

How to Use This Manual

Information Security Audit for Banks: Assessing Technology Risks is intended to assist all types of audit staff in performing audits of information. The manual also provides guidance on designing information security systems, outsourcing information security for support, and upgrading existing security systems. *Information Security Audit for Banks: Assessing Technology Risks* provides in-depth information regarding:

- Information security audit and the evaluation of systems and controls, including details regarding basic objectives
- Planning the information security audit
- Factors affecting the design and implementation of a dynamic information security audit program
- Weighing and/or measuring business considerations that affect the information security audit process
- Sample information security audit policy and general procedures
- Sample information security audit questionnaires for information security-related controls and processes
- Significant regulatory implications pertaining to information security audits
- Reminders about unique systems issues
- Underscoring of the importance of information risk assessments
- Sample information security audit programs for specific areas
- Sample information security systems overviews
- Examination of a bank's information security controls by external third parties, particularly federal financial institution regulatory examiners

For the experienced information security auditor, the guidance provided in the manual may be, in part, a reminder of what is already known and/or in practice at the bank with respect to audit. Much of the information is based on interagency and specific agency issuances and guidelines pertaining to information security. To help readers effectively audit information security, this manual provides the tools and up-to-date information necessary to do the job.

This manual analyzes emerging issues regarding information security and presents practical step-by-step instructions for auditing and protecting your bank's information. Protecting customer information has always been a major focus of financial institutions; regulatory actions such as the Gramm-Leach-Bliley Act (GLBA) and the USA PATRIOT Act have further underscored the importance of protecting information with respect to privacy and security against identity theft. As the marketplace continues to emphasize personal information and individual identity, the importance of information security will continue to grow.

For years, there was talk of a checkless society; 2003 brought a new first to the banking industry. For the first time, electronic payments surpassed cash and checks as the consumers preferred form of payment for in-store purchases. Decreasing check volume presents an enormous growth opportunity for electronic payments. The Federal Reserve Board approved revisions/amendments to Regulation CC to implement the Check 21 Act which became effective October 28, 2004. Check 21 authorized a new negotiable instrument called a substitute check and provides that a properly prepared substitute check is the legal equivalent of the original check for processing purposes. A substitute check, therefore, is a reproduction of the original check that meets specific legal

requirements and can be processed like a check. While checks are clearly a part of the financial services system, the movement of funds is edging closer to a paperless check environment.

The emergence of a checkless economy, additional ACH transactions, wire transfers, and online banking brings about growing IT demands. While technology continues to evolve, the issue of information security remains a permanent focus for financial institutions. Some key areas include:

- Data security
- Information breaches
- Acceptable Internet usage/security
- Disaster recovery and business continuity planning
- Service provider selection

Regulatory agencies have published numerous statements on the importance of information security and IT audits. Material in this manual incorporates guidance from the following sources:

- Office of Thrift Supervision
Various publications, including brochures, issuances, and documents that detail the regulatory requirements and current guidelines pertaining to trust powers and fiduciary account administration.
- Federal Deposit Insurance Corporation
Various publications, including brochures, issuances, and documents that detail the regulatory requirements and current guidelines pertaining to trust powers and fiduciary account administration.
- Office of the Comptroller of the Currency
Various publications, including brochures, issuances, and documents that detail the regulatory requirements and current guidelines pertaining to trust powers and fiduciary account administration.
- Board of Governors of the Federal Reserve System
Various publications, including brochures, issuances, and documents that detail the regulatory requirements and current guidelines pertaining to trust powers and fiduciary account administration.
- Accounting Profession Associations
Various publications, including brochures, issuances, and documents that detail specific audit requirements and current guidelines pertaining to trust powers and fiduciary account administration.
- Federal Trade Commission
Publications that underscore the significance of information security.
- Trade Associations
Publications that underscore the significance of information security.
- Security Organizations
Security organizations that promote sharing of information security insights and information between those responsible for managing and monitoring information security.

MULTI-FACTOR AUTHENTICATION

The federal regulatory agencies require each financial institution to have multi-factor authentication processes and controls in place for their e-banking programs. Institutions should work closely with their primary data processing

service providers to have a multi-factor software security program that encompasses the following types of controls:

- Layered security levels reflecting different risk ratings assigned by the institution and/or customer, utilizing different authentication techniques, e.g., response to phrase, date, picture, unique identifier, or other type of question.
- Registration of customer PC location

In addition, institutions should utilize multi-level tokens. This approach facilitates access by the designated individual from different PCs. Implementing a security software package for customer e-banking access, e.g., the software security program incorporates multi-factor authentication solution and also facilitates multi-level security for customers.

Regarding informing customers, the following are common techniques utilized to advise account holders of enhanced security procedures:

- E-mail communication
- Web site notice
- Statement stuffers
- Personalized letters and/or mailings, e.g., by name and specific account relationship
- Web site training video

In several instances, management team member point out that in preparing and implementing the multi-factor authentication controls, a major review was undertaken of internal policies and procedures. These reviews served as a process to further enhance internal controls and procedures and therefore, management commented there were ancillary benefits to the review.

ORGANIZATION OF MANUAL

The information security audit program and related procedures described in this manual represent a specialized audit focus; other specialized audit programs that internal auditors must address include technology, sale of retail nondeposit investment products, and insurance products. While it is critical that the information security audit program have specific procedures, internal questionnaires, reporting processes, and tracking of corrective actions, it is important that this specialized audit focus also be a subset of the institution's overall audit program. Through consistent audit approaches, well-founded basic audit objectives, and standard programs and procedures, the board of directors will receive a consistent overview of all audited activities. Therefore, in developing an information security audit program, it is important to build off the basics of a solid total organizational internal audit program.

The first chapters of this manual describe the basic audit philosophies and mechanics of a sound internal/external audit program. These basic foundations are the standards under which an information security audit program should function; the remaining chapters build on these basic audit concepts and guidelines to describe a proactive information security audit program.

YOUR COMPANION CD

As part of your purchase of *Information Security Audit for Banks* you receive a companion CD. This disc contains all of the information in your print manual that shows you how to make sure your information security audit process is being followed and accomplishing what it was intended to do.

Insert your CD into your desktop computer, and the autoplay feature will assist you in navigating the files. You can search quickly and easily for specific guidance and audit checklists.

Customize Your Program

To manage your information security audit function, the CD contains sample internal audit checklists, examples of documentation, and clear guidelines you can use for your own operation.

You can easily customize the documents on the CD using Microsoft Word so that you keep your audit reviews current with the latest compliance issues. Sample documents are provided so that you can easily adapt them to your specific requirements.