

## Volume 1

### **Chapter 1** Planning the IT Audit

An effective IT Audit begins with solid planning. The right workprograms, questionnaires, and requests for information will increase the effectiveness and the applicability of the IT audit. It is during this phase that the necessary resources to complete the audit become clear. This chapter describes the phases in the audit cycle, how to conduct a risk assessment, and how to develop effective internal control questionnaires.

### **Chapter 2** The IT Environment

This section explores the rapidly changing IT environment, the systems, and the processes of a financial institution. It is important to the IT audit that you understand the areas, such as the system selection process, in-house versus outsourced solutions, and strategic technology planning that impact the IT environment. This chapter will help the person charged with the IT audit responsibility to become more familiar with the technology used in the institution. This chapter provides background that will help navigate through the IT environment.

### **Chapter 3** IT Audit Areas

This chapter offers practical suggestions for addressing important areas involved with the IT audit. Is management kept informed of IS activities? Should you review employee accounts for unusual activity? Does the contingency plan serve as a guide for effectively dealing with disasters? Does the Internet banking policy communicate the strategic, operational, and risk management considerations to effectively manage this new technology? This chapter also covers one of the highest risk areas in financial institutions — wire transfers.

### **Chapter 3A** IT Auditing and Fraud Detection and Prevention

This chapter discusses analytical techniques that can be used by fraud auditors and relates, where applicable, how these same techniques are used in external audits. IT is often asked to assist with this effort. Therefore, the material in this chapter should help IT to understand the fraud audit objectives used to structure analytical techniques using computer software and files.

### **Chapter 4** Network and Internet Security

Due to decentralized computing environments and increased connectivity to the outside world, Network Security Reviews have become a natural extension of the tradition IT audit. Because most security breaches occur internally, the best IT audits consider internal and external conditions, as well as situation-specific issues. This chapter discusses how information security weaknesses can disrupt operations, increase the risk of fraud, and inadvertently disclose confidential information. The chapter addresses vulnerability assessments, network design considerations, improved security using network addresses translations, host

naming and URL conversions, sample network security review workprograms, and a sample information security policy.

### **Chapter 5** Case Studies

These case studies are based on factual situations and presented in an easy-to-read format that is informative and entertaining.

### **Chapter 6** Business Continuity Planning

Business planning is the responsibility of the financial institution's management, not its vendors. But when writing a plan, what issues make the perfect plan? Usually People are at the top of the list of concerns followed by Power, Communications, and Physical process. This chapter provides a discussion of these issues, checklists for reviewing the contents of a plan, and a sample business continuity plan validation in accordance with the FFIEC.

### **Chapter 6A** Model Policies

This chapter contains model policies, related to information technology and information security. Examiners and auditors will expect a financial institution to maintain most, if not all, of the policies in this chapter.

## **Volume 2**

### **Regulatory Issuances Index**

## **IT Examinations**

### **Introduction** IT Handbook InfoBase

### **Chapter 7** IT Audit Guidance

The IT audit program has taken on greater significance in recent years, and the examiners are expecting to see an effective internal audit program in place. This chapter includes excerpts from the FFIEC's audit booklet and provides the examiners' audit examination procedures in a checklist format from which you can determine the quality and effectiveness of your audit function related to IT controls.

### **Chapter 8** Business Continuity Planning Guidance

Business continuity planning is clearly a business issue affecting the enterprise and requiring significant documentation and communication. This chapter contains excerpts from the FFIEC's booklet on business continuity planning and provides the examiner's procedures in a checklist format to help you determine the quality and effectiveness of your institution's business continuity planning process.

### **Chapter 8A** Intrusion Response Procedures

Unauthorized intrusion into the institution's network is a significant risk. Institutions must implement security procedures to prevent such intrusions from occurring and to respond should one occur. This chapter provides detailed intrusion response procedures to help you be prepared.

**Chapter 9** E-Banking Guidance

The term “e-banking” encompasses the older technology of ATMs up to the newer technology of Internet banking and self-serve kiosks. The risks involved in e-banking are clearly present, and the challenge for the banking industry is to balance security with convenience. This chapter presents excerpts from the FFIEC booklet on e-banking and provides the examiner’s procedures in a checklist format to help you determine if your e-banking products and services are provided in a safe and sound manner.

**Chapter 10** FedLine Guidance

The funds transfer function is one of many features of FedLine. It is the most important to the IT auditor and potentially carries the highest risk. This chapter contains excerpts from the FFIEC booklet on FedLine funds transfer application and the examiner’s procedures in a checklist format to help you determine the adequacy and effectiveness of your institution’s FedLine funds transfer internal controls environment and the related risk management process.

**Chapter 11** Information Security Guidance

The protection of a financial institution’s information is the foundation that establishes confidence and trust with its customers. To help you assess the quality of risk and the effectiveness of your institution’s processes, the chapter provides excerpts from the FFIEC’s latest booklet on information security and the examiners procedures in convenient checklist format.

**Chapter 12** Supervision of Technology Service Providers Guidance

The responsibility to ensure your technology service providers operate in a safe and sound manner falls on your Board of Directors and management. This chapter contains excerpts from the FFIEC’s booklet on outsourcing supervision and will help you better understand what the regulators expect.

**Chapter 13** Retail Payment Systems Guidance

As check image exchanges and other third parties enter the payments system, the flow of transactions becomes more complex, calling for new controls to manage risk. This chapter addresses checks and electronic payments, and includes examination procedures, a glossary, and a list of laws, regulations, and guidance.

**Chapter 14** Development and Acquisition Guidance

Knowing how to define the institution’s requirements for information technology systems, acquire the right technologies, implement them successfully, and then maintain the systems is critical to the safety and soundness of any institution. This chapter summarizes the FFIEC’s guidance for project management, development, acquisition and maintenance. It also includes examination procedures and a glossary.

**Chapter 15** Management Guidance

Effective management of IT resources is integral to aligning the institution’s technology purchases with strategic business goals. With the increasing role of technology, one must manage the entire IT enterprise, not just the computer room. This chapter covers roles and responsibilities, IT risk management process, and management considerations for technology service providers, and includes examination procedures, a glossary, and a section on laws, regulations, and guidance.

**Chapter 16** Outsourcing Technology Services Guidance

Many financial institutions outsource typical business functions, such as credit card process, ATM/debit card processing, Internet banking, and electronic bill payment. Certain responsibilities exist for management to ensure that outsourcing relationships are properly managed. This chapter covers board and management responsibilities, risk management, and related topics. It also includes examination procedures, a section on laws, regulations, and guidance, and a section on foreign-based third-party service providers.

**Chapter 17** Operations Guidance

Despite all the hype surrounding electronic banking, outsourcing, and information security, in order to survive a financial institution must execute the fundamentals of daily operations. These fundamental business processes make up a financial institution's operations. This chapter gives an overview of the challenges financial institutions face on a daily basis, while laying the groundwork for operations that are scaleable and sound.

**Chapter 18** Wholesale Payment Systems Guidance

Wholesale payment systems allow a global exchange of funds in our increasingly interconnected world. This chapter offers guidance to help improve the current controls over wholesale payment systems, or prepare for the potential impact these systems may have on financial institutions originating or receiving such payments.

# TABLE OF CONTENTS

---

About the Author .....	iii
Acknowledgements.....	v
Introduction.....	vii
Chapter Overview .....	xi

## VOLUME 1

### CHAPTER 1

#### Planning the IT Audit

<b>Audit Planning</b> .....	1-1
<b>Selecting Outside Auditing Assistance</b> .....	1-1
Qualifications.....	1-2
Other Considerations.....	1-3
<b>Interviewing Potential Candidates</b> .....	1-3
Government Auditing Qualifications .....	1-3
<b>IT Audit Standards</b> .....	1-3
Statement on Auditing Standards No. 94 (SAS 94) .....	1-4
Statement on Auditing Standards No. 70 (SAS 70) .....	1-4
COSO .....	1-4
Shared Application Software Review (SASR).....	1-5
Basel Committee on Banking Supervision.....	1-6
BS 7799 — Code of Practice for Information Security Management .....	1-6
COBIT and the Information Systems Audit and Control Association (ISACA) .....	1-7
Federal Information System Controls Audit Manual (FISCAM) .....	1-7
<b>Audit Software</b> .....	1-7
<b>The IT Audit Cycle</b> .....	1-8
The IT Audit Cycle: The Three Phases of the Typical IT Audit.....	1-9
<b>Developing the IT Audit Schedule</b> .....	1-10
<b>Performing the IT Risk Assessment</b> .....	1-10
Risk Defined .....	1-10
Risk Assessment Methods .....	1-10
What Do the Regulators Say About Risk? .....	1-11
<b>One Simple Approach to the IT Risk Assessment</b> .....	1-12
The IT Risk Assessment Process .....	1-13
<b>Sample IT Risk Assessment Form</b> .....	1-14
<b>Sample Completed IT Risk Assessment Form</b> .....	1-20
<b>Sample IT Risk Assessment Summary</b> .....	1-25
<b>Sample IT Risk Assessment Condensed Summary</b> .....	1-30
<b>Top Ten Signs Your Financial Institution Needs a Technology Plan</b> .....	1-31
<b>Audit Workpapers</b> .....	1-32

<b>Developing the Request for Information</b> .....	1-33
<b>Developing the Internal Control Questionnaire</b> .....	1-33
<b>Overview of the Gramm-Leach-Bliley Act and Its Impact on Information Technology</b> .....	1-34
Privacy Notices .....	1-34
Regulatory Implications .....	1-34
Section 501(b) Requirements .....	1-34
The Risk Assessment: Getting Started .....	1-35
<b>The GLBA Risk Assessment Process</b> .....	1-36
<b>Instructions for Completing the GLBA Information Security Risk Assessment</b> .....	1-36
Final Steps.....	1-38
<b>Sharing of Account Number Information for Marketing Purposes</b> .....	1-38
<b>Five Keys to Surviving Your Next IT Examination</b> .....	1-39
Exhibit 1.1: Interviewing the IT Auditor .....	1-41
Exhibit 1.2: Sample 1: IT Audit Schedule .....	1-42
Exhibit 1.3: Sample 2: IT Audit Schedule .....	1-43
Exhibit 1.4: Gantt Chart for Audit Scheduling.....	1-44
Exhibit 1.5: Request for Information.....	1-45
Exhibit 1.6: Internal Control Questionnaire.....	1-47
Exhibit 1.7: Data Center Internal Control Questionnaire.....	1-57
Exhibit 1.8: IT Audit Workprogram.....	1-62
Exhibit 1.8A: IT Audit Checklist .....	1-77
Exhibit 1.8B: Network Vulnerability Assessment Checklist.....	1-81
Exhibit 1.9: Systems and Information Inventory .....	1-83
Exhibit 1.10: Information Asset Classification.....	1-84
Exhibit 1.11: Possible Threats.....	1-91
Exhibit 1.12: Input Sheet with Asset Classification.....	1-94
Exhibit 1.13: Information Security Risk Assessment Input Model with Asset Classification ...	1-102
Exhibit 1.14: Risk Matrix.....	1-111
Exhibit 1.15: Information Security Risk Assessment Summary.....	1-112
Exhibit 1.16: Risk Mitigation Action Plan.....	1-116

## CHAPTER 2

### The IT Environment

<b>Understanding the Financial Institution's Technology Environment</b> .....	2-1
<b>Strategic Technology Planning</b> .....	2-2
Anatomy of a Strategic Technology Plan .....	2-2
User Survey .....	2-2
SWOT Analysis .....	2-2
Competitive Analysis .....	2-2
Goal Setting.....	2-3
Defining the Team .....	2-3
Setting Priorities.....	2-3
Estimating Costs .....	2-4
The Action Plan .....	2-4
Strategic Technology Plan Benefits .....	2-4

<b>System Selection</b> .....	2-5
Changing Systems.....	2-5
System Selection Goals and Objectives.....	2-6
Proposal Evaluation/Decision Criteria.....	2-6
Anatomy of a System Selection .....	2-7
<b>Outsourcing vs. In-House</b> .....	2-10
Service Provider Documentation Checklist .....	2-11
<b>IT Infrastructure Issues</b> .....	2-12
<b>Information Systems Profile</b> .....	2-13
<b>Systems Development Life Cycle (SDLC)</b> .....	2-14
Death of a System .....	2-14
<b>Regulator “Hot Buttons”</b> .....	2-14
Business Continuity Planning.....	2-15
The Gramm-Leach-Bliley Act and Information Security.....	2-15
IT Risk Management .....	2-15
User Access Controls.....	2-15
Network Security .....	2-16
Directorate Awareness of IT Activities.....	2-16
<b>Technology Trends and Surveys</b> .....	2-16
How Is Your Bank’s Core Processing Done? .....	2-17
Top 10 Long-Term Technology Decisions Facing Your Bank.....	2-17
Top 10 Strategic Technologies for 2009.....	2-17
How People Use The Internet .....	2-18
Top Ten Inventions and Discoveries in History .....	2-18
Top Electronic Payment Instruments .....	2-18
Exhibit 2.1: 20 Questions for Vendor References.....	2-20
Exhibit 2.2: 20 Rules of Vendor Negotiation .....	2-21
Exhibit 2.3: Main Office and Two Branches with Frame Relay and Wireless Internet Access .....	2-23
Exhibit 2.4: Main Office and Five Branches, Point-to-Point T-1 Lines to Branches, Fiber to Contact Center, DSL Internet Access.....	2-24
Exhibit 2.5: Main Office and Eight Branches, Frame Relay and Point-to-Point, Integrated Voice and Data, Home VPN Users, T-1 Internet Access.....	2-25
Exhibit 2.6: Financial Institution Technology Environment .....	2-26

## CHAPTER 3

### IT Audit Areas

<b>Management</b> .....	3-1
Board of Directors.....	3-1
Position Descriptions .....	3-1
<b>Job Descriptions</b> .....	3-2
Sample Job Description for Chief Technology Officer (CTO).....	3-2
Qualifications .....	3-2
Responsibilities .....	3-2
Requirements.....	3-3

<b>Sample Organizational Charts for the IT Area</b> .....	3-3
IT Steering Committee.....	3-6
IT Steering Committee Charter.....	3-6
Strategic Technology Planning.....	3-7
System Selection Due Diligence.....	3-7
Review of Vendor Financials.....	3-8
Audit and Examination Response.....	3-8
<b>ABC Bank Sample Audit and Examination Response Procedure</b> .....	3-9
Purpose.....	3-9
Scope.....	3-9
Procedure.....	3-9
Sample Audit and Examination Response Procedure Table for ABC Bank.....	3-10
IT Training and User Education.....	3-10
Hiring Standards.....	3-11
Legal Arguments.....	3-11
Terrorist Attacks Make Organizations Reconsider Hiring Standards.....	3-12
Employment Eligibility Requirements.....	3-12
FDIC Criminal Offense Policy.....	3-13
Fair Credit Reporting Act Considerations.....	3-14
Criminal Background Checks.....	3-14
Verification of Education.....	3-14
Terminated Employees.....	3-15
Vacation Policies.....	3-15
Contract Management.....	3-16
<b>Audit and Control</b> .....	3-16
Auditor Independence.....	3-16
Internal Audit Involvement on Projects and Committees.....	3-16
Audit Schedule.....	3-17
Internal IT Audit Program.....	3-17
<b>Internal IT Audit Outsourcing</b> .....	3-17
Interagency Policy Statement on the Internal Audit Function and Its Outsourcing.....	3-17
Roles — The Internal Audit Coordinator.....	3-19
Board of Directors and Senior Management Responsibility.....	3-19
Workpapers and Reporting.....	3-19
<b>ACH Audit</b> .....	3-20
<b>Data Center Invoice Audit</b> .....	3-20
<b>Employee Account Reviews</b> .....	3-21
Stating the Case for Account Review.....	3-21
Conducting the Review.....	3-22
<b>Development and Acquisition</b> .....	3-23
Support and Delivery.....	3-24
Master File Changes.....	3-24
Dormant Account Transaction Processing.....	3-25
System Parameters.....	3-25
Item Processing.....	3-25
Items in Transit.....	3-26

Account Reconciliation .....	3-26
Data Analysis/Master File Downloads .....	3-27
<b>Protecting Information</b> .....	3-28
<b>Reviewing Internet Banking and the Web Site</b> .....	3-28
<b>Web Site Hosting Security</b> .....	3-28
<b>Imaging Technologies</b> .....	3-29
Report Archive.....	3-29
Image Item Processing.....	3-29
Document Imaging.....	3-30
Control and Security Risks in Electronic Imaging Systems .....	3-30
<b>Contingency Planning</b> .....	3-31
Preventive Measures .....	3-32
Sample Plan Contents.....	3-32
Off-Site Storage .....	3-34
Plan Testing Methods.....	3-34
Physical Security .....	3-35
Building Access .....	3-36
Emergency Power.....	3-36
Fire-Resistant, Not Fireproof.....	3-36
Backup Systems .....	3-37
Redundancy.....	3-37
Email Backups .....	3-37
Storage Area Networks (SANs).....	3-38
<b>Electronic Funds Transfer Activities</b> .....	3-38
FedLine II Local Security .....	3-38
Local Security Administration.....	3-39
Segregation of Duties .....	3-39
Wire Transfer Policy.....	3-39
Funds Transfer Insurance Coverage .....	3-40
Wire Transfer Credit Risk .....	3-40
Physical Security of FedLine Systems .....	3-40
Automated Teller Machine (ATM) Processing.....	3-40
Major ATM Risks .....	3-40
Typical ATM Processing Environments.....	3-41
Offline Processing .....	3-41
Online Processing .....	3-41
Debit Cards .....	3-41
ATM/Debit Card Audit Steps .....	3-42
Automated Clearinghouse (ACH).....	3-42
Managing ACH Risk .....	3-42
<b>Mobile Payment Security</b> .....	3-43
Mobile Payments Definition .....	3-43
Types of Mobile Services .....	3-43
Mobile Payment Services Framework.....	3-43
Regulatory Issues.....	3-44
Customer Registration .....	3-44

Technology and Security Standards .....	3-44
Inter-Operability .....	3-44
Clearing and Settlement for Inter-Bank Funds Transfer Transactions .....	3-45
Customer Complaints and Grievance Redress Mechanism .....	3-45
Need for Board Approval .....	3-45
Technology and Security Standards .....	3-45
Customer Protection Issues .....	3-47
List of Abbreviations .....	3-48
Exhibit 3.1: Ten Tips for Successfully Managing a Regulatory Examination or External Audit .....	3-50
Exhibit 3.2: Employment Eligibility Requirements.....	3-51
Exhibit 3.3: Regional Payments Associations .....	3-53
Exhibit 3.4: Data Center Invoice Audit, Core Processing Services Worksheet.....	3-54
Exhibit 3.5: Web Site and Internet Banking Features Checklist .....	3-59
Exhibit 3.6: Web Site Hosting Security Workprogram.....	3-63
Exhibit 3.7: Internet Banking System Questionnaire/Workprogram.....	3-66
Exhibit 3.8: Auditing Bill Pay: Bill Payment System Questionnaire/Workprogram.....	3-68
Exhibit 3.9: Imaging System Questionnaire.....	3-69
Exhibit 3.10: Document Imaging System Features Checklist.....	3-70

## CHAPTER 3A

### IT Auditing and Fraud Detection and Prevention

<b>Internal vs. External Fraud Audit Expectations</b> .....	3A-1
<b>Detecting Financial Statement Fraud</b> .....	3A-1
Conducting Analytical Auditing Procedures.....	3A-2
Auditing Accounting Estimates .....	3A-4
Think Like a Fraudster .....	3A-6
<b>Using Computer Software to Test for Fraud</b> .....	3A-9
Audit Software Capabilities .....	3A-9
Ratio Analysis .....	3A-11
Benford's Law .....	3A-11
How to Use Audit Software.....	3A-12
How Fraud Detection Programs Work .....	3A-13
Neural Networking Technology .....	3A-13
How Neural Networks Work .....	3A-13
Fraud Detection Software Resources .....	3A-14
<b>Implementing an Employee Surveillance Program</b> .....	3A-14
Employee Accounts.....	3A-15
Stating the Case for Account Review.....	3A-16
Conducting the Employee Review .....	3A-16
Step 1 — Evaluate Operational Risk Issues .....	3A-17
Step 2 — Review Privacy Laws.....	3A-18
Exceptions .....	3A-18
Step 3 — Establish Surveillance Program Policy Objectives.....	3A-19
Objective 1: Prevention .....	3A-20

Objective 2: Detection.....	3A-21
Objective 3: Investigation .....	3A-22
Objective 4: Reporting.....	3A-22
Step 4 — Establish Surveillance Policies.....	3A-22
Employee Information Privacy Policy .....	3A-22
Employee Medical Privacy Policy.....	3A-23
Employee Surveillance Policy.....	3A-23
Step 5 — Review Surveillance Best Practices .....	3A-24
Background Checks .....	3A-25
Medical Testing.....	3A-25
Litigation Prevention, Policies and Discipline .....	3A-25
Notifying Employees .....	3A-26
Surveillance and Monitoring.....	3A-26
Off-Premises Productivity Management and Physical Security.....	3A-26
Step 6 — Evaluate Available Technologies.....	3A-27
Desktop Monitoring Programs .....	3A-27

## CHAPTER 4

### Network and Internet Security

<b>Network Security</b> .....	4-1
More Security Incidents on the Radar .....	4-1
Security Industry Growing.....	4-1
Basic IT Audits Just Not Enough These Days.....	4-2
“We Have Met the Enemy and He Is Us” — Internal Security Breaches .....	4-2
Profile of the Average Hacker .....	4-3
The Internet Isn’t the Only Entrance.....	4-3
Fighting Phishing, Pharming, and Spoofing.....	4-3
Phishing .....	4-3
Pharming.....	4-4
Spoofing.....	4-4
Domain Name Security Checklist.....	4-5
Summary.....	4-5
Customer Guidance on Phishing Scams.....	4-5
FACTA Summary .....	4-8
Identity Theft.....	4-8
Free Credit Reports.....	4-8
Disposal of Customer Information .....	4-8
Fraud Alerts .....	4-8
Active Duty Alerts .....	4-9
Truncation of Credit Cards, Debit Cards, Social Security Numbers.....	4-9
<b>Notifying Customers of Security Breaches</b> .....	4-9
GLBA and the Customer Response Program Guidance — Related Issues .....	4-9
Security Guidelines .....	4-10
Risk Assessment and Controls.....	4-10
Service Provider Requirements .....	4-10

Response Program Requirements .....	4-11
Components of a Response Program .....	4-11
Assess and Identify .....	4-11
Notify the Regulators .....	4-12
Notify Regulators of Service Provider Security Incidents .....	4-12
Notify Law Enforcement .....	4-12
SAR Reporting for Computer Intrusions .....	4-12
Contain and Control the Situation .....	4-12
Customer Notice .....	4-13
Summary .....	4-15
<b>Network Security Audit Approaches .....</b>	<b>4-15</b>
<b>Network Best Practices Test .....</b>	<b>4-15</b>
<b>Network Design .....</b>	<b>4-17</b>
1985 to 1990 .....	4-18
1990 to 1995 .....	4-18
1995 to 2000 .....	4-18
2000 to the Present .....	4-18
Computing Power .....	4-18
The Typical Network .....	4-19
Network Benefits .....	4-19
Considerations When Designing or Planning the Network .....	4-20
Financial Institution-Specific Network Applications .....	4-21
<b>Network Administrator Job Description .....</b>	<b>4-22</b>
Required Skills .....	4-22
Responsibilities .....	4-23
<b>Network Topologies .....</b>	<b>4-23</b>
Star .....	4-24
Bus .....	4-25
Ring .....	4-26
<b>Novell Netware Security .....</b>	<b>4-26</b>
Step-by-Step Audit Guide .....	4-26
Novell Directory Services .....	4-27
Security Equivalences .....	4-28
Network User Account Settings .....	4-28
Terminated Employee User Accounts .....	4-29
<b>Windows NT/2000 Security .....</b>	<b>4-29</b>
IIS Issues (Microsoft Internet Information Server) .....	4-29
File Sharing .....	4-31
<b>Windows Security Settings .....</b>	<b>4-32</b>
The Center for Internet Security (CIS) Recommended Security Settings .....	4-32
Auditing Policy .....	4-33
Password Policy .....	4-34
Account Lockout Policy .....	4-35
<b>Wireless Networks .....</b>	<b>4-36</b>
Point-to-Point Wireless .....	4-36
Broadcast Wireless .....	4-37

---

Security Issues Becoming Clearer Through Security Audits .....	4-37
Wireless Network Design Considerations.....	4-38
Regulators Weigh in on Wireless .....	4-38
Summary .....	4-39
<b>Virus Protection</b> .....	4-39
Viruses, Worms, and Trojan Horses.....	4-39
Updating Virus Software.....	4-39
Virus Software Auditing .....	4-39
Virus Response.....	4-40
Virus Protection Awareness .....	4-40
The Case of the Vendor and the Worm .....	4-40
<b>Vulnerability Assessments</b> .....	4-41
Vulnerability Assessment Results Based on IP Addresses.....	4-41
Internet Banking Server Vulnerability Assessment .....	4-41
File Transfer Protocol (FTP) Access .....	4-41
Direct Dial Vulnerability Tests .....	4-41
Direct Dial Vulnerability Test Results .....	4-42
<b>Intrusion Detection Systems (IDS)</b> .....	4-42
Host-Based IDS .....	4-42
Network-Based IDS .....	4-43
Attack Signatures: Haven't I Seen You Somewhere Before?.....	4-43
Intrusion Response Policy: Someone's Knocking on the Door.....	4-43
A Trap: Like Flies to Honey .....	4-44
Before IDS: You Don't Know What You Don't Know .....	4-44
<b>The Importance of the Information Security Policy</b> .....	4-44
<b>The Twenty Most Critical Internet Security Vulnerabilities</b> .....	4-45
<b>Most Critical Internet Security Vulnerabilities</b> .....	4-45
Client-Side Vulnerabilities.....	4-46
Server-Side Vulnerabilities.....	4-46
Security Policy and Personnel.....	4-46
Application Abuse.....	4-46
Network Devices.....	4-46
Zero Day Attacks .....	4-46
<b>Protecting Vulnerable Ports on Your Network</b> .....	4-47
<b>Reviewing Routers</b> .....	4-48
Pinging the Router.....	4-50
<b>Tape Backups</b> .....	4-50
<b>Backup Matrix</b> .....	4-53
<b>VPN Security Considerations</b> .....	4-54
<b>Improved Security Using Network Address Translation</b> .....	4-54
What Is Network Address Translation .....	4-55
5 Steps to Improved Security Using NAT.....	4-56
Step 1 — Select the Best Type of NAT.....	4-56
Step 2 — Review the Processing Order for NAT.....	4-56
Step 3 — Understand NAT Limitations .....	4-57
Step 4 — Use Split Horizon DNS .....	4-58

Step 5 — Properly Configure Split Horizon DNS .....	4-59
<b>Host Naming and URL Conventions</b> .....	4-60
The Security Issue .....	4-60
Six Common Attack Threats .....	4-61
Registration of Similarly Named Domains .....	4-62
Manipulation of Complex URLs .....	4-62
Top Four Security Best Practices .....	4-63
1. Domain Names and Host Services .....	4-64
2. URL Referencing .....	4-66
3. Serial Host Naming .....	4-68
4. Domain Registration Monitoring .....	4-69
Exhibit 4.1: Sample Network Security Review Workprogram .....	4-70
Exhibit 4.1A: Network Vulnerability Assessment Workprogram .....	4-78
Exhibit 4.2: Sample Vulnerability Assessment Test .....	4-81
Exhibit 4.3: Sample AS/400 Operations Internal Audit Workprogram .....	4-82
Exhibit 4.4: Sun Solaris Security Workprogram .....	4-84
Exhibit 4.5: Change Management Form .....	4-86
Exhibit 4.6: VPN Security Implementation Checklist .....	4-87

## CHAPTER 5

### Case Studies

<b>Good Teller or Bad Craps Player?</b> .....	5-1
Lessons Learned .....	5-3
<b>The Perfect Loan Officer?</b> .....	5-3
Lessons Learned .....	5-4
<b>Human Resources: Who Would Look There?</b> .....	5-5
Lessons Learned .....	5-5
<b>Mind If I Borrow Your Password During the Conversion?</b> .....	5-6
Lessons Learned .....	5-7
<b>Truth Is Stranger Than Fiction, Especially When It Involves Fictional Loans</b> .....	5-8
Lessons Learned .....	5-9
<b>Oh, the Things You Learn When You Fire Your Network Administrator</b> .....	5-9
Lessons Learned .....	5-11
<b>No WAN Is an Island</b> .....	5-11
Lessons Learned .....	5-13
<b>The Enemy Within</b> .....	5-14
Lessons Learned .....	5-15
<b>The “No Email Left Behind” Act</b> .....	5-15
Lessons Learned .....	5-16
<b>When Your ISP Is DOA</b> .....	5-17
Lessons Learned .....	5-18
<b>You Don’t Need a Definition: You’ll Know It When You See It</b> .....	5-18
Lessons Learned .....	5-20

## CHAPTER 6

### Business Continuity Planning

<b>A New Day for Business Continuity Planning</b> .....	6-1
Management's Role in Business Continuity.....	6-1
Writing the Perfect Plan .....	6-2
Business Impact Analysis.....	6-2
Step One: Identify Critical Functions and Resources .....	6-3
Step Two: Establish Time Frames for Recovery .....	6-4
Step Three: Prioritize Functions/Resources Chronologically.....	6-5
Business Continuity's Big Four.....	6-6
Three Types of Disasters .....	6-7
Natural Disasters .....	6-7
Human-Caused Disasters.....	6-7
Technological Disasters.....	6-7
Communications .....	6-8
Alternate Communications .....	6-8
New Business Continuity Technologies.....	6-9
Email Retention.....	6-10
Distribution Record.....	6-10
Transportation Issues.....	6-10
Master Vendor List.....	6-11
Local Authorities/Emergency Numbers.....	6-11
Insurance Considerations .....	6-12
Testing and Validation .....	6-12
Manual Operations.....	6-12
Public Relations/Reputation Management .....	6-13
Financial Issues .....	6-13
Security Issues .....	6-13
Security Awareness Training.....	6-14
<b>Pandemic Influenza Threat</b> .....	6-14
What's Happening Now? .....	6-14
H1N1 Flu (Swine Flu).....	6-15
The Private Sector and Critical Infrastructure Entities .....	6-16
<b>Technological Advances Help ... and Hurt ... Personal Disaster Preparedness</b> .....	6-16
1. Get to Know Your Telephone — Single Line Analog to Voice over IP (VoIP).....	6-16
2. View Your Automobile as a Potential Power Source and Mobile Communications Tool .....	6-17
3. Don't Count Terrestrial Radio Out Just Yet .....	6-17
4. Get the Right Fire Extinguishers and Know How to Use Them.....	6-17
5. Copy or Scan Personal Information .....	6-17
6. Back up Your Home PC: It Probably Packed on a Few More Bytes Recently.....	6-18
7. Stock Up on Bottled Water .....	6-18
8. Establish a Friends and Family Communications Plan .....	6-18
Summary .....	6-19
Business Continuity Web Resources.....	6-19
<b>Business Continuity Plan Checklist</b> .....	6-19

<b>Sample Business Continuity Plan Roundtable Test</b> .....	6-24
Summary of Roundtable Test .....	6-24
Index of Disaster Scenario/Disaster Events .....	6-25
Core Business Processes.....	6-26
Contingency Plan Testing Matrix .....	6-26
Validation Scenarios/Disaster Events .....	6-27
<b>Business Continuity Risk Assessment</b> .....	6-35
Final Steps.....	6-36
Business Continuity Risk Assessment .....	6-37
Sample Completed BCP Risk Assessment .....	6-39
Business Continuity Risk Assessment Summary .....	6-41

## CHAPTER 6A

### Model Policies

<b>Asset Management Policy</b> .....	6A-3
<b>Blackberry Policy</b> .....	6A-4
<b>Blogging Policy</b> .....	6A-6a
<b>Business Continuity Planning Policy</b> .....	6A-7
<b>Cell Phone Policy</b> .....	6A-8
<b>Disposal of Information Policy</b> .....	6A-10
<b>Electronic Banking Policy</b> .....	6A-11
<b>Email Usage Policy</b> .....	6A-19
<b>Firewall Administration Policy</b> .....	6A-21
<b>Hardware and Software Standards Policy</b> .....	6A-22
<b>Information Security Program Policy</b> .....	6A-24
<b>Internet Banking Policy</b> .....	6A-31
<b>Internet Usage Policy</b> .....	6A-37
<b>Intrusion Response Policy</b> .....	6A-39
<b>IT Steering Committee Policy</b> .....	6A-41
<b>Laptop Policy</b> .....	6A-43
<b>Network Administration Policy</b> .....	6A-46
<b>Pandemic Influenza Policy</b> .....	6A-48
<b>Patch Management Policy</b> .....	6A-49
<b>PDA Policy</b> .....	6A-50
<b>Physical Security Policy</b> .....	6A-51
<b>Remote Access Policy</b> .....	6A-53
<b>Security Administration Policy</b> .....	6A-55
<b>Security Awareness Training Policy</b> .....	6A-58
<b>Software Management and Licensing Policy</b> .....	6A-60
<b>Spam Policy</b> .....	6A-62
<b>Spyware Policy</b> .....	6A-63
<b>System Access/Change Management Form</b> .....	6A-65
<b>Systems Backup Policy</b> .....	6A-66
<b>User ID and Password Standards Policy</b> .....	6A-68
<b>Virus Protection Policy</b> .....	6A-71

---

<b>VPN Security Considerations Policy</b> .....	6A-72
<b>Wireless Network Security Policy</b> .....	6A-74

## VOLUME 2

### REGULATORY ISSUANCES INDEX

<b>FDIC Issuances</b> .....	Index-1
<b>OCC Issuances</b> .....	Index-4
<b>OTS Issuances</b> .....	Index-7
<b>NCUA Issuances</b> .....	Index-8
<b>FFIEC Issuances</b> .....	Index-10

## IT Examinations

### INTRODUCTION IT Handbook InfoBase

### CHAPTER 7 IT Audit Guidance

<b>Introduction</b> .....	7-1
<b>Audit Examination Procedures Checklist/Workprogram</b> .....	7-3
Tier I Objectives and Procedures .....	7-3
Conclusions.....	7-14
Tier II Objectives and Procedures .....	7-16
Management.....	7-16
Systems Development and Acquisition .....	7-17
Operations.....	7-19
Information Security.....	7-20
Payment Systems .....	7-22
Outsourcing .....	7-25
<b>Excerpts from the Audit Booklet</b> .....	7-27

### CHAPTER 8 Business Continuity Planning Guidance

<b>Introduction</b> .....	8-1
<b>Examination Procedures Checklist/Workprogram</b> .....	8-2
Examination Objective .....	8-2
Conclusions .....	8-18

### CHAPTER 8A Intrusion Response Procedures

<b>Meeting Regulatory Requirements</b> .....	8A-1
--	------

<b>Interagency Security Guidelines</b> .....	8A-2
<b>Risk Assessment and Controls</b> .....	8A-3
<b>Service Providers</b> .....	8A-3
<b>Response Program</b> .....	8A-3
Components of a Response Program.....	8A-4
<b>Customer Notification Requirements</b> .....	8A-4
When a Customer Notice Should Be Provided.....	8A-5
Customer Notice.....	8A-5
Standard for Providing Notice.....	8A-5
Sensitive Customer Information.....	8A-6
Affected Customers .....	8A-6
Content of Customer Notice.....	8A-6
Delivery of Customer Notices .....	8A-7
<b>Establishing an Intrusion Response Plan</b> .....	8A-7
United States Computer Emergency Readiness Team (US-CERT) Checklist .....	8A-8
Phase I: Detection, Assessment, and Triage .....	8A-8
Phase II: Containment, Evidence Collection, Analysis and Investigation, and Mitigation .....	8A-8
Phase III: Remediation, Recovery, and Post-Mortem .....	8A-9
<b>Intrusion Response Plan Requirements</b> .....	8A-9
Intrusion Categories.....	8A-10
Intrusion Response Team Members.....	8A-10
Roles of the Intrusion Response Team .....	8A-10
Intrusion Response Lifecycle .....	8A-11
Intrusion-Related Contacts .....	8A-11
Nonintrusion-Related Contacts .....	8A-12
Intrusion Response Organization Services.....	8A-12
<b>Monitoring Critical Systems</b> .....	8A-13
Notifying Your Intrusion Response Team.....	8A-14
Contacting Outside Resources .....	8A-14
<b>Web Site Spoofing Response Procedures</b> .....	8A-16
Identification .....	8A-16
Detection.....	8A-17
Information Gathering.....	8A-17
Disabling Spoofed Web Sites and Recovering Customer Information.....	8A-18
Legal Considerations.....	8A-18
Contact the Regulators and Law Enforcement Authorities .....	8A-19
<b>Practical Tips for Improved Intrusion Response</b> .....	8A-20
<b>Intrusion Response Procedures Manual</b> .....	8A-21
Appendix 8A.A: Sample Intrusion Response Procedures Manual.....	8A-22

## CHAPTER 9

### E-Banking Guidance

<b>Introduction</b> .....	9-1
<b>Examination Procedures Checklist/Workprogram</b> .....	9-3
Discussion Points for Examiners .....	9-4

General Procedures .....	9-5
Board and Management Oversight.....	9-8
Information Security Process.....	9-15
Legal and Compliance Issues.....	9-22
Examination Conclusions .....	9-25
E-Banking Request Letter Items.....	9-27
<b>Excerpts from the FFIEC E-Banking Booklet .....</b>	<b>9-33</b>

## CHAPTER 10

### FedLine Guidance

<b>Introduction .....</b>	<b>10-1</b>
<b>Examination Procedures Checklist/Workprogram.....</b>	<b>10-2</b>
Tier I Objectives and Procedures .....	10-2
Conclusions .....	10-7
<b>Excerpts from the FFIEC FedLine Booklet.....</b>	<b>10-9</b>

## CHAPTER 11

### Information Security Guidance

<b>FFIEC Information Security Booklet .....</b>	<b>11-1</b>
<b>Examination Procedures Checklist/Workprogram.....</b>	<b>11-4</b>
Examination Objective.....	11-4
Tier I Procedures.....	11-4
Quantity of Risk .....	11-6
Quality of Risk Management .....	11-7
Conclusions .....	11-15
Tier II Objectives and Procedures .....	11-17
Authentication and Access Controls.....	11-17
Authentication .....	11-20
Network Security .....	11-23
Host Security .....	11-28
User Equipment Security (e.g., Workstation, Laptop, Handheld).....	11-30
Physical Security .....	11-31
Personnel Security.....	11-31
Application Security.....	11-32
Software Development and Acquisition .....	11-33
Business Continuity — Security.....	11-35
Service Provider Oversight — Security.....	11-36
Encryption.....	11-37
Data Security .....	11-39
Security Monitoring.....	11-40
<b>Excerpts from the FFIEC Information Security Booklet.....</b>	<b>11-47</b>

## CHAPTER 12

## Supervision of Technology Service Providers Guidance

<b>Introduction</b> .....	12-1
<b>Examination Procedures Checklist/Workprogram</b> .....	12-3
Conclusions .....	12-4
<b>Excerpts from the FFIEC Supervision of Technology Service Providers</b> .....	12-5

## CHAPTER 13

## Retail Payment Systems Guidance

<b>Introduction</b> .....	13-1
<b>Examination Procedures Checklist/Workprogram</b> .....	13-2
Examination Objective.....	13-2
Tier I Objectives and Procedures.....	13-2
Conclusions .....	13-13
Tier II Objective and Procedures.....	13-14
A. EFT/POS and Bankcard Agreements and Contracts.....	13-14
B. Personal Identification Numbers (PINs) .....	13-15
C. Information Security .....	13-15
D. Card Issuance .....	13-17
E. Business Continuity Planning .....	13-18
F. EFT/POS and Bankcard Accounting and Transaction Processing.....	13-18
G. EFT/POS Operational Controls .....	13-19
H. ACH ODFI and RDFI Responsibilities .....	13-20
I. ACH Accounting and Transaction Processing.....	13-22
J. ACH Funding and Credit .....	13-23
K. Web and Telephone-Initiated ACH Transactions.....	13-24
L. ACH Contingency Plans .....	13-25
M. Check 21 .....	13-26
N. Remote Deposit Capture Risk Management .....	13-28
O. Vendor Management .....	13-35
Appendix 13.1: Regulation CC Requirements and Examination Procedures .....	13-38
Appendix 13.2: Excerpts From the February 2010 FFIEC Retail Payment Systems Booklet.....	13-79

## CHAPTER 14

## Development and Acquisition Guidance

<b>Introduction</b> .....	14-1
<b>Examination Procedures Checklist/Workprogram</b> .....	14-3
Examination Objective.....	14-3
Objectives and Procedures.....	14-3
Conclusions .....	14-18
<b>Excerpts from the FFIEC Development and Acquisition Booklet</b> .....	14-21

## CHAPTER 15 Management Guidance

<b>Introduction</b> .....	15-1
<b>Examination Procedures Checklist/Workprogram</b> .....	15-3
Examination Objective.....	15-3
<b>Excerpts from the Management Booklet</b> .....	15-17

## CHAPTER 16 Outsourcing Technology Services Guidance

<b>Introduction</b> .....	16-1
<b>Examination Procedures Checklist/Workprogram</b> .....	16-3
Examination Objective.....	16-3
Tier I Objectives and Procedures.....	16-3
Tier II Objectives and Procedures .....	16-8
<b>Excerpts from the FFIEC Outsourcing Technology Services Booklet</b> .....	16-15

## CHAPTER 17 Operations Guidance

<b>Introduction</b> .....	17-1
<b>Examination Procedures Checklist/Workprogram</b> .....	17-3
Examination Objective.....	17-3
Tier I Objectives and Procedures.....	17-3
Conclusions .....	17-15
Tier II Objectives and Procedures .....	17-16
<b>Excerpts from the FFIEC Operations Booklet</b> .....	17-31

## CHAPTER 18 Wholesale Payment Systems Guidance

<b>Introduction</b> .....	18-1
<b>Examination Procedures Checklist/Workprogram</b> .....	18-3
Examination Objective.....	18-3
Tier I Examination Objectives and Procedures.....	18-4
Conclusions .....	18-9
Tier II Examination Objectives and Procedures.....	18-10
<b>Excerpts from the FFIEC Wholesale Payment Systems Booklet</b> .....	18-29