

HOW TO USE THIS MANUAL

Securing financial systems is a task better suited for the Corinthian king Sisyphus. Just as Sisyphus was condemned to watch the boulder roll back down the hill throughout eternity, the goal of a secure infrastructure seems equally unattainable for technology managers. Across the country, Information technology (IT) departments at financial institutions have implemented billions of dollars of security improvements. Hundreds of critical vulnerabilities have been secured. Still, the prospect of a secure infrastructure seems as distant as it was when the first firewalls were installed more than twenty years ago.

While the business of banking continues to change, so do the risk exposures that financial institutions face. In an environment of accelerating change, information technology has increasingly taken center stage as institutions continue to strive to offer new and more efficient means of delivering products and services to customers who rush to adopt them. The reality is that, as financial institutions increase their reliance on technology, they must also face and resolve an ever-changing host of new IT security risks.

At the center of this drama is the IT staff, and its responsibility is clear: to continue the movement toward new technologies without compromising the privacy and integrity of customer information, which would have a significant impact on the institution in terms of its operations, reputation, and the response from regulators. In meeting these challenges, IT professionals face a host of increasing and uncertain IT-related security risks. The purpose of this manual is to aid IT professionals in addressing those risks, armed with both an expert's guidance and a practical set of tools to meet the challenges they face every day.

ABOUT THIS REVISION

The IT Security Management Manual has been in publication for almost a decade. This revision reflects the factors influencing technology security in financial institutions within the past few years, and the increased focus on risk management. Cloud computing, virtualization, consumerization, and mobile access are addressed for the first time. And this is only the beginning.

In 2012, as in every year before, new technologies, threats, and regulations will demand critical updates to this manual. Among the most important is the first update to the FFIEC's authentication guidelines in six years. In conjunction with the release of the new version of this manual is the announcement of the IT Security Manual blog: (<http://www.itsecuritymanual.com>). Subscribe to the blog for updates on all security issues affecting IT systems at financial institutions. Your feedback is valuable to us. Please comment on the blog or contact us at inforeply@alexinformation.com. Use "K35" in the subject line of your communications.

ORGANIZATION OF THE MANUAL

The IT Security Management Manual has undergone a considerable reorganization and divides the original book into three sections: Assessments, Implementation, and Management. This structure provides an optimized framework that will allow for exciting new additions in the coming months.

PART I: ASSESSING IT SECURITY RISKS

Chapter I-1: Assessing IT Security Risks-A Regulatory Perspective

To respond to the ever-increasing computer security threats, the regulators have issued guidance on how to identify threats and vulnerabilities that your financial institution could be facing. In this chapter, we summarize the risks addressed in regulatory releases.

Chapter I-2: Conducting an IT Security Risk Assessment

Many of the items that regulatory examiners are required to review are the same as the items that management should already have carefully considered and reviewed as they developed their IT security strategy. Ensuring that these items have been properly developed will both protect the institution and its customers and prepare the institution to receive better results in its examinations.

Chapter I - 3: Internet Banking Risk Assessment

Assessing the risks involved in Internet banking is the necessary first step in instituting controls for those risks. Given the features of the Internet as a communication system, verifying with whom the institution is actually conducting business is essential.

Chapter I-4: Assessing Cloud Security

This chapter was written for financial institutions considering cloud solutions, which provides a thorough assessment framework. This chapter discusses assessment concerns in multi-tenant environments, cloud classification for assessment, contracts and service level agreements, and confidentiality of data. At the end of this chapter, you will find an exhibit with questions to ask possible cloud vendors to help decide compatibility and an appendix to help you create a Cloud Services Minimum Security Requirements document.

Chapter I-5: Snapshot Assessment

Rapidly understanding the immediate security situation is critical in planning a more in-depth approach. The Snapshot Assessment provided in this chapter will outline the steps required to gain this rapid understanding. For managers and executives facing a turn-around project this can prove invaluable.

Chapter I-6: Assessing Privacy Policies

This checklist is used to review the institution's disclosures and procedures for providing the privacy disclosure to consumers. The checklist is set up to conduct the review for individual consumers to determine if they received the required disclosure, but the review can be conducted on a global basis as well. For example, you could review the disclosures for a class of consumers.

PART II: IMPLEMENTING IT SECURITY RISK SOLUTIONS

Chapter II-1: Technology Risk Management in Financial Institutions: Getting Started

This chapter presents seven steps to manage technology risks. From the initial assignment of responsibilities, the steps walk the user through classifying risks, identifying risks, performing a risk assessment, reviewing policies, developing and implementing procedures, and conducting monitoring and examinations on an ongoing basis.

Chapter II-2: Internet Banking Risk Management

The unique delivery method of the Internet produces unique risks. In addition to highlighting common Internet service risks, this chapter also addresses compliance basics, key questions about Internet service operations, and an overview of what examiners will scrutinize.

Chapter II - 3: Desktop, Server, and Network Security

This chapter focuses in more detail on applying the security risks identified in the previous chapter to specific applications. Areas covered in this chapter include: desktops, network administration, email, and Internet.

Chapter II-4: Physical Security Risk

The risk of external threats from hackers via the Internet is a common topic of conversation when discussing security concerns, because the news media reminds us regularly how dangerous this situation can be. This chapter addresses the most common breaches of security: those that come directly from within an organization due to a lack of physical security and controls.

Chapter II-5: Securing Mobile and Wireless Systems

Wireless networking has its own set of components, standards, risks, vulnerabilities. This chapter discusses benefits and security issues associated with a wireless network, as well as with specific devices and formats.

Chapter II-6: Security of Customer Information

Specific safeguards are required by Sections 501 and 505(b) of the Gramm-Leach-Bliley Act. This chapter reviews the definitions and requirements, and includes checklists for both customer information security and a customer response program.

Chapter II-7: Securing Remote Deposit Capture

This chapter contains overviews of remote deposit capture, branch capture, Check 21, and the ACH rules. Following the overview, the focus is on the risks inherent in offering remote deposit capture and on managing those risks to better protect the financial institution.

Chapter II-8: Public Website Security

There are a number of issues surrounding the establishment of links between a financial institutions and third parties. This chapter discusses the primary risks involved with weblinking relationships and public website security.

PART III: MANAGING AND MONITORING IT SECURITY RISKS

Chapter III-1: Information Security Metrics

The performance metrics development process described in this chapter will assist information security practitioners in establishing a relationship between information system and program security activities under their purview and the organization mission, helping to demonstrate the value of information security to their organization.

Chapter III-2: IT Security Awareness Program

An important part of an overall IT security program is to make sure employees are trained in the dos and don'ts associated with using the institution's hardware and software and accessing the network and the Internet. This chapter presents a general outline on which to base a staff training program.

Chapter III-3: Mitigating Information Security Risk Through Insurance

Financial institutions are turning to insurance companies for help in managing information security risks. Until recently, most insurance coverage has failed to keep up with risks related to the Internet. However, new policies are coming out that specifically deal with losses stemming from entire systems crashing because of sabotage or hackers or virus attacks that destroy data and programs.

Chapter III-4: Computer Security Logs and Audit Trails

Sound computer security log management and audit trails are essential in the IT environment. This chapter provides practical, real-world guidance on developing, implementing and maintaining effective security log management and audit trail practices throughout an organization.

Chapter III-5: Backup and Recovery Planning

One of the most important operational responsibilities assigned to the IT area is to create, manage, and test procedures for reducing or eliminating down time. This section reviews the best way to address creating a data backup and recovery plan for your IT network operations.

Chapter III-6: Creating a Disaster Recovery Plan

In planning for its recovery from a disaster, a financial institution can benefit from best practices developed by organizations that have had real experience. This chapter addresses writing effective disaster recover procedures, maintaining continuity for the work force, following the 12 critical steps to disaster recovery, and managing remote access to data.

Chapter III-7: Continuity Planning and the Systems Development Life Cycle

The system development life cycle (SDLC) refers to the full scope of activities associated with a system during its life span. The life span begins with project initiation and ends with system decommission. Although business continuity planning is associated with activities occurring in the operation/maintenance phase, contingency measures should be identified and integrated at all phases of the computer system life cycle. This chapter describes approaches in which contingency strategies can be incorporated throughout the SDLC.

Chapter III-8: Monitoring IT Security

One of the most important operational responsibilities assigned to the IT area is to create, manage, and test procedures for reducing or eliminating down time. In this chapter, we look at how to monitor and manage security risks.

Chapter III-9: Security Policies

The management of an effective IT security program is based, in part, on a series of separate but related policies and procedures. In this chapter, we provide sample policies and procedures for major policy areas.

Chapter III-10: Required Disclosures

Under the “Electronic Signatures in Global and National Commerce Act” (15 USC 7001) (E-Sign Act), if a statute, regulation, or other rule of law requires that disclosures or other information relating to transactions be provided or made available to a consumer in writing, the information can be provided to the consumer electronically.

Chapter III-11: Complying with Customer Identification Requirements

Customer identification program requirements relate to the identity of any person who applies to open an account. This chapter covers the requirements for financial institutions.

COMPANION CD

With your order of the *IT Security Management Manual*, you can receive the entire contents of the manual, plus sample programs, policies and worksheets on CD. The easy-to-browse companion CD presents the entire manual, and allows you to search for information and print materials.