of the data center, including computer operations, systems and programming, and input/output controls.

Many of the controls that the third-party auditor is to check at the service provider have companion pieces at the individual financial institution. In the third-party review report the auditor typically will address corresponding controls, sometimes known as "client control considerations" that should be maintained at the thrift institution. OTS and FFIEC reports covering service providers may also contain client control consideration. You should review these reports as part of the initial assessment of the institution's IT environment.

Training

Institutions must educate and support customers and staff to achieve user acceptance of and confidence in information technologies. Institutions should provide training so participants 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 help-line or customer service representatives, should be kept informed of changes and updates to systems. They should be trained on how to execute disaster recovery plans. Management should also provide backup training for key job functions so that human emergencies will not disrupt service.

Internet Activities

The information integrity, business continuity, vendor management, and the management oversight control activities discussed thus far in this chapter pertain to all types of information technologies including Internet activities. This section discusses risks and controls specific to Internet banking and other Internet activities.

Internet Banking

The level of risk posed by Internet banking depends in part on whether the web site is informational or transactional, and if the latter, the nature of the transactions the customer can effect. Informational or information-only web sites are less risky, but not without their vulnerabilities. The web site, for example, may be vulnerable to alteration, so management should establish controls to prevent unauthorized access.

Configurations that provide for electronic mail between the thrift and its customers require additional controls, such as encryption, to protect the confidentiality of customer's accounts and other sensitive data. Customers should be forewarned about including sensitive data such as account numbers in unprotected emails to the institution. Customer passwords rules should be structured to minimize the potential for unauthorized access. For example, institutions should not use readily

available customer information for the initial default password, such as, social security number, customer initials, etc. Configurations that permit transactions, including balance/account inquiries, require yet more controls.

OTS-regulated institutions intending to establish a transactional web site must file a notice with OTS at least 30 days in advance of the site opening for business. If an institution implemented a transactional web site since the previous examination, examiners should determine that the institution filed a notice with the appropriate OTS regional office. Examiners should contact the regional office to determine if there were any issues that require a follow-up review.

In planning a transactional web site, it is important to consider the implications on the long-term goals and strategy of the institution and to have input from all of the parties impacted, including managers from both the business and technology sides of the organization, other internal users, auditors, and customers. Planning should begin with a thorough review of objectives to achieve and areas of risk associated with the new activity.

Financial institutions often contract with outside providers to help plan, implement, and maintain Internet banking services. If this is the approach used, institutions should exercise care in selecting a service provider. Also, institution management should give someone in the organization responsibility for monitoring and overseeing their performance on an ongoing basis. In this regard, it is crucial to negotiate a contract that clearly addresses both parties' rights and responsibilities.

Security and internal control are major concerns. Data encryption and digital certificates issued by a reliable certificate authority can be used to protect data and verify the identity of parties communicating online. See CEO Memo 143, Authentication in an Electronic Banking Environment for more detail. An array of firewalls and intrusion detection systems are available to help protect data from theft or alteration. It is important to recognize, however, that those systems do not provide complete protection from attack, and all must be continually monitored and maintained. It is also important to augment electronic security measures with adequate physical security and procedural controls. When adding a transactional web site, institutions need to review and update access to PCs and data, power protection, back-up files, physical locks, security guards, and other common security measures.

Institutions should anticipate the consequences of high demand for electronic services or interruption of service. Institutions should update contingency and recovery plans to address the new activities.

Before opening the transactional web site for use by customers, institutions must update and approve policies and procedures, train employees, and thoroughly test the systems. A plan for periodic risk assessments and audit review should also be in place. Institutions should schedule periodic testing by independent experts in computer security issues, and obtain and review such tests that are conducted for the institution's service providers.

Consumer Compliance and Privacy Issues in Internet Banking

The institution must address consumer compliance and privacy issues in the context of online business. Compliance and legal staffs should review and update procedures for information posted to the web site and all types of transactions to be conducted online. CEO Memorandum No. 90, dated July 23, 1998, regarding Interagency Guidance on Electronic Financial Services and Consumer Compliance may be helpful. See § 573 of the OTS Regulations regarding Privacy of Consumer Financial Information.

General Internet Activities

Management should have policies and controls in place to govern the general Internet activities of its employees. These should include:

<u>Software import</u>: Rules designed to minimize risks (viruses, or other damaging program code) associated with the downloading of software over the network or other sources.

<u>Browsing the Internet</u>: Rules should require the browser to be configured to only access the Inter-

net through a designated firewall and restrict the downloading of certain files.

Encryption: Encryption may be needed to protect sensitive information in transit, such as electronic mail messages, a file being downloaded, or information in storage (for example, databases).

EXAMINATION COVERAGE

Examination coverage for technology risk controls is assigned for each thrift OTS regulates. In general, information technology (IT) examiners review technology risk controls at Internet-only thrifts and those institutions that host their own web sites or that otherwise have complex operations and activities or difficult or non-routine situations. Safety and soundness (S&S) examiners review technology risk controls at the remainder. This remainder actually represents the great majority of thrifts. Most serviced thrifts will have their technology risk controls evaluated at a regular examination by an S&S examiner, but S&S examiners may also examine other thrifts, including some with in-house data centers or mixed environments.

The regional offices will determine when to assign IT examiners by considering the following factors:

- Recent or pending systems conversions.
- Recent or pending mergers and acquisitions.
- Volume and nature of in-house IT operations.
- Existence of novel or complex applications, systems, networks, or equipment.
- Volume and nature of servicing or software from non-examined entities.
- Problems and concerns at previous examinations.

These factors do not automatically require the presence of an IT examiner, but are indications that may warrant further consideration of such. Similarly, the preceding list does not illustrate the universe of situations that may require the involvement of IT examiners. You should consult with the Regional IT Manager on technology concerns that arise during planning, scoping, or conducting an examination. Such consultation helps ensure proper evaluation and consistent regulatory treatment.

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. Consult with your Regional IT Manager if you have any questions about technology risk exposure.

Expanded investigation and analysis may be necessary for some situations, especially significant internal control weaknesses. The examiner completing this program, the examiner in charge (EIC), the Regional IT Manager, and other appropriate regional staff should determine what additional procedures are needed, who should perform them, and whether to do them at the current examination or at a future safety and soundness or IT examination.

S&S examiners should review technology risk controls at all thrifts that are not examined by IT examiners. Technology may have a positive or negative effect on customer service and operating efficiencies, depending on what technologies are employed and how. The availability or unavailability of data and its completeness and accuracy affect decisions in every area of operations. The board of directors and management cannot delegate responsibility to service providers, software vendors, or in-house technology staff, but must ensure that adequate controls exist throughout the organization.

The review of technology risk controls is not a stand-alone task completed by just one examiner. Throughout the examination, all examiners assess the quality and reasonableness of data provided by the institution. For example, examiners evaluating asset quality depend on accurate and complete records of originations, delinquencies, and concentrations for just a few examples. Instances of data that appears questionable or inconsistent and instances of weak controls should be pursued and adverse findings should be relayed to the EIC and the examiner completing Program 341.

In addition, examiners should be sensitive to how the adequacy of the institution's management of information technology can impact our evaluation of each of the CAMELS areas. Listed below are examples of various aspects of information technology and how they impact the CAMELS components.

Capital and Earnings: Information technology may have a positive or negative impact on earnings and capital. The outcome is influenced by several factors.

- Appropriate use of technology can help thrifts improve profitability and ultimately build added capital. On the other hand, adverse impacts could take place if technology acquisitions that are not well coordinated fail to achieve business plan requirements.
- Successful information systems conversions result in meeting tangible and intangible benefits. Poorly executed systems conversions can create large quantities of unposted accounting entries. The resources and time needed to research unposted items increase expenses, and delays in clearing the entries may result in increased charge-offs and dissatisfied customers.
- Using outside vendors may reduce the thrift's capital investments, but may also unnecessarily increase annual expenses and reduce control and flexibility over processing. Long duration contracts with vendors pose risks to a thrift's future earnings and overall performance if the contract process is not closely tied to the corporate business planning.
- Appropriate processing controls are needed to ensure proper reporting of the Thrift Financial Report and various SEC filings.

Asset Quality: Institutions use information technology extensively for processing new loan applications, servicing large pools of loans, and monitoring loan portfolios in a competitive marketplace. Other aspects of automation include the real estate appraisals, loan approval processes, and secondary mortgage activities.

Areas involving technology risks may include:

- Decision support software such as credit scoring used to enhance the credit granting process.
- Internet-based delivery channels.

Management: CEOs and boards of directors are increasing their involvement in information technology decisions. Technology touches every aspect of the institution's operations, and impacts earnings, capital, liquidity, and asset quality:

- Risk management processes, for example, vendor management; information security; contingency planning; project management, may be less robust in small institutions.
- Quality of management information systems.
- Other thrift activities such as general ledger reconciliation, system balancing, and clearing of suspense items. These depend on or affect information systems operations. This includes an institution's internal controls.

Liquidity and Sensitivity: Information technology serves a significant role in cash management. Disruptions could impact customers, cause operating losses, cause an increase in borrowings to offset any cash shortfalls, and place a heavy burden on existing staff to correct the problems.

Technology risks are inherent in all of the following:

- Paper-based cash collections, including check processing, lock-box arrangements, and clearing house activities.
- Electronic based cash collections, including electronic funds transfers such as ATM transactions, ACH, wire transfers, and purchases made with credit or debit cards.
- Management decision-support software used to determine thrift's asset liability mix and balance sheet structure.
- Internet-based delivery channels introduce new technology environments with different kinds of risks, including the potential for a more volatile deposit base.

The review of technology risk controls is not confined entirely to Safety and Soundness or Information Technology examinations. Information technology also supports records and activities reviewed during Compliance and Trust examinations. For example, Truth-in-Lending documents disclosing Annual Percentage Rates and Finance charges commonly are prepared by electronic loan documentation programs and trust administration activities are often automated. Incorrect programming or data entry could result in improper disclosures or untimely action. Again, consult with your Regional IT Manager if you have questions about technology risks in these specialty areas.

Finally, where aspects of a thrift's information technology environment are provided or managed by a holding company or other affiliate, you may need to coordinate the review of some controls with another federal banking agency. Nonetheless, while you should avoid duplication of regulatory oversight, the thrift itself must maintain appropriate internal technology risk controls, which you should assess when completing this program.

EXAMINATION PROGRAM

OTS examinations are risk-based and provide for a comprehensive approach to information technology risks. You use a top-down methodology by determining the information technology environments and risks, evaluating management oversight and control activities, and assessing significant unmitigated risks.

The risk-based examination approach relies on audit work and results that match regulatory needs (for example, audit scope, objectives, and evidence and timing of work). One key criterion is whether or not there is evidence of independent testing and reporting on management policies and operating procedures. If there is no audit to rely on, you will need to perform adequate testing to support conclusions.

"Audit" here refers to the type of work being performed, not the job title of the person doing the work. While internal or external (independent) auditors may complete this work, in many situations, other employees may also perform audit work.

Examination Comments and Rating

You should generally incorporate examination findings and conclusions about Technology Risk Controls into the Management section of the safety and soundness report. ***At a minimum, the report should include a brief description of the institution's use of information technology and an overall conclusion as to the adequacy of controls. You should describe significant adverse findings in sufficient detail to identify specific conditions that warrant corrective action by the institution. Carry forward a summary of such findings to the Examination Conclusions and Comments page.***

The strength or weakness of Technology Risk Controls is one of several factors you consider in assigning a rating to the Management component of CAMELS. You should consider all of the following:

- 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.
- Anticipated expansion of products, services, or platforms.

Generally, if you identify serious deficiencies with the controls, the management rating should reflect such findings.

OTS Information Technology Database System

The OTS Information Technology Database System provides management information on the industry's data processing activities. This database tracks information on each thrift institution's information technology and electronic banking environment. The database also captures information, for example, name, address, and types of services, on the institution's service providers and software vendors.

Data collection and data verification is handled during the regularly scheduled safety and soundness examination or an information technology examination. The data is collected from the PERK. The S&S or IT examiner should review the information for completeness and accuracy and forward it to the regional office for entry into the database.

REFERENCES

Code of Federal Regulations (12 CFR)

§ 555	Electronic Operations
§ 568	Security Devices and Procedures
§ 563.17	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 563.190(c)	Bonds for Directors, Officers, Employees, and Agents

Part 570

Appendix A	Interagency Guidelines Establishing Standards for Safety and Soundness
Appendix A, II. A.	Internal controls and information systems
Appendix A, II. B.	Internal audit system

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 and Systems
TB 50	Regulatory Review of Certain Third-Party Contracts
TB 59	Interagency Supervisory Statement on EFT Switches and Network Services
CEO Memo 59	Risk Management of Client/Server Systems
CEO Memo 70	On-Line PC Banking
CEO Memo 72	Revised FFIEC Policy Statement: Corporate Business Resumption and Contingency Planning
CEO Memo 109	Transactional Web Sites
CEO Memo 133	Risk Management of Technology Outsourcing
CEO Memo 143	Authentication in an Electronic Banking Environment

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

Technology Risk Controls Program

Examination Objective

To assess the extent to which management identifies and mitigates the institution's primary information technology (IT) risks.

Examination Procedures

Technology risk controls essentially are internal controls that an institution should build into daily operations. This program complements traditional examination procedures in the evaluation of specific activities, such as lending, deposit-gathering, and nondeposit activities. You may need to contact examiners in other examination areas to comprehensively evaluate an institution's activities. In addition, you should coordinate efforts to review written policies, internal controls, and other related functions.

If you note problems or unusual factors, consider referrals to information systems, compliance, and other examiners (for example, capital markets specialists). You may also consult with the Regional IT Manager whenever you need additional technological information.

Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Procedures in this program provide for the review and evaluation of a financial institution's compliance to guidelines establishing standards for safeguarding customer information that implement sections 501(b) and 505 of the Gramm-Leach-Bliley Act (GLB). The Interagency Guidelines Establishing Standards for Safeguarding Customer Information is in three parts consisting of: I. An introduction that describes the scope of the guidelines. II. Standards for Safeguarding Customer Information. III. Development and Implementation of information security program.

Part I - Scope: The guidelines apply to customer information maintained by or on behalf of entities over which OTS has authority. These entities are savings associations whose deposits are FDIC insured and any subsidiaries of such savings associations, except brokers, dealers, persons providing insurance, investment companies, and investment advisers.

Part II – Standards: (A) The savings association shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the savings association's size and complexity and the nature and scope of its activities. (B) The savings association shall design the information security program to ensure the security and confidentiality of customer information, protect it against anticipated threats, hazards, and unauthorized access that could result in substantial harm or inconvenience to any customer.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Part III – Development and implementation of information security program: Describes the regulatory agencies' expectations for the creation, implementation, and maintenance of an information security program, consisting of the following:

A. Involve the Board of Directors

B. Assess risks to customer information

C. Manage and control the risks

D. Oversee related service provider arrangements

E. Adjust the information security program, as necessary.

F. Provide a written report to the board regarding the status of the program

G. Implement the (GLB guideline) standards by July 1, 2001.

To evaluate management's compliance to the GLB guidelines, we include and identify the guidelines in Level I and II procedures under Audit, Management Oversight, Information Integrity, Business Continuity, and Internet Banking.

Wkp. Ref.

Level I

1. Ascertain the institution's IT environment and risks. Review the following documents:

   - Standard scoping materials (prior ROE, Regulatory Profile, supervisory correspondence).
   - Preliminary Examination Response Kit (PERK 005), including information related to the Information Technology Database (ITD). Review ITD data for completeness and accuracy. Forward a copy to the regional office according to local instructions.
   - Internal or external audit reports, third-party reviews, and client control letters.
   - Examination reports (by OTS or other FFIEC agencies) pertaining to the institution's IT environment (service providers, software vendors and others).

   _____ _____

2. Gain an understanding of the institution's IT environment and risks, including:

   - Identify mission-critical systems.
   - Develop an understanding of the IT infrastructure, including Local Area Networks (LANS), Wide Area Networks (WANS), and other IT resources.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Obtain information on recent, current and planned major IT projects, such as systems conversions, the introduction of a new product, or the introduction or expansion of electronic banking (including websites).

_____ _____

Audit

3. Assess the adequacy of audit coverage of the institution's IT-related risks and management's responsiveness to audit issues.

   - Determine whether IT audit plans, schedules, and/or audits completed since the preceding examination are commensurate with the institution's IT environment and IT-related risks. The institution should regularly schedule evaluations of the information security program. (GLB III-C)
   - If audit plans and schedules are appropriate:
     - Determine whether audits have been performed according to plan.
     - Determine whether audits have appropriately addressed the risks identified in this program.
   - Determine whether significant audit concerns are timely reported to senior management and the board of directors.

_____ _____

4. Assess management's overall responsiveness to audit concerns, including the timeliness of corrective action.

_____ _____

5. Determine whether other examiners identified significant IT-related issues such as deficiencies related to data integrity, computer models, or information security in areas of their review. If so, investigate the underlying cause(s) and implications. Consult with the examiner in charge and, if appropriate, the Regional IT Manager.

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

If the thrift has well-qualified staff that conduct a thorough audit of technology risk controls (including the assessment of compliance to GLB information security guidelines), and management responds quickly and appropriately to audit and examination issues, you may conclude this Program now or selectively complete other Level I procedures before concluding.

If an internal or external audit covers technology risk controls, but one or more aspect is weak, lacking, or out-of-date, continue within Level I, and select and complete procedures that correspond to the situation at hand.

If there is no independent review of technology risk controls by an internal auditor, external auditor, or another qualified individual, generally you should complete all of the remaining Level I procedures.

If Level I procedures reveal or suggest weaknesses, complete corresponding Level II procedures.

You may also selectively complete Level II procedures to test Level I findings.

Management Oversight

6. Determine whether the institution has an IT plan appropriate to the size and complexity of its technology environment. Determine whether the board approved the plans, and whether the approval process ensures that the IT plan aligns with the business plan.

_____ _____

7. Review minutes of board and management meetings for evidence of involvement in and approval of significant IT matters. Board minutes should reflect the review and approval of the institution's written information security program and continued oversight over the maintenance of the program. (GLB III-A)

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

Information Integrity

8. Review guidance for employees pertaining to the need to protect the integrity and confidentiality of customer and corporate information. Such guidance may describe the employee's responsibilities and consequences of improper actions. It may also give examples of improper activity, such as, the unauthorized disclosure of customer account information.

_____ _____

9. Determine whether an adequately designed information security program has been established for the institution (GLB III-G requires implementation by July 1, 2001). Information security policies, procedures, and standards now in operation provide for the following (GLB III-B and III-C):

   - Implementation and periodic adjustment of a risk assessment process pertaining to customer and corporate information.
   - Controlled assignment of user access to customer information and sensitive corporate data.
   - Monitoring of access to and use of sensitive or powerful system capabilities (such as the ability to override overdraft or check-cashing limits).
   - Internet services access controls.
   - Data input quality controls (for new accounts, the interest rate control file, and spreadsheets).

_____ _____

10. Review a sample of user access profiles for conformance to policies and procedures. Include sample profiles of teller, back-office, and security administrator access for at least one of the institution's primary systems (such as the deposit, mortgage loan, general ledger system, or Fedline).

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

Business Continuity

11. Assess the overall policy for disaster recovery (Business Continuity and Business Resumption) to determine management's requirements for departments or other operating units to establish, maintain, and test plans for their areas.

_____ _____

12. Review the institution's disaster recovery plans for one or more mission- critical systems and determine if the plans provide for the following (GLB III-C):

    - Recovery of lost customer and corporate data.
    - A management-approved time line for completion of recovery.
    - Testing and periodic updating of the plans.

    For internally operated systems selected, also determine if the plans provide for:

    - Replacement of damaged resources (such as hardware and software).
    - An alternate processing location.

_____ _____

Vendor Management

13. Determine if the institution established adequate vendor-related policies. Ensure that the institution exercises appropriate due diligence in managing and monitoring its service providers. Confirm that the thrift maintains effective information security programs to protect customer information.

_____ _____

14. Assess the institution's controls for monitoring its primary service provider's service-level performance.

    - Determine whether the institution periodically verifies the service-level performance reports supplied by the service provider.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Determine whether executive management is promptly informed of significant deficiencies in vendor performance.

_____ _____

Internet Banking

Thrift institutions generally outsource the implementation and operation ("hosting") of Web sites to one or more Internet Service Providers (ISPs). We limit the scope of this program to the review of controls thrift management established to minimize the risk of operating within an internet environment. However, hardware and software controls related to operation of the ISP service are not within the scope of this program.

If the institution hosts its own web site (i.e., the thrift operates its own computer and software to support its web site), an IT examiner should assess the associated controls.

15. Assess the institution's Internet-related information security controls.

- Determine whether the institution is prepared to deal with Internet information security matters through the support and advise of qualified employee(s) or outside consultants.
- Determine whether the thrift has established policies and standards related to the use of Internet facilities and services by its employees. The policies should indicate the user authorization process, the Internet services allowed, and the need for controls such as authentication, firewalls, and encryption. (GLB III-C)
- Assess management's process for verifying the adequacy of its Internet service provider's (ISP) information security and transaction verification controls. (GLB III-D)

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

16. If the institution created a transactional website since the previous exam determine that they provided the notice to OTS as required by CEO memo No. 109. Contact the regional office to determine the need for follow-up to ensure compliance with the requirements set forth in the CEO memo.

Level II

Management Oversight

17. Assess the adequacy of IT resource acquisition and outsourcing policy and determine whether it covers cost / benefit analysis; vendor selection and due diligence; management approval (authority limits or guidelines); contract execution; and software licensing. (GLB III-D)

_____ _____

18. Assess the appropriate corporate policy (IT or other) covering insurance to determine whether IT insurance coverage is periodically reviewed and approved by senior management.

_____ _____

19. Determine whether management provides the board with report(s) that describe the overall status of the information security program and the institution's compliance with the GLB guidelines. (GLB III-F)

_____ _____

Information Integrity

20. Determine whether the design of the information security program complies with GLB guidelines as regards the scope and standards for safeguarding customer information. (GLB I and II)

_____ _____

21. Evaluate the customer and corporate information risk assessment process. Management should (GLB III-B):

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Maintain an inventory of all repositories of customer and corporate information. Management should take particular note of non-public customer information and mission-critical corporate information. Repositories include electronic and paper files.
- Identify threats to the integrity and confidentiality of the information.
- Assess the sufficiency of policies and procedures intended to control the risks. Management can accomplish assessments through self-inspection, or through independent audits.
- Monitor, evaluate, and adjust the risk assessment, taking into consideration any change in the IT environment or sensitivity of the information.

_____ _____

22. Assess the user-access assignment process. Determine whether institution managers have (GLB III-C):

- Identified the system's sensitive customer-record fields and powerful transactions.
- Assigned job responsibilities that provide for proper segregation of duties and dual control over sensitive fields and powerful transactions.
- Assigned user information retrieval and transaction processing capabilities according to defined job responsibilities.
- Appropriately limited the assignment of highest user access capabilities (for example, Security Administrator).
- Created and authorized the user access profiles for implementation by the information security officer.

_____ _____

23. Perform sampling tests to verify that user-access assignments are in conformance with management-designed user access profiles (or, in the absence of such profiles, that user access assignments are appropriate).

- Obtain printouts of access profiles of selected users from one of the institution's systems. Include a range of users.
- Ascertain if the system access profiles show inconsistencies with management-designed user access profiles or defined job responsibilities.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Identify the sensitive data and transaction processing capabilities of selected users and ascertain if their execution is protected by prudent controls.

_____ _____

24. If you find any user access assignments to be inappropriate, determine if the condition was caused by (a) control deficiencies in the granting of user access assignments or (b) deficiencies in the system's security controls (system rules or software).

_____ _____

25. Determine if management periodically reviews and updates user-access assignments. (GLB III-E)

_____ _____

26. Determine if appropriate controls are in place to monitor activities of employees in areas where proper segregation of duties is not feasible, and of other sensitive activities such as the file maintenance of customer records. (GLB III-C)

_____ _____

27. Determine if appropriate user access and monitoring policies and procedures are adequately documented.

_____ _____

28. Evaluate information security policies and standards in effect for (GLB III-C):

- User-ID controls.
- Passwords.
- System log-on and log-off.
- Virus-protection.
- Encryption of sensitive customer or corporate information whether used and stored within the institution or transmitted elsewhere.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Destruction or disposal of sensitive customer and corporate information to ensure that the information will not be unintentionally made available to unauthorized persons. Proper disposal could include shredding of paper media, deleting, or degaussing (erasing) of data in electronic media, etc.

_____ _____

29. Assess data-input quality controls. Determine whether controls are in place to verify the completeness and accuracy of sensitive input data that are not readily verifiable by the editing capabilities of the automated system.

_____ _____

30. Assess personnel access restrictions at locations containing customer or corporate information, such as buildings, computer facilities, work areas, and records storage facilities. (GLB III-C)

_____ _____

Business Continuity Risk

31. Assess the institution's disaster recovery plans and testing related to outsourced systems. Obtain and review the institution's service provider-related contingency plan to determine if it (GLB III-C):

- Identifies all the categories and sources of data input into the service provider's systems by the thrift.
- Describes the steps required to recover previously input data and prepare them for resubmission when requested by the service provider.
- Identifies the person or teams responsible for executing the recovery steps.
- Provides a management-approved time line for input resubmission.

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

32. Determine if the institution periodically reviews the plan to help ensure that it is current and effective. (GLB III-E)

_____ _____

33. Assess the institution's disaster recovery plans and testing related to internally operated systems. Obtain and review the plan for a selected mission critical system, and determine if the plan provides for (GLB III-C):

- The recovery of key resources, including the computer, operating system software, application system software and data.
- An alternate processing site/work area.
- Staff assignments, contact lists, and other recovery related provisions as indicated in OTS CEO Memo 72.
- A management-approved recovery time line for the completion of recovery.
- Storage of backup files at a safe location.
- Updated inventory of files maintained at backup sites.

_____ _____

34. Determine if the plan is reviewed periodically to help ensure that it is current and effective. (GLB III-E)

_____ _____

35. Determine if there is adequate protection against destruction of institution-maintained customer or corporate information against potential physical hazards such as fire and water damage (GLB III-C).

_____ _____

Vendor Management Risk

36. Evaluate the appropriateness of existing contracts. Determine if contracts adequately define performance measures related to vendor commitments and if contracts include recommended contract provisions such as those in TB 46 and CEO Memo 133. Also, determine if there are

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by the service providers.

37. Assess the institution's controls for monitoring vendor performance and ascertain whether (GLB III-D):

- The institution verifies periodic performance level reports supplied by the service provider.
- The unit that monitors vendor performance verifies and approves vendor charges for routine and special services.
- The institution adequately monitors delivery of nonproduction deliverables.
- Senior management is being promptly informed of significant deficiencies in vendor performance.

Internet Banking

Vendor-Related Controls (GLB D)

38. Review documentation of any due diligence review related to the adequacy of prospective ISPs' information security controls. If you identify significant weaknesses, ascertain their status of resolution. Potential areas of weakness are:

- Authentication controls
- Firewall controls
- Encryption controls
- Intrusion-detection controls
- Incidence-handling controls.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

39. Assess the effectiveness of controls for the ongoing verification of the adequacy of the ISP's information security program.

_____ _____

40. Assess management's process for verifying the adequacy of its ISP's business continuity plans. Determine whether management has obtained documented assurance from ISPs that customer transactions are adequately backed up to ensure that they are recoverable in the event of a disaster affecting the ISP.

_____ _____

41. Determine if management monitors the results of tests of the ISP's disaster recovery plans.

_____ _____

42. Assess the appropriateness of the terms and conditions of existing ISP contracts.

_____ _____

43. Assess management's process for monitoring ISP service-level performance.

_____ _____

Institution Controls (GLB III-C)

44. Determine if the institution established policies and procedures to deal with its contractual responsibilities related to outsourced services such as Internet banking, customer bill payment, etc. Procedures should be in place to deal with problem transactions for which the institution is responsible and related customer service activities.

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

45. Assess controls over the institution's web site systems administrators, if any. The number of administrators should be limited and management should review and approve their web site maintenance capabilities.

_____ _____

46. Determine if the institution's firewall control parameters (i.e., "filters") are described in a document that management reviewed and approved.

_____ _____

47. Determine if there are modems in PCs or workstations that would allow unauthorized Internet users (e.g., hackers) to circumvent the institution's firewall. If yes, assess existing controls or management's action plan, to mitigate the risk.

_____ _____

Conclusions

48. Summarize findings, obtain management responses, and update programs and the continuing examination file (CEF), if applicable, with any information that will facilitate future examinations. File exception sheets in the general file.

_____ _____

49. Ensure that your review meets the *Objectives* of this Handbook Section. State your findings and conclusions, appropriate recommendations for any necessary corrective measures, on appropriate work papers and report pages.

_____ _____

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____