Information Technology Risks and Controls

Summary: This Regulatory Bulletin transmits Examination Handbook Section 341, Information Technology Risks and Controls. The Office of Thrift Supervision substantially revised and reorganized this section of the Examination Handbook. This handbook section replaces existing guidance found in Thrift Activities Handbook Section 341, Technology Risk Controls. This bulletin rescinds RB 32-21 dated January 7, 2002.

For Further Information Contact: Your OTS Regional Office or Kathleen M. McNulty, Technology Program Manager, in the Information Technology Risk Management Division of the OTS, Washington, DC, at (202) 906-6322. You may access this bulletin at our website: **www.ots.treas.gov**.

Regulatory Bulletin 37-15

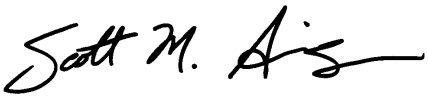
341 Information Technology Risks and Controls

The rapid growth and extensive deployment of information technology (IT) requires a thorough assessment of the risks inherent in such activities. The Examination Handbook section issued today outlines OTS expectations that savings associations fully address the risks and challenges posed by using technology, and establish effective risk management practices commensurate with the association's size and complexity. Use this Handbook section and its examination procedures in conjunction with other Handbook sections that provide guidance for reviewing an association's internal control environment.

The Section 341 guidance addresses responsibilities of the board and management for overseeing a strong control environment for IT. OTS believes this should include audit or other independent reviews on a frequency determined by an association's audit risk assessment, comprehensive association-wide business continuity planning, and proactive service provider management and oversight. The Handbook guidance also discusses responsibilities that the board of directors and management have to develop, implement, and maintain an effective written information security program tailored to the complexity of an association's operations.

Because we substantially revised Examination Handbook Section 341 we did not use change bars in the margins of the handbook section to indicate revisions. A revised program with new or updated examination procedures accompanies this new Handbook section. OTS examiners will conduct the procedures for this Handbook section as part of every comprehensive examination unless the association is scheduled to receive a separate IT examination.

In November 2005, we also revised PERK 005 to ensure information requests in the PERK 005 are consistent with the revised Examination Handbook Section 341 guidance and program.



—Scott M. Albinson

Examinations, Supervision, and Consumer Protection

Information Technology Risks and Controls

This Handbook Section presents the agency's examination guidance and program for assessing information technology (IT) risks in comprehensive examinations of savings associations that do not undergo a separate IT examination. OTS uses this section to evaluate technology risks in an association and assess the strength of an association's internal controls for information technology. The Handbook section focuses on the important control activities of proactive management oversight for information security, business continuity, and vendor management, as well as technology-related audit work.

Technology has revolutionized daily operations in savings associations. Associations have moved away from mainframe-oriented computer processing environments and toward increased reliance on newer technological environments, for example, networks, the Internet, and enterprise-wide processing. This examination guidance reflects these changes. Examiners assess the risks of the association's usage of technology, the overall resulting exposure to technology risks, and the adequacy of controls to mitigate those risks.

LINKS

Program

If the savings association does not properly identify and mitigate technology risks, there can be serious adverse consequences to its reputation. Examples of technology risks that can substantially damage an association's reputation include unauthorized access to corporate data and customer records, identity theft, inadequate business continuity planning, or fraud. These can also cause significant financial losses to an association. Use this Handbook Section to determine, on a risk-focused basis, whether an association's use of technology is consistent with a safe, sound, and secure operating environment. This Handbook guidance and program complements Section 340, Internal Controls.

Overview

Increasingly, associations are using technology to develop and deliver financial products and services, with the goals of improving customer service and reducing operating costs. Even the most traditional, conservative associations have embraced more technology. Associations have made, and continue to make, huge investments in technology to maintain and upgrade their infrastructure, to provide new electronic information-based services, to manage their risk positions and pricing, and to monitor transactions to detect and prevent money laundering and terrorist financing under the Bank Secrecy Act and the PATRIOT Act. At the same time, new electronic products, such as online banking, make it possible for small associations to take advantage of newer technologies at lower costs.

Improved processes, such as automated underwriting and credit scoring, have given borrowers the opportunity to obtain credit cards, mortgages, and small business loans from more financial services providers. Automated underwriting and credit scoring substantially reduce the time and costs involved in making sound credit decisions. These tools have also improved the ability of lenders to evaluate and price credit risk, which allows extensions of credit to a wider range of borrowers. Individuals can easily obtain their credit reports and credit scores and verify the information. They can contact the credit bureau if information in the report is incorrect, and thereby, improve their credit standing.

Information technology has made other significant contributions to associations' profitability. In mortgage lending, credit decisions are made in minutes rather than days and at a much lower cost than a decade ago. New technology has also enhanced competition, making it easier for local associations to offer new products and compete successfully with out-of-market associations. In addition, securitization, which is also highly dependent on advances in information technology, has broadened the pool of mortgage lenders and made the primary and secondary markets far more efficient.

Associations use software and computers in operations due to the volume and complexity of transactions processed each day; in fact, almost every aspect of operations within an association is able to use some technology. Savings associations use technology to develop budgets and business plans, underwrite loans, measure and model interest rate risk, track trust accounts, and monitor suspicious activities; in short, to manage almost every aspect of their operations. As technology evolves, and associations continue to increase their reliance on it, risks increase. The increased risks require effective controls to ensure the integrity, confidentiality, and availability of data.

Risks are inherent in using any technology, and threats to associations come from both internal and external sources. Hackers, disgruntled employees, and errors can adversely affect reliability. Unauthorized parties might access networked systems that are connected to an association's database, and obtain sensitive, nonpublic customer information. Association websites may be inappropriately altered. Electronic mail containing confidential, proprietary corporate information may be distributed in error.

> An association's board of directors and management should establish policies, procedures, and controls to ensure confidentiality, integrity and availability of information.

Clearly, this increased reliance on technology has significantly increased the risks of financial and reputation losses due to unauthorized access to customer and corporate financial records, interruption of services to customers, and fraud. Associations must make choices regarding how to manage and control these risks.

Associations must establish and maintain adequate control systems so management can identify, measure, monitor, and control IT risks that could adversely affect performance or pose safety and soundness concerns. Similar to basic internal controls, associations should design IT risk controls to prevent, to mitigate, and/or to detect and address errors and problems. This process should involve representation from all functional areas, for example, audit, finance, legal, lending, marketing, and IT. These areas should all be involved from the beginning of the process to assess collectively the effects on the association. However, ultimately the board of directors and management are responsible for

developing and implementing the processes, policies, and controls that ensure confidentiality, integrity, and availability for an association's data and systems:

- Confidentiality: Customer and corporate information is protected from unauthorized access or use.
- Integrity: Information is not altered without permission.
- Availability: Authorized users have prompt and continuous access.

The level of technical knowledge required by boards of directors and senior managers varies and is dependent on the size and nature of the association's operations and the degree of complexities within its technology environment. Nonetheless, at a minimum, 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.

EXAMINATION OVERSIGHT ACTIVITIES

In conducting risk-focused reviews of information technology in comprehensive examinations, examiners:

- Review the association's IT environment.
- Determine the association's significant technology risks.
- Evaluate management's technology oversight activities, including any technology audit work.
- Assess the strengths of the association's control activities.

You should always consider the level of IT risks and adequacy of the control environment when scoping for examinations and assigning the Management and, as appropriate, the composite CAMELS ratings.

Consistent with a risk-focused approach, you should use judgment in determining the depth of the technology review in comprehensive examinations. The examination work should be consistent with the characteristics, size, complexity, and business activities of the association. To determine the appropriate review, close coordination is needed between the Examiner-in-Charge (EIC), other members of the examination team, and examiners who review the IT risks and controls.

Examination Coverage

IT examiners review technology risks and controls at associations that have complex operations and activities. Safety and soundness examiners review IT risks and controls during comprehensive examinations, using this examination guidance and its related examination procedures. To supplement

the examination guidance in this Section, we encourage you to refer to the FFIEC IT Examination Handbook Booklets, if necessary.

Regional managers determine whether to assign an IT examiner to review an association's information technology. They consider the most recent information available regarding the association's technology environment and the strength of IT controls. As complexity within an association's technology environment increases, stabilizes, or decreases, examination responsibilities for some associations may move from IT examiners to non-IT examiners.

Factors suggesting an IT examiner may need to review this area include the following:

- Recent, pending, or proposed system conversions.
- Recent or pending mergers and acquisitions.
- Problems and concerns at previous examinations.
- Volume and type of internal processing conducted.
- Complex applications, systems, networks, or equipment.
- Volume of loan servicing.

While these factors suggest a need for an IT examiner, they are not determinative. In scoping, the EIC should consult with the Regional IT Examination Manager regarding IT concerns. Such consultation helps ensure proper evaluation and consistent regulatory treatment.

Significant internal control weaknesses warrant expanded investigation and analysis. In those situations, the examiner completing this program, the EIC, the Regional IT Examination Manager, and the regional Caseload Management team will determine what additional procedures are needed, who should perform them, and whether to conduct them at the current examination or at a future comprehensive or IT examination.

Information Technology and Management Ratings

The strength of the information technology control environment is one of the factors considered in assigning a rating to the Management component of CAMELS. As stated in Examination Handbook Section 070, the Management component rating must reflect the board's and management's ability and effectiveness in managing all aspects of an association's risks, including the findings and conclusions for IT risks and controls.

The Management rating should always reflect serious control deficiencies for technology risks. Generally, if you identify serious deficiencies with the technology controls, you should rate Management no higher than 2.

Ratings: IT Concerns

For examination types 10 and 16, the EIC completes the data field in the OTS Examination Data System (EDS) for the technology examination work. ***Note:*** This data field is encouraged for examination types 11 and 43, but is not required.

> The EIC should select Yes for IT Concerns whenever the exam findings disclose significant IT weaknesses.

This data field prompts the EIC to answer Yes or No to the question:

- Were significant IT concerns noted in the Report of Examination (ROE)?

The EIC should select Yes whenever the examination findings disclose significant IT weaknesses. A significant weakness is one that the EIC concludes is at least partially the cause for lowering the Management rating. A significant weakness could also be something that significantly impacts the association, and management lacks the will or ability to resolve it. If the IT program did not disclose any significant weaknesses, the EIC should answer No.

Examination Comments and Conclusions

You should incorporate IT examination comments and conclusions into the Management comments, either on the formal report page for Management, or in the Management-related comments summarized under overall Examination Conclusions and Comments. You should present findings under the caption or heading, Information Technology.

Examiners conducting this program assess an association's compliance with the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), 12 CFR Part 570 Appendix B, including Supplement A. The Security Guidelines implement Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act), and Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

The ROE comments should include a brief description of the association's IT environment, significant technology risks, and an overall conclusion as to the adequacy of controls. The report comments should also clearly state whether or not the association is in compliance with the requirements of the Security Guidelines. You must note material instances of noncompliance in the ROE.

You should present significant adverse findings in sufficient detail to identify the specific conditions that require corrective action. Whenever possible, these should include mutually agreeable deadlines for completion of corrective actions. Present corrective actions and deadlines in the Management page comments, or integrate them into the Management-related comments in the Examination Conclusions and Comments. Include significant findings, for example, violations of laws or regulations, on the Matters Requiring Board Attention page.

When examining a state-chartered association, you should also refer to state regulations and follow supplemental regional examination policies and procedures.

Information Technology Database

OTS developed and maintains the Information Technology Database (IT Database), a national system that provides agency management with information on the thrift industry's data processing activities and technology service providers. The Director, Information Technology Risk Management (ITRM), is the IT Database system owner. ITRM works with OTS Information Systems to maintain and enhance the system, oversee its operations, and update system standards, policies and procedures.

A staff person in ITRM serves as the IT Database National Administrator. In addition to the National Administrator, the regional IT Examination Managers have designated Regional IT Database Administrators. The Regional IT Database Administrators ensure that data collected from the associations, and reviewed by the safety and soundness examiners, are entered into the IT Database, as required.

The IT Database contains information on service providers used by associations, such as names, addresses, significant applications processed, and processing locations, domestic or foreign. The IT Database also collects information about significant applications processed internally by associations. Examiners and Caseload Managers use this information to produce reports that identify technology-related risks, which can be addressed in examinations, off-site monitoring, and other regulatory oversight activities.

The examiner completing the IT procedures collects and reviews the IT Database information for accuracy and completeness, and then provides the information to the regional office for input. The information in the IT Database must be updated every 18 months. If these examination procedures are not conducted within the 18-month timeframe, regional staff must obtain the IT Database information directly from the association.

Information Technology Environments in Associations

Background

Associations have a number of choices available to meet their IT needs. Many OTS-regulated associations outsource a significant amount of their information processing functions to one or more third-party service providers. Others maintain internal data centers to run software licensed from vendors or developed in-house. Mixes or hybrids of these basic approaches are common. An association might contract with one service provider for its general ledger and deposit systems, and with other service providers for loan servicing or its website. Associations also might use licensed software for investments and interest rate risk analysis, and spreadsheets developed in-house for asset quality and board reports.

In addition to outsourcing significant business operations to service providers, most associations are interconnected with various other entities, such as ATM networks and automated clearing houses (ACHs), to process daily business. Associations also maintain one or more internal networks, Local Area Networks, or Wide Area Networks. Each of these arrangements requires a different type and level

of management involvement with regard to data integrity, security measures, and business continuity plans.

OTS expects associations to develop and maintain strong control environments for the information technologies they use. A strong control environment enables management to identify, evaluate, and control risks associated with the business activities. In complex technology environments, it is critical that associations have effective risk management practices and strong internal controls to ensure that all of the technology risks are identified and appropriately addressed. Associations should have effective policies and procedures in place commensurate with the complexity of the IT environment. They also should identify the risks of using technology prior to deploying it, and ensure adequate controls are in place.

Components of Information Technology Environments

Personal Computers

The personal computer is the most prominent tool in an association's business environment. The power of personal computers has enabled information processing in associations to evolve from the traditional, centralized environment to a decentralized or distributed environment. In addition to its use as a word processor and terminal access device to other computers, a personal computer operates as a powerful standalone computer or within a network of computers. Most associations have at least one internal network, whether it uses third-party service providers, processes internally, or uses a combination of these arrangements.

Using personal computers, association staff can create applications to supplement those provided by third-party service providers or internally operated data centers. For example, staff can use personal computers to originate data, download and manipulate information from an association's databases, and upload the data back into the databases. Each of these activities creates information, which management uses to make decisions that affect business strategies, customer relationships, and regulatory reporting. Management should implement and maintain controls over these activities to ensure confidentiality, integrity, and availability of the information processed and produced.

Networks

A computer network is an arrangement in which multiple computers are connected to share information, applications, and equipment. By design, networks can increase efficiency, convenience, and access; however, the design also directly affects the specific risks that users must address and control.

Network access can be through a combination of devices such as personal computers, telephones, interactive television equipment, and card devices with imbedded computer chips. The connections are completed principally though telephone lines, cable systems, or wireless technology. It is important to note that not all networks are equally critical, vulnerable, or contain data that is equally sensitive. Every association must evaluate the risks it faces and address those risks.

The Internet is a public network that can be accessed by any computer equipped with a modem. While not centrally managed, the Internet is given order through the World Wide Web (Web), which facilitates visual interfaces and links or electronic connections to other information. The Web also provides multimedia capabilities such as text, graphics, audio, and video.

Intranets are private networks built on the infrastructure and standards of the Internet and the Web. Intranets allow access to databases and electronic documents by defined user groups that are generally limited to internal personnel.

Associations must review and address the security of internal networks, whether private, or configured as local or wide area networks. Internal attacks are potentially more damaging than attacks from outsiders because an association's personnel, who can include consultants as well as employees, have authorized access to critical computer resources. An internal attacker could exploit trusted relationships in networked systems to gain a level of access that allows the attacker to circumvent established security controls. After circumventing the security controls, the attacker could potentially access sensitive customer or corporate information.

Public networks pose additional risks over those of internal networks. Transmitting confidential data over public networks through the use of dedicated or leased lines may provide an inappropriate sense of security. These lines use the infrastructure of public networks; therefore, they are vulnerable to the same attacks as the public networks themselves. Confidential data transmitted via public networks may be intercepted or compromised by individuals for whom the data is not intended. It is therefore important to encrypt sensitive data transmitted via public network infrastructure.

Local and Wide Area Networks

A local area network (LAN) is a network that interconnects systems within a small geographic area, for example, a building or a floor within a building. Using personal computers or other terminals, users communicate via electronic mail, share printers, and access common systems, databases, and software. A wide area network (WAN) connects users in larger geographic areas. An association might have a LAN within its headquarters, and a WAN for its branches or lending offices to communicate with each other and the headquarters.

LANs and WANs provide substantial benefits in productivity and information access. They facilitate interaction among association staff and between the association and its service providers. Examples of services that associations can offer through their networks include telephone banking, banking by personal computer, ATMs, automatic bill payments, and automated clearinghouse systems for direct deposits or payments. Such access, however, requires that the association apply controls to the personal computers.

Associations that use LAN, WAN, or other network technologies should have policies and procedures that govern purchase and maintenance of hardware and software. Associations must also establish and maintain sound controls that limit access to data and applications based upon job responsibilities, and protect the data's confidentiality and integrity.

Firewalls

Firewalls are a combination of hardware and/or software placed between networks that regulate traffic that passes through them. They provide protection against unauthorized individuals gaining access to an association's network. Associations should consider firewalls for any system connected to an outside network.

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

Internet Activities

Association management should have policies, procedures, and controls to govern employee Internet activities. These should address the following:

- Minimizing viruses or other damaging program code associated with downloading files.
- Appropriate use of Internet facilities and services by employees.
- Using encryption to protect sensitive information in transit, for example, electronic mail messages.

Electronic Banking

Electronic banking is the delivery of information products and services between a customer and an association using electronic access devices such as telephones, automated teller machines, and personal computers. Typically, the devices are connected through a telecommunication line or the Internet.

Internet Banking

Internet banking refers to the systems that enable customers to access their accounts and information regarding the association's products and services from the association's website via a personal computer or similar communication device.

Transactional Websites

Transactional websites, as defined in CEO Memo 109, allow customers to do any of the following:

- Open an account.
- Access an account.
- Obtain an account balance.

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

CEO Memo 109, Transactional Web Sites, states that OTS-regulated associations planning to establish a transactional website must file a Notice with OTS at least 30 days in advance of opening the website to transact business with customers. The examiner conducting the IT examination procedures should determine that the association filed the required Notice with the appropriate regional office.

If the Notice was not timely and properly filed, the EIC should notify the regional caseload management team to determine appropriate remediation. If the Notice was filed pursuant to CEO Memo 109, the examiner reviewing IT risks and controls should contact the regional office to determine if there were any issues that require onsite follow-up review.

Transactional websites also pose specific consumer protection and privacy issues associations should address. See Handbook Section 1375, Privacy, for additional guidance.

Transactional websites that provide for electronic mail between the association and customers require additional controls, for example, encryption, to protect the confidentiality of customer accounts and other sensitive data. Associations should clearly caution customers about sending sensitive data, for example, account numbers, in electronic mail messages to the association or anyone else. For additional guidance see CEO Memo 228, Interagency Guidance on Authentication in an Internet Banking Environment.

Informational Websites

Informational websites provide general information about an association's products and services. Informational websites often highlight loan and deposit programs, branch locations, and operating hours. These may also provide electronic mail addresses for contacting the association and its employees.

Some informational websites provide links to other websites that provide community interest information or other related product information. Thrift Bulletin 83 provides guidance regarding these web-linking arrangements.

CONTROL ACTIVITIES FOR INFORMATION TECHNOLOGY RISKS MANAGEMENT OVERSIGHT

Responsibilities of the Board of Directors

Boards of directors have the ultimate responsibility for all technology deployed in their associations. They should approve their associations' overall business and technology strategies. The board of directors and management cannot delegate responsibility for technology controls to service providers, software vendors, or even internal staff. The board of directors must ensure that strong controls for technology risks exist throughout the association.

The level of knowledge required by boards of directors and management is dependent on the size and nature of an association's operations and the degree of complexity within its technology environment. Nevertheless, association directors and management should have a clear understanding of the risks posed by using specific technology, provide clear guidance on risk management practices, and take a proactive role in overseeing technology risk mitigation activities. An association's board of directors and management must effectively plan for using technology, establish a strong control environment, including audit or other independent review of the controls, and educate and support the association's technology users.

To manage effectively the risks associated with complex technology environments, some associations have established a senior management Information Technology committee. This committee is responsible for overseeing the relevant technology control functions throughout the association, for example, in the auditing, legal, and financial divisions, and ensuring these controls are integrated into a framework of risk management for information technology. This senior management committee regularly reviews new products and activities and provides final approval of transactions. Such senior management committees can serve as an important part of an effective information technology control infrastructure.

Strategic Planning for Information Technology

Deficiencies in planning for deploying technology significantly increase the risks posed to an association and its ability to respond effectively. Therefore, regardless of asset size, associations should have an appropriate plan for technology that outlines the framework for the uses of technology. The substance and form of such a plan will vary from association to association and be dependent on the complexity of the association's operations. The key elements are whether and how well the technology planning process meets the association's needs.

Associations should update their technology plans annually. A satisfactory technology plan coordinates the technology initiatives and activities to the overall business planning process. It should also address the technology strategy used, for example, a combination of internal and outsourced processing that supports delivery of the selected products and services.

Associations intending to implement a transactional website should address this in the technology plan. Management should consider the implications of a transactional website on the association's long-term goals and strategies, and obtain input from the affected business line and technology managers. Planning for a transactional website should address the required advance notice to OTS and include a thorough review of the risks posed by a transactional website to information security, business continuity, and vendor management.

Training Information Technology Users

Associations must properly educate and support employees and customers to achieve user acceptance of, and confidence in, the association's information systems and technology. Associations should provide training to employees and customers to use applications properly. Associations must also support users with prompt responses to problems. If an association fails to provide reasonable training and support for customers and staff, commitment to the system and its applications deteriorates, administrative costs increase, and avoidable errors may occur. Training deficiencies also raise the risk of data integrity problems and potential for complaints.

Associations should fully inform staff of any changes or updates to systems. Associations should also train staff on how to respond to and execute the business continuity plan. If the association chooses to outsource this function, it must carefully evaluate the third-party vendor's qualifications prior to signing any contracts. Management should also provide backup training for key job functions.

For additional guidance on Management control activities, see Examination Handbook Sections 310, Oversight by the Board of Directors, and 330, Management Assessment, and CEO Memo 201, FFIEC IT Examination Handbook, Management Booklet.

Audits and Other Independent Reviews

All associations should adopt and maintain an audit program. An effective audit function is essential to an association's safe and sound operations. It provides the framework for assessing the effectiveness of the association's risk management practices. It also facilitates reporting to the board of directors and management on the strengths and weaknesses within the association's internal controls. To ensure adequate audit coverage, associations may use internal audit work, external audit work, or a combination of both depending on the association's audit risk assessment. Effective audit coverage substantially improves an association's ability to detect potentially serious problems.

The audit work may be completed internally or externally, however, someone that is qualified and independent of the process or function reviewed must complete the work. This independent person can conduct the audit work separately, as an audit of a specific technology activity, or incorporate it into the audit work for a specific operating department or business line.

The complexity of financial products, services, and delivery channels makes the inclusion of risk-based IT audit coverage an important consideration in establishing an effective overall audit program. Effective audit coverage of technology risks requires personnel that have the skills and experience to identify and report on compliance with the association's policies and procedures. These skills and

experience should include strong abilities to understand technology risks, as well as a detailed understanding of the association's IT policies and procedures.

Audit procedures are most effective when designed into the technology or system during development. When combined with a strong risk management program, a comprehensive, ongoing audit program allows the association to protect its interests and those of customers. In developing an audit program for technology, an association should consider how each application protects fully the financial and informational assets, system reliability and availability, and user confidence.

See Thrift Bulletin 81, Interagency Policy Statement on the Internal Audit Function and Outsourcing, for additional guidance on OTS expectations for an internal audit program.

Technology Audit Plan

An association's audit plan should provide for reviewing its technology risks. It is the responsibility of the board of directors and management to determine how much auditing will effectively monitor the internal control system, taking into account the audit function's costs and benefits. For associations that are large or have complex operations, the benefits derived from a full-time manager of audit or an auditing staff will likely outweigh the costs. For small associations with few employees and less complex operations, these costs may outweigh the benefits. Nevertheless, even a small association without an internal auditor can ensure it maintains an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls.

Generally, a technology audit will:

- Review technology policies, standards, and procedures.
- Assess how technology affects association operations.
- Determine if technology activities are consistent with management policies and procedures.
- Substantiate the integrity of employee activities and appropriateness of user access rights.

Audit work for technology should validate that all the business lines are complying with the association's standards for technology usage, and appropriately identify any exceptions. This validation should include transaction testing that confirms policy compliance, existence of proper approvals, adequacy of documentation, and integrity of management reporting.

Technology audit work should have clear procedures for when and how to expand the scope of audit activities. There should also be procedures for reporting audit findings directly to the association's board of directors or audit committee, as well as management in the audited area. Associations should implement follow-up procedures to ensure that management resolved all audit findings satisfactorily and the business unit or department implemented audit recommendations in a timely manner.

The complexity of the association's technology environment may cause some associations to retain outside consultants, accountants, or lawyers to review this area. The retention of independent expertise may be an effective method to control effectively the overall risk. For example, associations may employ external auditors to test the technology environment and ensure compliance with policies and procedures. The resulting reports can provide valuable insight to the association in improving its risk controls and oversight.

Additional guidance regarding External and Internal Audit is found in Handbook Sections 350 and 355, and CEO Memo 182, FFIEC IT Examination Handbook, Audit Booklet.

Information Security Risks and Controls

An association's corporate data and customer information must be available, accurate, complete, valid, and secure. Information security is the process or methodology an association uses to protect its corporate and customer information. Strong and effective information security is essential to an association's safety and soundness, and should be commensurate with the complexity of its operations and IT environment. The most effective information security has strong board of directors and management support and controls implemented throughout the association's business operations.

Effective information security is not a judgment or conclusion about the condition of IT controls at a particular point in time. Rather, effective information security is an ongoing and evolving process. An association has effective information security when it successfully integrates its processes, people, and technology to mitigate risks to acceptable levels in accordance with its risk assessment. OTS expects an association's information security program will have an incident response component for responding to specific risks, for example, unauthorized access attempts. The information security program should also provide for regular testing as well as security training of employees and other users.

An effective information security program serves as the overall framework that identifies risks, develops and implements a security strategy, tests key controls, and monitors the risk environment. This framework stresses the important roles of senior management and boards of directors by emphasizing their responsibility to recognize security risks in their associations and effectively mitigate security risks by assigning appropriate roles and responsibilities to management and employees.

The scope of an association's information security program should address all technology activities, for example, personal computers, Internet-based banking, and processing by the association's service providers. Effective security does not rely on one solution; rather it requires several measures, which, taken together, serve to identify, monitor, control, and mitigate potential risks to that information. Associations should use several differing controls to manage and ensure information security. Among these commonly found in associations are controls for authentication, passwords, user identification (ID), user access, system log-on and log-off, virus protection, and encryption.

Information Security Controls

Authentication

Savings associations use authentication controls to verify and recognize the identity of parties to a transaction. Typically, such controls include computerized logs, digital signatures, edit checks, and separation of duties. Weak authentication controls can allow the accuracy and reliability of data to be compromised from unauthorized access and fraud, errors introduced into the systems, or corruption of data and information. Associations should use effective authentication controls to restrict access and preserve integrity of data.

Authentication procedures for access to sensitive data minimally require a password. Maintenance procedures should ensure that only the user has knowledge of the user's password. Associations should have procedures that allow only users to change their own passwords. Password controls should have all of the following:

- Length of at least six characters, preferably more.
- A mixture of alphabetic, numeric, or other characters.
- Expiration dates that require users to change passwords frequently.
- Restrictions on reuse of previous passwords.
- Automatic lockouts after a defined number of failed log-on attempts.
- Suppression over the display of user passwords in any form.
- Encryption of password files.

On October 12, 2005, OTS and the other federal financial regulators issued updated guidance on risks and risk management controls to authenticate identity of customers accessing an association's Internet-based financial services. This guidance, distributed in CEO Memo 228, Authentication in an Internet Banking Environment, addresses the increased risks to associations and their customers from the growth of Internet banking and other electronic financial services, and the increased incidents of identity theft and fraud. As this guidance relates, associations need effective authentication systems to comply with requirements for safeguarding customer information, prevent money laundering and terrorist financing, and reduce fraud and theft of sensitive customer information.

The level of authentication an association uses should be commensurate with the risks of the Internet-based products and services offered. Associations should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where an association's risk assessment indicates the use of single-factor authentication – only a log-on ID or password – is inadequate, the association should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate these risks. OTS considers single-factor authentication

inadequate as the only control mechanism for higher-risk transactions involving access to customer information or movement of funds to others.

OTS expects associations to achieve substantial compliance with the authentication guidance distributed in CEO Memo 228 by December 31, 2006.

User Access Rights and Controls

Associations should also establish controls to limit user access. For example, associations should limit access to the Security Administrator account to the smallest number of persons practical without adversely affecting operations. Security Administrators should not have access to customer records. In addition, the association may grant contractors and consultants access to an association's systems. The association should tightly control these access rights.

Access rights to a system enable transaction processing and information retrieval. For outsourced systems, service providers typically set up generic access profiles for common job categories, for example, teller profiles. Associations should not accept and use the vendor access profiles without reviewing them. This increases the risk of inappropriate user access and weakens the control environment for sensitive data. To ensure user access is appropriate, associations should:

- Assign job responsibilities to provide for segregation of duties and dual control.
- Assign user retrieval and information processing capability profiles, based on job responsibilities.
- Ensure separate access profiles for their different systems.

User identification controls should require:

- Management approval to issue a new user ID.
- A unique user ID for each user. Multiple users should not be assigned to one user ID unless there are mitigating controls.
- Restrictions on issuing multiple identifications unless there are mitigating controls.
- Effective procedures to delete, disable, or change access rights promptly for terminated or reassigned employees.

Inappropriate user access assignments could be caused by control deficiencies in granting these rights or by weaknesses in the system security controls. System security control weaknesses can result from software rules that permit inappropriate grouping of user access rights. Weaknesses also arise when software capabilities are not properly invoked. Not enabling the supervisory override capability over dormant accounts is an example of such a weakness.

Management should periodically conduct independent reviews of user access rights to ensure user access assignments are appropriate and properly controlled. Management should document the findings of these reviews and resolution of any recommendations. Regardless of the cause, you should comment in the ROE on inappropriate user access rights.

Other Information Security Controls

System log-on and log-off controls should limit the number of unsuccessful log-on attempts to a user account. Associations should consider a control that notifies users of unsuccessful attempts since the user's last log-on. Associations should also require that personal computers and system access terminals automatically log-off after a brief period of inactivity.

Associations should install virus protection software on all personal computers and servers to prevent corruption of data or systems. Virus protection controls should include both association policies and installed software. An association's policies should restrict employees from adding software to their personal computers. The policy should also provide for periodic review or audit of the employees' personal computers to ensure conformance with association policies. Anti-virus software should be updated regularly to protect against new viruses.

Acknowledgement controls, such as batch totaling, sequential numbering, and one-for-one checking against a control file, verify proper completion of electronic transactions. For example, if an electronic transmission is interrupted, the association should have controls in place to notify the sender of the incomplete transaction and prevent duplication during re-submission.

Encryption technology scrambles data and information so it cannot be read or understood without the proper codes for unscrambling. Confidential or sensitive data and information in transit should always be encrypted. This includes email containing confidential or sensitive information, as well as Internet banking transactions. As part of performing its risk assessment, association management should identify the strength of encryption needed for specific categories of information.

For additional guidance regarding information security, see CEO Memo 172, FFIEC IT Examination Handbook, Information Security Booklet. This booklet will be updated and reissued in 2006.

INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

12 CFR Part 570 Appendix B and Supplement A Security Guidelines and Association Responsibilities

The Interagency Guidelines Establishing Information Security Standards implement:

- Section 501(b) of the GLB Act, which requires the federal financial regulators, including OTS, to establish standards for administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity, and proper disposal of customer information.

- Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which requires the federal financial regulators to issue regulations directing associations to ensure the proper disposal of consumer information. See Examination Handbook Section 1300, Fair Credit Reporting Act, for guidance on the FACT Act.

For additional guidance on an association's compliance obligations for the Security Guidelines, see CEO Memo 231, Compliance Guide for the Interagency Guidelines Establishing Information Security Standards.

Differences Between Security Guidelines and Privacy Rule

The requirements of the Security Guidelines, 12 CFR Part 570 Appendix B and Supplement A, and the Privacy Rule, 12 CFR Part 573, both relate to confidentiality of customer information. However, they have different focuses:

- The Security Guidelines address safeguarding confidentiality and security of a customer's information and ensuring proper disposal. The focus of the Security Guidelines is preventing or responding to foreseeable threats against, or unauthorized access or use of, that information. Further, the Security Guidelines state that associations must contractually require their service providers that have access to customer information to protect that information.

- The Privacy Rule limits disclosure of nonpublic personal information. The Privacy Rule prohibits disclosure of a consumer's nonpublic personal information unless certain notice requirements are satisfied and the consumer does not elect to opt out of the disclosure. The Privacy Rule does not impose any obligations with respect to safeguarding information. The Privacy Rule only requires associations to provide privacy notices to customers and consumers that describe their policies and practices to protect the confidentiality and security of nonpublic personal information.

Role of Board of Directors

The Security Guidelines require the association's board of directors, or an appropriate committee of the board, to develop, implement, and maintain a written information security program. Initially, the board or a committee must approve the written information security program. Thereafter, the board, or an appropriate committee, must oversee implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing reports prepared by management. Management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and the association's compliance with the Security Guidelines.

> An association's board of directors is responsible for developing, implementing, and maintaining a written information security program.

Information Security Program

Under the Security Guidelines, each association must develop and maintain an effective written information security program tailored to the complexity of its operations. Associations must identify and evaluate risks to its customers' information, including the risk of improper disposal of customer and consumer information. An association must also develop plans to mitigate these risks and implement appropriate controls, including proactive oversight and monitoring of its service providers that have access to the association's customer information.

Additionally, the Security Guidelines require that associations test, monitor, and update the information security program, as needed. Management should report the status of the information security program to the board of directors at least annually. The reports should discuss material issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

Objectives

As detailed in the Security Guidelines, the objectives of a written information security program are:

- Security and confidentiality of customer information.
- Protection against anticipated threats or hazards to the security or integrity of customer information.
- Protection against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.
- Proper disposal of customer and consumer information.

Risk Assessment

A written information security program begins with conducting an assessment of the reasonably foreseeable risks. Like the other elements of its information security program, the association's risk assessment should be documented. The Security Guidelines recommend the following steps in conducting a satisfactory risk assessment:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

- Assessing the likelihood and potential damage of the identified threats, taking into consideration the sensitivity of customer information.

- Evaluating the sufficiency of the policies, procedures, customer information systems, and other arrangements an association has in place to control risks identified.

- Applying the preceding three steps in connection with disposal of customer information.

For additional guidance regarding conducting an information security risk assessment, see the FFIEC IT Examination Handbook, Information Security Booklet.

Managing and Controlling Risk

Managing and controlling information security risk is an ongoing process. An association should review its policies and procedures on an ongoing basis to ensure they are adequate to safeguard customer information and customer information systems, and to ensure proper disposal of customer and consumer information. The association should include the review and findings in reports on the written information security program. The association should also update its risk assessment for new products and services and before implementing system changes.

The Security Guidelines provide a list of control measures associations must consider and adopt, as appropriate. For example, an association must consider controls to restrict access to sensitive or nonpublic customer information. These controls should restrict access only to individuals who have a need to know such information. Associations must also consider whether encryption of customer information maintained in electronic form is warranted in light of its information risk assessment. If so, the association should adopt appropriate encryption measures to protect information in transit, storage, or both.

Associations should train staff to implement and maintain the written information security program. Associations should provide specialized training to ensure personnel protect customer information in accordance with requirements of the information security program. For example, they should train staff to recognize and respond to attempted fraud and identify theft, guard against pretext calling, and dispose properly of customer and consumer information.

Associations also should test key controls, systems, and procedures of the information security program. The association's risk assessment should determine the scope, sequence, and frequency of testing. OTS expects testing to be done periodically at a frequency that takes into account the rapid evolution of threats to information security. Independent third parties or staff other than those who develop and maintain the information security program should perform and review the testing.

An association should adjust its written information security program to reflect the results of the ongoing risk assessment and key controls. An association should adjust the program to take into account changes in technology; the sensitivity of customer information maintained; internal or external threats to information; and its own changing business arrangements, such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

Security Guidelines and Service Providers

The Security Guidelines have specific requirements that apply to service providers. In addition to exercising due diligence in selecting a service provider, an association must enter into and enforce a contract that requires the service provider to implement appropriate measures designed to meet the objectives of the Security Guidelines. The contract guidance in the Security Guidelines applies to all service providers, affiliated and nonaffiliated.

Consistent with OTS and interagency outsourcing guidance, the Security Guidelines also require an association to monitor its service providers to confirm they satisfy all contractual obligations to the association. Among other things, these obligations include protecting against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer, and proper disposal of customer and consumer information.

The Security Guidelines do not impose specific requirements regarding methods used or frequency of monitoring service providers to ensure they are fulfilling their obligations under contracts. An association must monitor each service provider in accordance with its risk assessment for potential risks posed by the service provider. These activities could include reviewing audits or summaries of test results conducted by a qualified party independent of management and personnel responsible for development and maintenance of the service provider's security program. An association should document its reviews of service providers in the written information security program.

Security Guidelines and Disposal Rule

The Security Guidelines direct associations to require in contracts that their service providers implement appropriate measures designed to meet the obligations of the guidelines regarding the proper disposal of consumer information. Although the Security Guidelines do not prescribe a specific method of disposal, OTS expects associations to have appropriate risk-based disposal procedures for records. As indicated in their risk assessments, associations should ensure that paper records containing customer or consumer information are rendered unreadable. Associations should also recognize that computer-based records present unique disposal problems.

The Security Guidelines required associations to satisfy the disposal guidelines by July 1, 2005, and to modify affected contracts with service providers by July 1, 2006.

Supplement A to 12 CFR Part 570 Appendix B

Incident Response Program

On March 29, 2005, OTS and the other federal financial regulators issued guidance regarding programs to respond to unauthorized access to customer information and when to provide customer notice (Incident Response Guidance). According to this guidance, an association should develop and implement a response program to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The components of an effective response program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused.
- Prompt notification to OTS once an association becomes aware of an incident involving unauthorized access to or use of sensitive customer information.
- Notification to appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate action.
- Filing a timely Suspicious Activity Report, consistent with OTS regulations and instructions.
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence.
- Notification to customers, when warranted.

Customer Notification

The Incident Response Guidance describes when and how associations should provide notice to customers affected by unauthorized access or misuse of their information. In particular, once an association becomes aware of an incident of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine the likelihood the information has been or will be misused. If it determines that misuse of customer information has occurred, or is reasonably possible, the association should notify the affected customer as soon as possible.

Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a PIN or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow an

unauthorized third party to log onto or access the customer's account electronically, such as user name and password or password and account number.

The Incident Response Guidance also states that an association's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to customer information, including notification to the association as soon as possible following any incident. For additional guidance on response programs for security breaches and notifying affected customers, see CEO Memo 214, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

If OTS finds an association's performance is deficient under the Security Guidelines, it may take appropriate corrective action. The agency could require the association to file a compliance plan in accordance with the regulations implementing the Prompt Corrective Action provisions of the Federal Deposit Insurance Act. Or, OTS could initiate an enforcement action under 12 CFR § 568.5 for noncompliance with the Security Guidelines.

Business Continuity Risks and Controls

Board of Directors and Management Responsibilities

The board of directors is responsible for developing and annually reviewing test results and approving the association's Business Continuity Plan.

Associations must be capable of restoring critical information systems, operations, and services quickly after an adverse event. Effective business continuity planning can ensure associations are prepared to respond to events such as natural disasters, human error, terrorist activities, or a pandemic. For additional guidance on preparations for a pandemic, see CEO Memo 237, Interagency Advisory on Influenza Pandemic Preparedness.

An association's board of directors and management are responsible for all of the following:

- Establishing policies and procedures, and assigning responsibilities to ensure that comprehensive business continuity planning, including testing, takes place.
- Annually reviewing the adequacy of the association's business continuity plan and test results.
- Documenting such reviews and approval in the board minutes.
- Evaluating adequacy of contingency planning and testing by service providers.
- Ensuring that the association's business continuity plan is compatible with that of its service providers.

Business continuity plans can minimize disruptions caused by problems that impair or even destroy the association's processing and delivery systems. Extended disruptions to the association's business operations pose substantial risks of financial losses, and could lead to the failure of an association. Effective business continuity planning requires a comprehensive, association-wide approach, not a narrow focus on recovery of the association's systems and technology.

Business Continuity Planning Process

Business continuity planning is the process of reviewing all of an association's departments and business lines and assessing the importance of each to the association and its customers. Association management then develops and maintains a written business continuity plan that addresses all significant products and services, and the outsourced and internally operated information systems and technology that support these.

The complexity of an association's IT environment should dictate the level of detail contained in the business continuity plan. As the association adds new information systems and technology to its environment, it should revise the business continuity plan. The beginning point should be a business impact analysis. This assesses the risks posed to each system, and then identifies the principal departments, resources, activities, and users potentially affected by a problem. This includes assessing the response capability of the association, the alternate processing site, transportation and storage of backup media, and third-party vendors who can provide alternate processing locations.

If the association has contracted with a third-party vendor, management must obtain, review and determine adequacy of the service provider's business continuity plan and testing. The vendor's plan should be compatible with, and integrated into, the association's business continuity plan. However, merely maintaining the vendor's business continuity plan, and participating in its periodic connectivity testing, is not adequate to satisfy this requirement. An association must have its own business recovery and continuity plan specifically designed for its operating profile and IT environment.

Business Continuity Plan Development

A business continuity plan should define the roles and responsibilities for recovery team members. The detail will vary among associations, depending on the degree of risk inherent in operations, the level and complexity of information technology used, and the association's available resources. However, the business continuity plan should be in sufficient detail so an association can respond effectively to a problem situation.

Typically, an association's business continuity plan should:

- Designate the individual(s) responsible for coordinating all activities in responding to a disaster when the business continuity plan is invoked.

- Define roles and responsibilities for each team member.

- State clearly how potential disasters could affect the association's departments, products, services, employees, and customers.

- Provide details on potential risks and describe strategies, resources, and procedures for recovery.

- Establish the periodic frequency for testing and ongoing training of employees.

- Specify a clear timeline for recovering significant operations.

A clear timeline for recovery is critical to the business continuity plan. Recovery does not mean when an affected system becomes available again. In achieving full recovery, the association may have to correct or resubmit transactions that were in process when the disaster or disruption occurred. This could involve a full day's transactions or more.

Additionally, an association's business continuity plan should address the differing requirements posed by outsourced and internally operated systems. For outsourced systems, the association's business continuity plan should address the following for each significant service provider:

- Categories and sources of data input, for example, branch transactions entered by personal computers or terminals.

- Work steps or processes to recover for resubmission data previously input.

For each internally operated system, the association's business continuity plan should address:

- Recovery of lost data, for example, day-of-disaster online input.

- Replacement of damaged hardware and software resources.

- Alternate processing locations.

Business Continuity Plan Monitoring and Testing

An association should test its business continuity plan at least annually. Acceptable testing methodologies include tabletop drills, walk-through exercises, and simulations. An association should modify its business continuity plan to reflect testing results and any changes to the association's information systems and technology environment.

The association's business continuity plan should also designate an incident response team. Generally this team would consist of a small number of staff from the departments and functions designated as critical to recovery of operations. Collectively, the team provides the resources necessary to respond quickly and decisively to problems.

For additional guidance on business continuity planning, see CEO Memo 176, FFIEC IT Examination Handbook, Business Continuity Planning Booklet.

Vendor Management Risks and Controls

An association's board of directors and management should develop and approve policies for overseeing its service providers.

Associations use outsourcing to reduce costs and achieve strategic goals more efficiently. More and more, associations use third parties to conduct business operations associations previously conducted directly. Given current technology environments, these outsourcing arrangements are becoming increasingly complex, and may involve foreign-based entities. **Note:** Outsourcing is use of a third party, either affiliated or nonaffiliated, to perform activities on a continuing basis, that the association would normally handle.

Outsourcing can be the initial transfer of an activity or function from the association to a third party, or from the original third party to another third-party service provider, which is sometimes referred to as subcontracting. Another major trend in outsourcing is offshore outsourcing or moving processing activities outside the United States.

Offshore outsourcing introduces country risk for associations. In offshore outsourcing, associations must also monitor foreign government policies, and political, social, economic, and legal conditions in the country where it has a contractual relation with the service provider. Because of this, an association should develop appropriate contingency plans and an exit strategy for foreign outsourcing relationships. The association should have a strategy to transfer the processing activities back to the United States should it become necessary.

Examples of commonly outsourced operations include accounting, human resources administration, and customer call centers. Associations may also determine that use of a specific technology is too sophisticated or dynamic to be supported effectively within the association. These associations may determine that some or all of such technology should be outsourced to a third-party vendor.

As stated in Thrift Bulletin 82a, Third Party Arrangements, the Home Owners' Loan Act (HOLA) requires associations to notify OTS of arrangements with all third-party providers. HOLA requires such notice regardless of whether or not there is a contract. Generally, associations must provide notice to a Regional Director, for both domestic and foreign third-party arrangements, within 30 days after the earlier of:

- The date the association enters into the contract with the third party.
- The date the third party initiates performing the services.

Service Provider Due Diligence

The association must also conduct adequate due diligence in selecting its service providers. Prior to the formal selection, it should develop specific criteria to assess a third-party service provider's capacity and ability to perform the outsourced activities effectively. Appropriate due diligence includes selecting those service providers that are qualified and have adequate resources to perform the work. It also involves ensuring the service provider understands and can meet the association's requirements. It is also important that an association verifies the service provider's financial soundness to fulfill its obligations.

Prior to outsourcing any aspect of its operations, the association should establish specific policies and procedures. Management should demonstrate a comprehensive understanding of outsourcing's expected benefits and costs. Management also should develop and implement a formal program to monitor the service provider relationship. A comprehensive vendor management oversight program should provide for ongoing monitoring and controlling of all relevant aspects of the service provider relationship.

If a service provider fails, or is otherwise unable to perform the outsourced activities, it may be costly and problematic to find alternative solutions. The association should consider transition costs and potential business disruptions. An association should not outsource activities to a service provider that does not meet all of an association's due diligence criteria.

Service Provider Contracts

A clearly written contract should govern all outsourcing arrangements. Associations can mitigate outsourcing risks by carefully negotiating and reviewing service provider contracts, including contract renewals, prior to signing. Legal counsel should always review the vendor contracts to determine that the association's interests are adequately protected. Associations should actively monitor vendor performance, and verify performance level reports periodically.

Key contract provisions should:

- Define clearly outsourced activities and expected service and performance levels.
- Provide for continuous monitoring and assessment of the service provider so the association can take timely corrective action.
- Include a termination clause and time period or conditions under which it would be exercised.
- Address issues related to subcontracting for all or part of the outsourced activity.
- Cover requirements detailed in the Security Guidelines that are contained in the association's written information security program.

Service Provider Management and Monitoring

Typically, the association forwards data to the service provider's processing center, usually via on-line data entry terminals; output reports are available at the association's on-line terminals and printers. For those portions of the service provider's systems that are within the association, the association has responsibility for establishing and maintaining appropriate controls. For example, an association should develop controls that restrict access to teller terminals to tellers and other specifically authorized personnel. An association should also develop controls for balancing and reconciling items processed by the third-party vendor. The contract should address these responsibilities.

An association that is part of a holding company structure may have an affiliated company provide its technology needs. The affiliated service provider could be a department within the parent holding company, or a separate affiliate of the association. This type of arrangement typically reduces costs and achieves enterprise-wide economies of scale. However, contracts among affiliated entities may raise supervisory concerns. See the Holding Company Handbook for additional guidance on transactions with affiliates.

Vendor contracts should specify performance measures; two key metrics are online up time and terminal response time. Up time refers to the hours and days online services will be available. Often, these are the hours the association's branches operate, plus two or three additional hours daily. Contracts should state the vendor's performance commitment, for example, 99 percent up time. Terminal response time refers to the customary elapsed time between transaction initiation, when the enter key is pressed, and delivery of information to the screen. Response time should be measured in seconds.

Service provider contracts should also address non-production or non-processing products and services. Examples of these are audited financial statements for the vendor, third-party audits of the service provider, or summaries of the vendor's disaster recovery testing results. An association should obtain and review these as part of a proactive vendor management program.

An association should obtain IT ROEs for its significant service providers. An association should also obtain third-party reviews of its significant service providers. A third-party review is an independent evaluation the service provider obtains to meet the needs of client associations. A qualified auditor who is independent of the service provider conducts the third-party review. The scope of this audit should be broad enough to satisfy the audit objectives of the service provider and the client associations.

The American Institute of Certified Public Accountants' Statement of Auditing Standards 70 (SAS 70) provides guidance for auditors performing the service provider review and to auditors of client financial associations. The SAS 70 reviews should determine the adequacy of controls in areas such as the service provider's data center, systems and programming, and input/output controls. The controls reviewed at the service providers should have reciprocal controls at the individual client associations. In the SAS 70 review, the auditor will address these corresponding controls, in a section typically referred to as "client control considerations." An association should obtain and review these reports, and take appropriate actions for any client control considerations or weaknesses discussed. It is also important that an

association understand the scope of the SAS 70 review to determine if it adequately assesses all relevant control areas.

For additional guidance on vendor management oversight activities, see Thrift Bulletin 82a, Third Party Arrangements, and CEO Memo 201, FFIEC IT Examination Handbook Outsourcing Technology Services Booklet.

Other Association Controls for Information Technology Risks

Input and Output Controls

An association should require additional controls for technology used to process information, which has direct monetary effects on either the association or its customers. These controls should include requirements that there be segregation of duties between input of information and review of that information post-processing. Such controls should also require the post-processing reviewer to reconcile the processed information.

For large dollar transactions, for example, funds transfers, associations should require that all phases of the transaction be performed under dual controls. For mortgage loan set-ups, verification procedures should consist of manually comparing a sample of source documents against system reports. The association's written policies and procedures should describe these controls in full detail.

Change Control Management

An association must prepare to adapt activities and information technology to meet changing requirements and circumstances. Association management should ensure that changes to existing technology undergo the same due diligence as new technology selections. An important consideration in technology changes is that there be thorough testing. Additionally, an association should maintain accurate and complete records describing the changes, reasons for the changes, and those responsible for making them.

Conversion Project Management

Any association that uses IT to perform operations or provide services must commit to update continuously its activities to keep current with technological changes. For example, if an association experiences a corporate merger or acquisition, wants to reduce or more effectively control costs, or offer new products or services, it must plan to convert its operations and systems to accommodate these changes.

In highly technological environments, it is likely that an association will experience at least one or more systems conversion. A systems conversion is the process of replacing existing applications with new ones developed internally, or with third-party vendor software through an outsourcing agreement. The association should conduct planning, testing, and monitoring of new activities as part of its risk mitigation processes.

A conversion presents significant risks to an association, which can be mitigated with adequate project management controls. Flawed or failed conversions are very costly, and can compromise the integrity and reliability of books and records, causing unsafe and unsound conditions within the association. For example, in a flawed check processing conversion, an association could be forced to charge-off significant, unresolved bookkeeping differences. In a flawed deposit conversion, management could have unreconciled deposits requiring adjustments and write-offs. These can cause significant financial losses and waste management resources.

The board of directors should monitor planning and implementation of major system conversions. The directors should also hold management accountable for the success or failure of these conversions. Management should develop and oversee the successful completion of tasks and milestones by both the vendor and association personnel. User testing, debugging, and staff and customer training should occur before implementation or conversion of any system.

Regulatory Guidance and References

Code of Federal Regulations (12 CFR)

§ 555	Electronic Operations
§ 563.161	Management and Financial Policies
§ 563.170	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 568	Security Procedures
Part 570	Safety and Soundness Guidelines and Compliance Procedures
Appendix A Part 570	Interagency Guidelines Establishing Standards for Safety and Soundness
Appendix B Part 570	Interagency Guidelines Establishing Standards for Information Security
Supplement A Appendix B Part 570	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

Office of Thrift Supervision Guidance

CEO Memoranda

No. 109	Transactional Web Sites

No. 139	Identity Theft and Pretext Calling
No. 172	Information Technology Examination Handbook – Information Security Booklet
No. 176	Information Technology Examination Handbook – Supervision of Technology Service Providers and Business Continuity Planning Booklet
No. 179	Request for Comment on Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
No. 182	FFIEC Information Technology Examination Handbook – Audit Booklet, FedLine Booklet, Electronic Banking Booklet
No. 193	'Phishing' and E-mail scams
No. 196	Information Technology Examination Handbook – Retail Payment Systems Booklet
No. 199	Information Technology Examination Handbook – Development and Acquisition Booklet
No. 201	Information Technology Examination Handbook – Management Booklet and Outsourcing Technology Services Booklet
No. 204	Information Technology Examination Handbook – Operations Booklet and Wholesale Payment Systems Booklet
No. 205	'Phishing' Customer Brochure
No. 207	Interagency Guidance – Risk Management of Free and Open Source Software
No. 214	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
No. 228	Interagency Guidance on Authentication in an Internet Banking Environment
No. 231	Compliance Guide for Interagency Guidelines Establishing Information Security Standards
No. 237	Interagency Advisory on Influenza Pandemic Preparedness

Thrift Bulletins

TB 81	Interagency Policy Statement on the Internal Audit Function and Its Outsourcing
TB 82a	Third Party Arrangements

TB 83 Interagency Guidance on Weblinking: Identifying Risks and Risk Techniques

Handbook Sections

Section 340 Internal Controls

Section 1300 Fair Credit Reporting Act

Section 1370 Electronic Banking

Section 1375 Privacy

Information Technology Risks and Controls Program

Examination Objectives

To determine whether management effectively identifies and mitigates the association's information technology (IT) risks.

To determine whether the board of directors adopted adequate policies, procedures, and operating strategies appropriate for the size and complexity of the association's IT environment.

To determine that the association has a written information security program to comply with the requirements of the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), which implement Sections 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act) and 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

To initiate corrective action when policies, procedures, or controls are deficient or when you note violations of laws or regulations.

Examination Procedures

WKP. REF.

Level I

Level I procedures assess the association's processes for identifying and managing IT risks. Level I procedures are sufficient when an association has an effective internal control environment for IT risks, and there are no findings, which would cause you to expand your scope.

1. Review the association's response to the PERK 005, previous examination reports, including IT Reports of Examination, internal and external audit reports, and supervisory correspondence. After verifying completeness and accuracy of the IT database information, provide this information to your regional office for processing and input.

2. Determine that the association implemented effective corrective actions for all previously cited IT exceptions, criticisms, or violations. This includes any matters cited in IT Reports of Examination.

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

WKP. REF.

3. Determine the complexity of the association's information technology environment. Identify the association's significant systems. Significant means those critical to ensure information security, satisfactory customer service, and continuity of operations. Review the association's networks. Determine what significant applications are processed on the networks.

4. In conjunction with the Examiner-in-Charge (EIC) or examiner(s) performing the other Management programs, review board of directors' minutes of regular, special, and committee meetings for discussion and approval of significant IT matters. Examples of significant IT matters would include the association's written information security program, new or ongoing service provider relationships, and the association's business continuity plan.

5. In conjunction with the examiner(s) performing the reviews of Management and Earnings, determine the effectiveness of the board of directors and senior management in implementing strategic planning for IT. Evaluate plans for any significant changes. Review the association's strategic or business plan for IT-related activities.

6. Review the association's policies and procedures for IT. Determine whether these are effective for monitoring and controlling the association's IT risks considering the complexity of its IT environment.

7. In conjunction with the examiner(s) performing the review of the audit function, assess the adequacy of the association's audit coverage for IT risks. Verify that audit policies, practices, and programs for IT audits or other independent reviews are adequate for the size and complexity of the association's IT environment.

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

WKP. REF.

8. Review IT audits or other independent reviews completed since the preceding examination. Determine that IT audit work products are adequate for the size and complexity of the association's IT environment.

9. Assess management's responsiveness to IT audit concerns. Review the timeliness and adequacy of corrective actions. Confirm that the board of directors is informed of significant audit concerns, and that the board ensures completion of corrective actions.

10. Determine that IT audit expertise and training are sufficient for the complexity of the IT risks of the association.

11. Determine the association's compliance with the objectives of the interagency Security Guidelines implementing Sections 501(b) of the GLB Act and 216 of the FACT Act. The Security Guidelines require associations to have a comprehensive, written information security program that includes the administrative, technical, and physical safeguards to achieve the following objectives:

    - Ensure the security and confidentiality of customer information.
    - Protect against any anticipated threats or hazards to the security or integrity of customer information.
    - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
    - Ensure proper disposal of customer and consumer information.

    To meet the objectives and comply with the Security Guidelines, an association must:

    - Implement a written information security program that the board of directors approved.

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

WKP. REF.

- Conduct and prepare a written information security risk assessment.
- Require in contracts that service providers implement appropriate information security programs designed to meet the objectives of the Security Guidelines.
- Monitor, evaluate, and adjust the information security program for changes in the association's IT environment.
- Report to the board of directors annually regarding the association's compliance with the Security Guidelines and the status of the written information security program.

12. Review measures the association has implemented in its written information security program to manage and control risks. Determine that the association considered and adopted, as appropriate:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals.
- Controls and procedures to prevent employees from providing customer information to unauthorized individuals through pretext calling or other fraudulent methods.
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.
- Encryption of electronic customer information, including while in transit or in storage, or on networks or systems, to ensure unauthorized individuals do not gain access.
- Procedures designed to ensure that modifications to customer information systems are consistent with the association's written information security program.
- Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of misuse of customer information.
- Monitoring systems and procedures to detect actual and attempted attacks or other intrusions into customer information systems.

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

WKP. REF.

- Response programs that specify actions to take when the association suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies .
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

13. Confirm that the association has ongoing training for employees that implement and maintain the information security program. Review guidance to association employees for protecting customer and corporate information. Such guidance should describe the employee's responsibilities and consequences of improper actions.

14. Determine that the association has an incident response program consistent with the guidance in CEO Memo 214. Evaluate the effectiveness of the association's program for responding to incidents of unauthorized access to sensitive customer information and providing notification, as required. Confirm that the association's response program contains measures to:

- Assess the nature and scope of the incident.
- Notify OTS, either directly or through the association's service providers.
- Notify law enforcement agencies.
- File Suspicious Activity Reports when required.
- Controlthe incidents of unauthorized access.
- Notify customers, when necessary.

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

WKP. REF.

15. If the association had incidents of unauthorized access to sensitive customer information, determine that it:

- Conducted a prompt investigation to determine the likelihood the information accessed has been or will be misused.
- Notified customers when the investigation determined misuse of sensitive customer information has occurred or is reasonably probable.
- Delivered notification to customers, when warranted, by means the customer can reasonably be expected to receive, for example, by telephone, mail, or electronic mail.

16. Review the association's customer notice and determine it contains:

- A description of the incident, including type of information subject to unauthorized access.
- Measures taken by the association to protect customers from further unauthorized access.
- Telephone numbers customers can call for information and assistance.
- Reminders to customers to review account statements over a reasonable period – 12-to-24 months – and to report immediately suspicious activity and suspected identity theft incidents.
- A description of a fraud alert and how to place one in a customer's report.
- Recommendations to obtain credit reports from each nationwide credit-reporting agency and have information related to fraudulent transactions deleted.
- An explanation of how customers can obtain free credit reports.
- Information concerning availability of online guidance by the Federal Trade Commission regarding steps the consumer can take to protect against identity theft.

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

WKP. REF.

17. Evaluate the effectiveness of the association's measures to authenticate customers accessing Internet-based services and other electronic banking activities. Ensure that the association's authentication methods and controls specifically address the need for risk-based assessments, customer awareness, and security measures consistent with the guidance in CEO Memo 228. An association should:

    - Ensure its information security program identifies and assesses risks associated with Internet-based products and services, identifies risk mitigation actions, and evaluates customer awareness efforts.
    - Adjust its information security program for changes in IT, sensitivity of customer information, and internal or external threats to information.
    - Implement appropriate risk mitigation strategies.

18. Review password controls used on the association's operating systems and significant applications. Confirm these address password length, change intervals, composition, history, and reuse or lockout. Assess the effectiveness of these controls.

19. Assess the association's user access assignment policies and procedures for its information systems. Determine that these policies and procedures:

    - Provide for proper segregation of duties and dual controls.
    - Assign processing capabilities according to job responsibilities.
    - Limit system administrator capabilities appropriately.
    - Create user access profiles or user access assignments that are differentiated according to job duties.
    - Ensure that the association periodically reviews and updates user access assignments for job changes and terminations.

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

WKP. REF.

20. Review user access profiles or user access assignments for at least one of the association's significant systems, for example, lending, deposits, general ledger, or funds transfers. Determine that system access rights are consistent with the association's policies and procedures for assigning system access.

21. Confirm that the association has current written procedures to ensure security over its funds transfer activities, and that personnel are adequately trained to follow these procedures.

22. Confirm that each authorized user involved in the association's funds transfer activities maintains a unique password known only to the user. Verify that system users change passwords frequently.

23. Review the association's business continuity plan. Verify that the business continuity plan is based on a business impact analysis and that it identifies recovery priorities. Confirm that the association tested the business continuity plan within the past twelve months and that the board of directors annually approves testing results and the business continuity plan.

24. Review the association's back-up procedures. Determine what data are backed up, the rotation schedule, where the back-up media are stored, and how soon the back-up media are taken offsite.

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

WKP. REF.

25. Ensure that the association excercises appropriate due diligence in selecting, managing, and monitoring its service providers. Determine the association has established adequate policies and procedures to manage its service provider or vendor relationships.

26. Determine that the association's contracts with its service providers have clauses that require the vendors to implement measures designed to meet the objectives of the Security Guidelines. Review the association's policies, procedures, and practices used to confirm that its service providers satisfied obligations under the contract regarding customer information.

27. Determine that the association's board of directors, or an appropriate committee, approves new service provider relationships, or significant changes to existing oursourcing arrangements. These changes should be supported by a written risk analysis consistent with the association's business plan and the proposed or planned activity.

28. Determine that association management and the board of directors periodically review significant service provider contracts and service level agreements.

29. If the association created a transactional website since the previous exam determine that it provided the notice to OTS as required by CEO Memo 109. If the Notice was not timely and satisfactorily filed, contact the regional office to discuss appropriate remediation actions. Discuss with the regional office the need for follow-up review to ensure compliance with the requirements set forth in the CEO memo.

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

WKP. REF.

30. Review the association's website to determine there are no inappropriate or misleading website links.

31. Discuss with your EIC any planned or pending system conversion, transactional website plans not previously communicated to or filed with OTS, system-generated errors that affect integrity of management information or regulatory reports, or any other significant IT issues or concerns. After discussion with your EIC, notify your regional IT Examination Manager, as appropriate.

LEVEL II

After you complete the Level I examination procedures, if you need additional review to support an examination conclusion for a particular IT risk, you should review examination guidance and procedures in the FFIEC Information Technology Examination Handbook for the specific subject matter. These FFIEC Information Technology Examination Handbook procedures are considered Level II procedures for Examination Handbook Section 341.

You should complete the examination procedures in the FFIEC Information Technology Examination Handbook you deem necessary to test, support, and present conclusions derived from performing Level I procedures. Level II procedures provide additional verification regarding the level of technology risk and the effectiveness of a savings association's risk management processes and controls. You can use the FFIEC examination procedures in their entirety or selectively, depending on the examination scope and need for additional verification.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

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