

### **PART I: ASSESSING IT SECURITY RISKS**

---

- Chapter I-1**      Assessing IT Security Risks — A Regulatory Perspective
- Chapter I-2**      Conducting an IT Security Risk Assessment
- Chapter I-3**      Internet Banking Risk Assessment
- Chapter I-4**      Assessing Cloud Security
- Chapter I-5**      Snapshot Assessment
- Chapter I-6**      Assessing Privacy Policies

### **PART II      IMPLEMENTING IT SECURITY RISK SOLUTIONS**

---

- Chapter II-1**      Technology Risk Management in Financial Institutions: Getting Started
- Chapter II-2**      Internet Banking Risk Management
- Chapter II-3**      Desktop, Server, and Network Security
- Chapter II-4**      Physical Security Risk
- Chapter II-5**      Securing Mobile and Wireless Systems
- Chapter II-6**      Security of Customer Information
- Chapter II-7**      Securing Remote Deposit Capture
- Chapter II-8**      Public Website Security

### **PART III      MANAGING AND MONITORING IT SECURITY RISKS**

---

- Chapter III-1**      Information Security Metrics
- Chapter III-2**      IT Security Awareness Program
- Chapter III-3**      Mitigating Information Security Risk Through Insurance

- Chapter III-4** Computer Security Logs and Audit Trails
- Chapter III-5** Backup and Recovery Planning
- Chapter III-6** Creating a Disaster Recovery Plan
- Chapter III-7** Continuity Planning and the Systems Development Life Cycle
- Chapter III-8** Monitoring IT Security
- Chapter III-9** Security Policies
- Chapter III-10** Required Disclosures
- Chapter III-11** Complying with Customer Identification Requirements

**Part I — Assessing IT Security Risks**

CHAPTER I-1

Assessing IT Security Risks — A Regulatory Perspective

What Do the Regulators Say About Risk?.....I-1—1

Regulating Agencies .....I-1—2

    Federal Financial Institutions Examination Council (FFIEC) .....I-1—2

    Federal Deposit Insurance Corporation (FDIC) .....I-1—2

    National Credit Union Administration (NCUA) .....I-1—2

    National Automated Clearing House Association (NACHA) .....I-1—2

    Federal Reserve System .....I-1—2

    Office of the Comptroller of the Currency .....I-1—3

    Consumer Financial Protection Agency (CFPB) .....I-1—3

    Financial Services Oversight Council .....I-1—3

    Office of Thrift Supervision (OTS) .....I-1—3

Important Acts and Regulations .....I-1—3

    Dodd-Frank Act.....I-1—3

    Bank Secrecy Act.....I-1—4

    PATRIOT Act .....I-1—4

    The Financial Services Modernization Act of 1999.....I-1—4

Regulatory Requirements .....I-1—4

    Level I Service .....I-1—5

    Level II Service.....I-1—7

    Level III Service .....I-1—8

    Documentation Required by Examiners.....I-1—10

        Strategic Plan .....I-1—10

        Feasibility Studies .....I-1—10

Regulatory Risk assessments .....I-1—12

FDIC Issuances .....I-1—14

OCC Issuances.....I-1—19

OTS Issuances (OTS authority Transferred to OCC, July 21, 2011) .....I-1—21

NCUA Issuances .....I-1—22

CHAPTER I-2

Conducting an IT Security Risk Assessment

Risk Assessment Defined.....I-2—1

Risk Assessment Methods.....I-2—1

Major Points for IT Risk Assessments..... I-2—2

- Maintaining a Uniform Rating System for Information Technology..... I-2—2
- Emergency and Disaster Recovery Policies ..... I-2—3
  - Business Resumption Plans ..... I-2—3
  - Internet Banking System..... I-2—5

Performing the security Risk Assessment ..... I-2—6

- Identification ..... I-2—6
- Quantification or Measurement ..... I-2—8
- Prioritization ..... I-2—8
- Risk Categories ..... I-2—8

Performing the IT Risk Assessment ..... I-2—9

- Identification ..... I-2—9
- Quantification or Measurement ..... I-2—10
- Prioritization ..... I-2—10
- Exhibit I-2.1: Information Security Risk Assessment Worksheet ..... I-2—11
- Exhibit I-2.2: Information Technology Risk Assessment Worksheet ..... I-2—14

**CHAPTER I-3**  
**Internet Banking Risk Assessment**

Introduction..... I-3—1

Authentication ..... I-3—1

- Multi-Factor ..... I-3—2
- Out-of-Band Authentication ..... I-3—2
- Dual Customer Authorization ..... I-3—3
- Mutual Authentication..... I-3—3
- IP Based GeoLocation..... I-3—3
- Device Identification..... I-3—4
- Challenge Questions ..... I-3—4

Money Mules and Identify Theft ..... I-3—5

Client Device Health Requirements ..... I-3—5

Phishing Attacks..... I-3—6

SQL Injection Attacks..... I-3—7

Infrastructure ..... I-3—7

Mobile Banking Security ..... I-3—8

Anomalous/Fraud Detection ..... I-3—9

Customer Employee Fraud..... I-3—9

Password Management Tools..... I-3—10

Cash Management ..... I-3—10

Denial of Service ..... I-3—11

Customer Education ..... I-3—12

Web Page Redirection ..... I-3—12

- Detection ..... I-3—13
- Prevention..... I-3—13

## CHAPTER I-4

### Assessing Cloud Security

Introduction.....	I-4—1
Assessment Concerns in Multi-Tenant Environments.....	I-4—2
The Nature of the Beast.....	I-4—2
The Challenges Are Surmountable .....	I-4—2
Cloud Classification for Assessment .....	I-4—3
Software-as-a-Service (SaaS).....	I-4—3
Platform-as-a-Service (PaaS) and Infrastructure as a Service (IaaS):.....	I-4—3
Assessment Methodology .....	I-4—4
Supervision of Technology Service Providers .....	I-4—6
Accountability: The Management of Technology.....	I-4—6
Certifications .....	I-4—7
ISO 27001.....	I-4—7
SAS 70 Type II .....	I-4—7
PCI DSS Level 1 and Level 2.....	I-4—7
Contracts and Agreements .....	I-4—8
Service Level Agreements .....	I-4—8
Internal Controls, Insurance, and Disaster Recovery .....	I-4—9
Vendor’s Liability for Delays or Errors.....	I-4—9
Audits .....	I-4—9
Data Ownership and Access.....	I-4—9
Assignment .....	I-4—10
Evergreen Clauses .....	I-4—10
Non-Disclosure Agreements.....	I-4—10
Compliance .....	I-4—10
GLBA.....	I-4—10
HIPAA .....	I-4—10
FISMA .....	I-4—11
Transparency, Communications, and Disclosure Notifications .....	I-4—11
Change Management.....	I-4—12
e-Discovery and Law Enforcement.....	I-4—13
Terms of Use.....	I-4—13
Integrity of Data.....	I-4—13
Backup and Recovery Capability.....	I-4—13
Distributed Storage Systems.....	I-4—14
Retention Periods .....	I-4—14
Testing and Validation .....	I-4—14
Time to Recovery.....	I-4—15
Disk Only Systems .....	I-4—15
Local Storage or Other Data .....	I-4—15
ACID/Durability .....	I-4—16
Durability.....	I-4—16
Administrative Access to Data.....	I-4—17
Logging .....	I-4—17

Portability .....	I-4—18
Confidentiality of Data .....	I-4—19
Identity and Access Management .....	I-4—20
Single Sign On (SSO) Services.....	I-4—20
Multi-Factor Authentication .....	I-4—21
Out-of-Band Authentication.....	I-4—21
Dual Customer Authorization.....	I-4—21
Mutual Authentication .....	I-4—22
IP Based GeoLocation .....	I-4—22
Client Device Health Requirements.....	I-4—22
Device Identification.....	I-4—23
Challenge Questions.....	I-4—23
Encryption.....	I-4—23
Isolation.....	I-4—24
Hypervisor.....	I-4—24
Storage.....	I-4—24
Data Deletion .....	I-4—25
Network Firewalls .....	I-4—25
Packet Filtering.....	I-4—26
Penetration Testing.....	I-4—26
VLANs .....	I-4—26
Co-Residence Checks.....	I-4—27
Side-Channel Attacks.....	I-4—27
Isolation Concerns with IaaS.....	I-4—28
Isolation Concerns with PaaS.....	I-4—28
Isolation Concerns with SaaS .....	I-4—28
Physical Security .....	I-4—29
Availability of Services.....	I-4—29
Increased Rewards for Attackers .....	I-4—29
DDoS .....	I-4—30
Transparency as a Pejorative .....	I-4—30
Homogeneous Environments.....	I-4—31
Third Party Control .....	I-4—31
Scalability .....	I-4—31
Financial Stability.....	I-4—32
Privacy Concerns .....	I-4—32
Profitability.....	I-4—32
Resources .....	I-4—32
Guidance .....	I-4—33
Insurance .....	I-4—33
Credit References .....	I-4—33
Exhibit I-4.1: Determining Cloud Services Minimum Security Requirements .....	I-4—34
Exhibit I-4.2: Supplement to Authentication in an Internet Banking Environment .....	I-4—40

## CHAPTER I-5 Snapshot Assessment

Introduction to Snapshot Self-Assessment .....	I-5—1
Management Reporting on Security Risk .....	I-5—1
Physical Security and Controls .....	I-5—3
Desktop Security and Controls.....	I-5—3
Network Administration .....	I-5—4
General .....	I-5—4
User Management.....	I-5—5
Network Security .....	I-5—5
Remote Access .....	I-5—6
Internet Access .....	I-5—6
Wireless Security.....	I-5—6
Email Security and Controls.....	I-5—6
Internet Banking Security and Controls .....	I-5—7
Business Resumption Planning.....	I-5—8
Electronic Funds Transfer (EFT) Activity .....	I-5—9
Wire Transfer Operations.....	I-5—9
Automated Teller Machine (ATM) Processing.....	I-5—9
Self-Audit Network Security Review Work Programs .....	I-5—10
Network Administration .....	I-5—10

## CHAPTER I-6 Assessing Privacy Policies

Coverage .....	I-6—2
Timing of Initial Disclosure .....	I-6—2
Timing of Annual Disclosure .....	I-6—3
Contents of Standard Disclosure .....	I-6—3
A Note Regarding “Opt-Outs”.....	I-6—4
Contents of Simplified Disclosure .....	I-6—5
Short-Form Disclosure for Consumers That Are Not Customers.....	I-6—5
“Clear and Conspicuous” .....	I-6—6
Changing the Terms of the Privacy Policy .....	I-6—7
Form and Content of Opt-Out Notice to Consumers .....	I-6—7
Compliance with “Opt-Out” Election .....	I-6—9
Continuing Right to Opt Out .....	I-6—9
Duration of Consumer’s Opt-Out Election.....	I-6—9
Disclosure of Information to Nonaffiliated Third Parties.....	I-6—9
Exceptions to “Opt Out”.....	I-6—10
Exception for Service Providers and Joint Marketing.....	I-6—10
Exceptions for Processing and Servicing Transactions .....	I-6—11
“Other” Exceptions to Notice and Opt-Out Requirements .....	I-6—12
Exhibit I-6.1: Privacy Rule Checklist.....	I-6—15
Exhibit I-6.2: Privacy Model Form with Opt-Out.....	I-6—18

Exhibit I-6.3: Privacy Model Form with No Opt-Out.....	I-6—20
--	--------

## Part II — Implementing Security Risk Solutions

### CHAPTER II-1

#### Technology Risk Management in Financial Institutions: Getting Started

Overview of Technology Risk Management.....	II-1—1
Build a Security Team.....	II-1—1
Information Technology Steering Committee .....	II-1—1
IT Leadership.....	II-1—2
Network Administration .....	II-1—3
Support and Maintenance.....	II-1—3
Internal Training .....	II-1—4
Audit Department.....	II-1—4
Customer Education .....	II-1—4
Perform a Technology Risk Assessment .....	II-1—4
Identify Risks .....	II-1—5
Audit Systems .....	II-1—5
Gap Analysis .....	II-1—5
Report.....	II-1—5
Repeat.....	II-1—5
Mitigate Security Risks.....	II-1—6
Policies and Procedures .....	II-1—6
Technical Controls .....	II-1—6
End User Training.....	II-1—6
Customer Education Programs.....	II-1—6
Conduct Ongoing Monitoring and Examinations.....	II-1—7
Management Reviews.....	II-1—7
Compliance Reviews .....	II-1—7
Risk-Based Internal Audits.....	II-1—7
External Audits .....	II-1—7
Third-Party Certificates, Audits, and Reviews.....	II-1—8
Information Systems (IS) Reviews.....	II-1—8
Network Audits.....	II-1—8
Legal Opinions and Reviews .....	II-1—8

### CHAPTER II-2

#### Internet Banking Risk Management

Common Problems with Offering Internet Services .....	II-2—1
Deficiencies in Strategic Planning .....	II-2—1
Lack of Policies or Procedures .....	II-2—2
Insufficient Audit Coverage of Online Banking Activities.....	II-2—2

Lack of Evaluation of Written Contracts with Third-Party Providers .....	II-2—2
Incomplete Adoption of Regulator’s Risk Recommendations .....	II-2—2
Overreliance on Vendors .....	II-2—3
Weak System Access Controls .....	II-2—3
Lack of Adequate Security.....	II-2—3
Compliance Basics .....	II-2—3
Active Board and Senior Management Oversight .....	II-2—3
Risk Assessments.....	II-2—3
Written Policies and Procedures .....	II-2—4
Internal Controls .....	II-2—4
Independent Testing of Systems .....	II-2—4
Compliance with All Regulations.....	II-2—4
Contingency Plans .....	II-2—4
Web Site Security.....	II-2—5
Review of Regulator Bulletins Addressing Information Systems and E-Banking Issues .....	II-2—5
Key Questions Concerning Internet Service Operations.....	II-2—5
How Are Products Delivered Electronically?.....	II-2—5
What Products Are Offered? .....	II-2—7
What Type of Disclosures Have Been Provided?.....	II-2—7
Will the Customers Be Able to Open Accounts or Obtain Loans Online?.....	II-2—8
Opening a Deposit Account .....	II-2—8
Obtaining a Loan .....	II-2—9
What Is the Institution’s Privacy Policy? .....	II-2—10
What Is the Process for Updating Rates and Terms? .....	II-2—11
What to Do with the Customer Information Collected.....	II-2—11
Examination Categories by Level of Service Provided .....	II-2—12
Level I Service.....	II-2—12
Level II Service.....	II-2—14
Level III Service .....	II-2—16
What the Examiners Will Review.....	II-2—17
Strategic Plan .....	II-2—17
Feasibility Studies.....	II-2—17
System Designs and Their Relationship to the Institution’s Operating Systems.....	II-2—19
Issues to Consider in the Internet Banking Vendor’s Contract.....	II-2—20
Security Policy.....	II-2—22
Emergency and Disaster Recovery Policies .....	II-2—22
Business Resumption Plans .....	II-2—23
Internet Banking System.....	II-2—25
Network Servers That Serve Internet Banking Systems and Other Internet Services.....	II-2—26
Web Site Host.....	II-2—26
Internet Service Provider (ISP).....	II-2—26
Telecommunications Provider .....	II-2—27
Results of Disaster Recovery Tests .....	II-2—27
Schedule of Internal Audit and Frequency.....	II-2—27
User Guides and Agreements .....	II-2—28
Internet Banking Procedures — Consumer.....	II-2—28

ABC Finance Internet Banking Procedures — Business .....	II-2—30
Copies of Agreements and Contracts.....	II-2—32
Outsourcing Details.....	II-2—32
Disclosures Given to Customers.....	II-2—32
Online Applications and Advertisements.....	II-2—33
Customer and User Agreements .....	II-2—33
Privacy Policy.....	II-2—33
Vendor Agreements.....	II-2—33
Third-Party Certificates, Audits, and Reviews.....	II-2—33
Operating Policies and Procedures .....	II-2—33
Compliance Program .....	II-2—34
Legal Opinions and Reviews .....	II-2—34
Risk Assessments.....	II-2—34
Internal and External Audits .....	II-2—34
Network Audit Report .....	II-2—34
Information Systems (IS) Reviews.....	II-2—34
Summary of Internet Banking Risks.....	II-2—35
Exhibit II-2.1: Sample Technology Plan .....	II-2—37
Exhibit II-2.2: Network Audit Checklist.....	II-2—42
Exhibit II-2.3: Sample Privacy Policies.....	II-2—43
Exhibit II-2.4: Excerpts from Risk Management Section of ABC Finance’s Strategic Plan .....	II-2—58
Exhibit II-2.5: ABC Finance — Internal Audit Schedule .....	II-2—65
Exhibit II-2.6: Enrollment Form.....	II-2—66
Exhibit II-2.7: Privacy of Consumer Financial Information .....	II-2—67

## CHAPTER II-3

### Desktop, Server, and Network Security

Desktop and Workstation Security .....	II-3—1
Update Your PC.....	II-3—2
Turn on the Phishing Filter.....	II-3—2
Keep your Network Clean with Network Access Protection (NAP).....	II-3—2
Check Your Update History .....	II-3—2
Use the Network Profiles .....	II-3—2
Use a 64-bit Operating System.....	II-3—2
Get to Know Windows Firewall .....	II-3—3
Password Management.....	II-3—3
Self Service.....	II-3—3
Single Sign On (SSO) Solutions .....	II-3—4
Encrypted Password Databases.....	II-3—4
Securing Customer Data on PCs.....	II-3—4
Full Disk Encryption .....	II-3—5
Restricting Local Software Installation .....	II-3—5
Employee Monitoring.....	II-3—5
Employee Monitoring Software .....	II-3—6
Application Firewalls.....	II-3—6

Email .....	II-3—6
Email Security .....	II-3—7
Protecting PCs While Users Are Away from Their Desks.....	II-3—7
Secure Network Administration .....	II-3—7
Intrusion Detection Systems (IDS) .....	II-3—8
Host-Based IDS.....	II-3—9
Network-Based IDS.....	II-3—9
Attack Signatures: Haven't I Seen You Somewhere Before?.....	II-3—9
Intrusion Response Policy: Someone's Knocking on the Door.....	II-3—9
A Trap: Like Flies to Honey .....	II-3—10
Before IDS: You Don't Know What You Don't Know .....	II-3—10
Logical Access Controls.....	II-3—10
Tokens .....	II-3—11
Smart Cards .....	II-3—11
Biometrics .....	II-3—11
Encryption, Digital Signatures, and Certificate Authorities .....	II-3—11
Encryption .....	II-3—12
System Architecture and Design .....	II-3—13
Virtualization.....	II-3—14
Benefits of Virtualization Software.....	II-3—14
Concerns Before Implementation .....	II-3—15
Virtualization in Financial Institutions.....	II-3—15
Challenges Put into Practice.....	II-3—16
Storage Solutions .....	II-3—17
EFT Switches and Network Services .....	II-3—17
Document Imaging Systems.....	II-3—18
Taking Advantage of Windows Security Features.....	II-3—19
Microsoft's Recent Security Enhancements .....	II-3—19
Active Directory.....	II-3—19
Authentication Security .....	II-3—22

## CHAPTER II-4

### Physical Security

Definitions and Examples.....	II-4—1
Major Hazards .....	II-4—3
Fire .....	II-4—3
Flooding .....	II-4—3
Riot, Sabotage and Cyber-Terrorism .....	II-4—4
Fraud or Theft.....	II-4—5
Power Failure .....	II-4—5
Equipment Failure .....	II-4—5
Housekeeping Rules.....	II-4—5

## CHAPTER II-5

### Securing Mobile and Wireless Systems

Planning for Wireless Technologies.....	II-5—1
Networks .....	II-5—1
Wireless Security Concerns .....	II-5—2
Threats and Vulnerabilities.....	II-5—2
Mobile vs. Desktop .....	II-5—3
Security Requirements and Threats .....	II-5—4
Loss of Confidentiality.....	II-5—4
Risk Mitigation.....	II-5—4
Management Countermeasures.....	II-5—5
Operational Countermeasures.....	II-5—5
Technical Countermeasures.....	II-5—6
Authentication.....	II-5—6
Encryption.....	II-5—6
Antivirus Software .....	II-5—7
PKI.....	II-5—7
VPN and Firewalls.....	II-5—7
Enterprise Solutions.....	II-5—7
Wireless Security Auditing.....	II-5—8
Benefits of a Wireless Security Audit .....	II-5—8
Threats Identified by a Wireless Security Audit.....	II-5—8
Wireless Security Audit Work Plan.....	II-5—9
Local Area Networks .....	II-5—9
Security.....	II-5—9
Ad Hoc Networks — Bluetooth.....	II-5—10
Security.....	II-5—10
Security Requirements and Threats .....	II-5—11
Loss of Confidentiality.....	II-5—11
Risk Mitigation.....	II-5—12
Management Countermeasures.....	II-5—12
Operational Countermeasures.....	II-5—12
Software Countermeasures.....	II-5—12
Security Requirements and Threats .....	II-5—13
Loss of Confidentiality.....	II-5—13
Loss of Integrity.....	II-5—14
Loss of Network Availability .....	II-5—14
Other Security Risks .....	II-5—15
Risk Mitigation.....	II-5—15
Management Countermeasures.....	II-5—15
Operational Countermeasures.....	II-5—16
Technical Countermeasures .....	II-5—17
Point-to-Point Wireless .....	II-5—17
Security Issues Becoming Clearer Through Security Audits .....	II-5—18
Wireless Network Design Considerations.....	II-5—18

Regulators Weigh in on Wireless .....	II-5—19
Summary .....	II-5—19
Exhibit II-5.1: Technology Planning Survey .....	II-5—20
Exhibit II-5.2: Wireless Security Audit Work Plan .....	II-5—26

## CHAPTER II-6

### Security of Customer Information

Definitions .....	II-6—1
Standards for Safeguarding Customer Information .....	II-6—1
Information Security Program .....	II-6—1
Objectives .....	II-6—1
Development and Implementation of Information Security Program .....	II-6—2
Involve the Board of Directors .....	II-6—2
Assess Risk .....	II-6—2
Manage and Control Risk .....	II-6—2
Oversee Service Provider Arrangements .....	II-6—3
Adjust the Program .....	II-6—3
Report to the Board .....	II-6—3
Customer Response Program for Unauthorized Access to Customer Information .....	II-6—4
Components of a Response Program .....	II-6—4
Sensitive Customer Information .....	II-6—5
When Customer Notice Should Be Provided .....	II-6—5
Customer Notice .....	II-6—5
Delivery of Customer Notice .....	II-6—5
Exhibit II-6.1: Customer Response Program Checklist .....	II-6—6

## CHAPTER II-7

### Securing Remote Deposit Capture

What Is Remote Deposit Capture? .....	II-7—1
Check 21 .....	II-7—2
Substitute Checks .....	II-7—2
Warranties and Indemnity .....	II-7—3
Transportation of Checks .....	II-7—3
Industry Standards .....	II-7—3
Notice Requirements .....	II-7—4
Expedited Recrediting .....	II-7—4
New Opportunities and Benefits Under Check 21 .....	II-7—4
ACH Rules .....	II-7—5
Changes in ACH Rules .....	II-7—6
Corporate ACH Transactions .....	II-7—7
POP — Point-of-Purchase Entries .....	II-7—7
TEL — Telephone-Initiated Entry .....	II-7—8
WEB — Internet-Initiated Entry .....	II-7—8
PPD — Prearranged Payment and Deposit Entry .....	II-7—8

RCK — Re-Presented Check Entry .....	II-7—8
BOC — Back-Office Conversion .....	II-7—8
The Future of ACH.....	II-7—9
Corporate Check Identification .....	II-7—9
Back-Office Conversion.....	II-7—10
Feasibility.....	II-7—10
System Design and Financial Institution Operating Systems.....	II-7—12
Opportunities .....	II-7—12
Risk Factors.....	II-7—13
Vendor and System Risk .....	II-7—14
Vendor Selection.....	II-7—14
System Feature Function.....	II-7—14
Reporting .....	II-7—15
Research Capabilities .....	II-7—16
Vendor Compliance Risk.....	II-7—17
Vendor Management .....	II-7—17
Compliance Risk.....	II-7—17
Compliance with NACHA .....	II-7—18
Compliance with Check 21 .....	II-7—19
Compliance Monitoring.....	II-7—20
Item Processing Risk .....	II-7—21
Item Proof .....	II-7—23
Client Underwriting Risk.....	II-7—24
Nature of Industry and Type of Business.....	II-7—25
Reputation of Business.....	II-7—26
Industry Stability .....	II-7—26
Business Stability and Financial Strength .....	II-7—26
Business Ownership, Management, and Staff.....	II-7—28
Accounting Procedures .....	II-7—28
Internal Procedures.....	II-7—29
Deposit Analysis .....	II-7—29
Average Collected Balance .....	II-7—29
Remote Capture Solutions .....	II-7—29
System Solutions .....	II-7—30
Browser-Based Software .....	II-7—30
Front and Back Check Image Capture .....	II-7—31
Hardware Speed Options .....	II-7—31
Report Capabilities .....	II-7—31
Electronic Receipts.....	II-7—32
Check Frank/Endorsement .....	II-7—33
Duplicate Item Recognition .....	II-7—33
Check Writer Data Recognition.....	II-7—33
Negative Database.....	II-7—34
Credit Card Processing.....	II-7—34
MICR Repair.....	II-7—34
System Security.....	II-7—35

Scanning Methods .....	II-7—36
Feed-and-Key .....	II-7—36
Batch .....	II-7—37
CAR/LAR.....	II-7—37
Back Office Proof.....	II-7—38
Client Coupon Recognition.....	II-7—38
ACH vs. Check 21 Processing.....	II-7—39
Business Resumption and Contingency Planning.....	II-7—39
General Guidelines for Developing a Contingency Plan.....	II-7—40
Remote Deposit Capture Contingency Planning Process .....	II-7—42
Risk Analysis.....	II-7—44
Contingency Planning for Vendors .....	II-7—45
System Providers.....	II-7—46
Third-Party Item Processors .....	II-7—47
Financial Institution .....	II-7—49
Remote Deposit Capture Business Clients .....	II-7—50
Exhibit II-7.1: Remote Deposit Product Risk Register .....	II-7—52
Exhibit II-7.2: Sample Commercial Client Remote Deposit Risk Assessment .....	II-7—53
Exhibit II-7.3: Sample Commercial Client Risk Profile.....	II-7—57
Exhibit II-7.4: Remote Deposit Underwriting Checklist .....	II-7—58

## CHAPTER II-8

### Public Website Security

Website Security in the Public Sphere — Weblinking Relationships.....	II-8—1
Authority .....	II-8—1
Risks Involved.....	II-8—2
Reputation Risk .....	II-8—2
Transaction Risk .....	II-8—3
Compliance Risk.....	II-8—3
Strategic Risk .....	II-8—3
Addressing the Risks Involved .....	II-8—4

## Part III — Monitoring and Managing IT Security Risks

### CHAPTER III-1

#### Information Security Metrics

Overview.....	III-1—1
Introduction .....	III-1—1
Purpose .....	III-1—1
Security Metrics .....	III-1—2
Components of Security Metrics.....	III-1—3
Roles and Responsibilities .....	III-1—3

Board of Directors/Trustees.....	III-1—3
Executive Management .....	III-1—5
Chief Information Officer .....	III-1—5
Information Security Officer .....	III-1—6
Information System Owner .....	III-1—6
Information System Security Officer .....	III-1—7
Other Related Roles .....	III-1—7
Information Security Metrics Background .....	III-1—7
Definition .....	III-1—7
Benefits of Using Metrics .....	III-1—8
Increase Accountability .....	III-1—8
Improve Information Security Effectiveness .....	III-1—9
Demonstrate Compliance .....	III-1—9
Provide Quantifiable Inputs for Resource Allocation Decisions.....	III-1—9
Types of Measurements .....	III-1—9
Implementation Metrics .....	III-1—10
Effectiveness/Efficiency Metrics .....	III-1—11
Impact Metrics .....	III-1—11
Measurement Considerations .....	III-1—12
Organizational Considerations .....	III-1—12
Manageability .....	III-1—12
Data Management Concerns .....	III-1—12
Automation of Measurement Data Collection .....	III-1—13
Measurements in the Risk Management .....	III-1—13
Information Security Measurement Program Scope .....	III-1—13
Individual Information Systems .....	III-1—14
System Development Life Cycle .....	III-1—14
Bankwide Programs .....	III-1—14
Enterprise Strategic Planning and Information Security .....	III-1—15
Metrics Development Process .....	III-1—15
Phase 1: Stakeholder Interest Identification .....	III-1—16
Phase 2: Goals and Objectives Definition .....	III-1—17
Phase 3: Information Security Policies, Guidelines, and Procedures Review .....	III-1—17
Phase 4: Information Security Program Implementation Review .....	III-1—18
Phase 5: Metrics Development and Selection .....	III-1—18
Metrics Development Approach .....	III-1—19
Metrics Prioritization and Selection .....	III-1—19
Establishing Performance Targets .....	III-1—20
Metrics Development Template .....	III-1—20
Feedback Within the Metrics Development Process .....	III-1—20
Information Security Measurement Implementation .....	III-1—21
Phase 1: Prepare for Data Collection .....	III-1—21
Phase 2: Collect Data and Analyze Results .....	III-1—22
Phase 3: Identify Corrective Actions .....	III-1—23
Phase 4: Develop Business Case and Phase 5: Obtain Resources .....	III-1—24
Phase 6: Apply Corrective Actions .....	III-1—25

Metrics for Board of Directors/Trustees .....	III-1—25
Metrics for Management .....	III-1—26
Technical Metrics .....	III-1—27
Exhibit III-1.1: Sample SDLC Metrics.....	III-1—28
Exhibit III-1.2: Metrics Template and Instructions.....	III-1—30
Exhibit III-1.3: Metrics for Board of Directors/Trustees.....	III-1—32
Exhibit III-1.4: Metrics for Management .....	III-1—35
Exhibit III-1.5: Technical Metrics .....	III-1—40

## CHAPTER III-2

### IT Security Awareness Program

Technology's Value to the Institution.....	III-2—1
Real Threats in a Real World .....	III-2—2
Security Risks Take Various Forms: .....	III-2—2
Common Security Lapses.....	III-2—2
Mistakes Made by Users.....	III-2—2
Mistakes Made by Senior Executives.....	III-2—3
Mistakes Made by IT Departments .....	III-2—3
Security Responsibilities .....	III-2—3
Management's Responsibilities .....	III-2—3
User's Responsibilities .....	III-2—4
Security Initiatives.....	III-2—5
Security Guidelines .....	III-2—5
Information Security for Everyone .....	III-2—5
Information Security for Computer End Users.....	III-2—6
Information Security for Senior Executives.....	III-2—6
Information Security for IT Departments .....	III-2—7
Sample Security Policies .....	III-2—8
Email Usage.....	III-2—8
Internet Use .....	III-2—9
Communications Devices .....	III-2—10
Remote Access .....	III-2—10
Wireless Devices.....	III-2—10
Internet Users' Concerns .....	III-2—11

## CHAPTER III-3

### Mitigating Information Security Risk Through Insurance

Eight Cyber Risk Areas.....	III-3—1
Internal Criminal Acts .....	III-3—1
Hacker Attacks.....	III-3—2
Viruses.....	III-3—2
Crisis Management .....	III-3—2
Privacy Violations .....	III-3—3
Media Liability.....	III-3—3

Cyber Extortion .....	III-3—4
Global Risks.....	III-3—4
Risk Examples .....	III-3—4
Hacker Attacks.....	III-3—4
Online Banking Risks .....	III-3—5
Traditional Insurance Coverage .....	III-3—6
Commercial General Liability (CGL) .....	III-3—6
Professional Liability .....	III-3—6
Business Personal Property (BPP) .....	III-3—7
Electronic Data Processing (EDP) .....	III-3—7
New Insurance Policies for Computer Security.....	III-3—7
Examples of Cyber Insurance Policies for Financial Institutions.....	III-3—9
Internet Banking Liability Policy.....	III-3—9
Enhanced Financial Institution Bond.....	III-3—9
Business Interruption Endorsement .....	III-3—10
Public Relations Expense Endorsement .....	III-3—10
Cyber/Network Extortion Coverage Endorsement .....	III-3—10

## CHAPTER III-4

### Computer Security Logs and Audit Trails

Overview.....	III-4—1
Introduction .....	III-4—1
Definitions.....	III-4—1
Logs.....	III-4—1
Audit Trails .....	III-4—2
Background.....	III-4—3
Policies and Procedures .....	III-4—3
Prioritizing Log Management.....	III-4—4
Log Management Infrastructure.....	III-4—4
Log Management Responsibilities .....	III-4—4
Standard Log Management Processes .....	III-4—4
The Basics of Computer Security Logs and Audit Trails.....	III-4—5
Types of Security Logs and Audit Trails.....	III-4—5
Security Software .....	III-4—5
Operating Systems .....	III-4—6
Applications.....	III-4—7
Usefulness of Logs and Audit Trails .....	III-4—7
Benefits of Log Management .....	III-4—7
The Challenges in Log Management .....	III-4—8
Log Generation and Storage .....	III-4—8
Log Protection .....	III-4—9
Log Analysis .....	III-4—10
Overcoming the Challenges .....	III-4—10
Log Management Infrastructure .....	III-4—11
Architecture .....	III-4—11

Functions .....	III-4—12
Syslog-Based Centralized Logging Software .....	III-4—14
Syslog Format .....	III-4—14
Syslog Security .....	III-4—15
Security Event Management Software .....	III-4—17
Additional Types of Log Management Software .....	III-4—18
Organization-Level Log Management Processes .....	III-4—19
Define Roles and Responsibilities .....	III-4—19
Establish Logging Policies .....	III-4—20
Ensure that Policies Are Feasible .....	III-4—21
Divide Responsibilities Between System Level and Organization Level .....	III-4—23
Analyze Log Data .....	III-4—25
Perform Testing and Validation .....	III-4—27
System-Level Log Management Processes .....	III-4—28
Configure Log Sources .....	III-4—28
Log Generation .....	III-4—29
Log Storage and Disposal .....	III-4—29
Log Security .....	III-4—31
Support Logging Operations .....	III-4—32
Analyze Log Data .....	III-4—32
Respond to Identified Events .....	III-4—33
Manage Long-Term Log Data Storage .....	III-4—34
Exhibit III-4.1: Glossary of Security Log and Audit Trail Terms .....	III-4—35
Exhibit III-4.2: Security Log and Audit Trail Acronyms .....	III-4—37

## CHAPTER III-5

### Backup and Recovery Planning

Identifying Critical Data for Backup .....	III-5—2
Selecting a Retention Policy .....	III-5—2
Three Types of Backup: Full Backup, Differential Backup, and Incremental Backup .....	III-5—3
Full Backup .....	III-5—3
Differential and Incremental Backups .....	III-5—3
Routine vs. Non-Routine Backups .....	III-5—4
Tape Rotation/Replacement Strategy .....	III-5—4
Keeping Backups Secure .....	III-5—5
Mainframe Backups .....	III-5—5
Local Backup .....	III-5—5
Other Backups .....	III-5—6
Safe Deposit Box .....	III-5—6
Media Storage Service Providers .....	III-5—6
Online Backup Services .....	III-5—6
Site to Site Replication .....	III-5—6
Implementing Your Backup Plan .....	III-5—6
Testing Your Backup and Recovery Strategy .....	III-5—7
Train Employees on Backup and Disaster Recovery .....	III-5—9

Backup Logs.....	III-5—10
Exhibit III-5.1: Backup Log.....	III-5—11

## CHAPTER III-6

### Creating a Disaster Recovery Plan

Writing Effective Disaster Recovery Procedures .....	III-6—2
Maintaining Work Force Continuity.....	III-6—2
Following 12 Critical Steps to Disaster Recovery.....	III-6—4
Managing Remote Data .....	III-6—5
Disk-to-Disk Backup .....	III-6—7
FFIEC Business Continuity Requirements.....	III-6—7
Backup and Contingency Planning .....	III-6—8
Microcomputers .....	III-6—8
Backup Procedures for Physical Disasters and Other Disruptions.....	III-6—10
Risk Assessment of Potential Hazards.....	III-6—11
Protection of Information Systems .....	III-6—12
Computer Networks.....	III-6—13
Technology Risk and Contingency Planning.....	III-6—14
Technological Emergencies.....	III-6—14
Hardware Backup .....	III-6—15
Program and Software Backup .....	III-6—17
Data File Backup.....	III-6—19
Telecommunications Backup.....	III-6—19
Communications Disruptions .....	III-6—20
Communications Backup Systems and Planning.....	III-6—21
Information Systems Contingency Planning.....	III-6—21
Contingency Planning Coordinator .....	III-6—22
Backup Operations .....	III-6—22
Data File Backup .....	III-6—23

## CHAPTER III-07

### Continuity Planning and the Systems Development Life Cycle

Planning Phase.....	III-7—2
The Conceptual Design.....	III-7—2
Performing a Detailed Analysis.....	III-7—3
Development Phase.....	III-7—10
Implementation Phase.....	III-7—14
Operation/System Support Phase .....	III-7—16
Decommission Phase.....	III-7—17

## CHAPTER III-8 Monitoring IT Security

Introduction.....	III-8—1
Monitoring and Managing IT Security.....	III-8—2
Prevention vs. Response .....	III-8—2
Detecting Attacks.....	III-8—3
Responding to Incidents .....	III-8—3
Response Procedures for IDS Identified Attacks.....	III-8—3
Monitoring.....	III-8—3
Incident Handling .....	III-8—4
Forensic Analysis and Data Retention .....	III-8—4
Response and Reporting .....	III-8—5
Monitoring and Managing System Backup and Disaster Recovery .....	III-8—7
Backup Logs .....	III-8—8
Exhibit III-8.1: Sample Contact List for Hardware Vendors.....	III-8—9

## CHAPTER III-9 Security Policies

Policy Contents.....	III-9—1
Exhibit III-9.1: Intranet/Internet Acceptable Use Sample Policy .....	III-9—4
Exhibit III-9.2: Sample Personal Computer/Network Systems Policy.....	III-9—7
Exhibit III-9.3: Sample Information Systems Security Policy .....	III-9—22
Exhibit III-9.4: Sample Internet Banking Policy.....	III-9—52
Appendix III-9.1: ABC Finance Business Internet Banking Application.....	III-9—61
Appendix III-9.2: ABC Finance ACH Agreement.....	III-9—64
Appendix III-9.3: ACH Agreement.....	III-9—73
Appendix III-9.4: ACH Agreement Operational/Security Procedures.....	III-9—75
Appendix III-9.5: Resolution Authorizing ACH Agreement.....	III-9—77
Appendix III-9.6: Cash Management Services Agreement.....	III-9—78
Appendix III-9.7: Risk Assessment Matrix .....	III-9—91
Exhibit III-9.5: Sample Information Security, PC/Network, and Intranet/Internet/ Extranet Policies .....	III-9—92
Exhibit III-9.6: Emergency and Disaster Recovery Policy.....	III-9—116
Exhibit III-9.7: Change Management and Control Policy.....	III-9—123
Appendix III-9.8: Change Authorization Form .....	III-9—127

## CHAPTER III-10 Required Disclosures

E-Sign Act Compliance.....	III-10—1
Consent to Receive Electronic Disclosures.....	III-10—1
Contents of Consent Disclosure.....	III-10—1
Additional Requirements for Disclosures Provided Under Regulations B, E, Z, and DD.....	III-10—2

Additional Requirements for Electronic Disclosures Under Regulations B, E, Z, and DD .....	III-10—2
Regulation B Application Disclosures.....	III-10—3
Regulation Z Disclosures .....	III-10—3
Open-End Credit .....	III-10—3
Closed-End Credit.....	III-10—4
Regulation DD Disclosures.....	III-10—4
Change in Hardware/Software Requirements .....	III-10—5
Exceptions to Preemption.....	III-10—5

## CHAPTER III-11

### Complying with Customer Identification Requirements

Introduction.....	III-11—1
Anti-Money Laundering Record Considered in Applications .....	III-11—1
BSA Compliance Programs .....	III-11—1
Internal Controls .....	III-11—2
Independent Testing of Compliance.....	III-11—3
Compliance Officer.....	III-11—5
Training.....	III-11—5
Consolidated BSA/AML Compliance Programs .....	III-11—6
Overview .....	III-11—6
Holding Company or Lead Financial Institution .....	III-11—7
Common Problems in BSA Programs.....	III-11—8
BSA/Anti-Money Laundering Enforcement by the Regulatory Agencies .....	III-11—8
The Legal Background.....	III-11—9
Methods the Agencies Use to Communicate Their Concerns About an Institution's BSA Compliance Program .....	III-11—9
Enforcement Actions for BSA Compliance Program Failures .....	III-11—10
Failure to Establish and Maintain a Reasonably Designed BSA Compliance Program .....	III-11—10
Failure to Correct a Previously Reported Problem with the BSA Compliance Program .....	III-11—11
Other Enforcement Actions for BSA Compliance Program Deficiencies .....	III-11—12
Enforcement for Violations of the BSA Reporting and Recordkeeping Requirements .....	III-11—12
Suspicious Activity Reporting Requirements.....	III-11—12
Anti-Money Laundering Program Requirements.....	III-11—13
Customer Identification Program Rule and Address Confidentiality Programs .....	III-11—14
Customer Identification Program Requirements.....	III-11—14
Institutions Subject to the CIP Rule.....	III-11—15
Holding Companies and Subsidiaries.....	III-11—16
Bank Subsidiaries .....	III-11—16
CIP Requirements.....	III-11—17
Accounts Subject to CIP Requirements.....	III-11—18
Exemptions.....	III-11—18
Data Processing, Data Warehousing, and Data Transmission .....	III-11—19

Customers Subject to CIP Requirements .....	III-11—19
Additional or Substitute Accountholders.....	III-11—20
Accounts with Power-of-Attorney .....	III-11—20
Signatories .....	III-11—20
Accounts Held by Minors.....	III-11—21
Trust Accounts and Escrow Accounts.....	III-11—21
Pension Plan Administrators .....	III-11—22
Agent Banks for Credit Card Issuers .....	III-11—22
Administrators of Non-ERISA Accounts.....	III-11—22
Banks Acting as Transfer Agent .....	III-11—23
Exemptions.....	III-11—23
Required Contents for Customer Identification Program .....	III-11—24
Reliance on Third Parties .....	III-11—25
Identity Information Collection and Verification .....	III-11—26
Required Customer Information To Be Collected .....	III-11—26
Customer Verification .....	III-11—28
Additional Procedures for Certain Signatories.....	III-11—30
Lack of Verification.....	III-11—31
Recordkeeping.....	III-11—31
Sales of Loans While Retaining the Servicing Rights.....	III-11—32
Comparison with Government Lists .....	III-11—33
Customer Notice.....	III-11—33
Additional Exemptions .....	III-11—34
BSA Risk Assessment.....	III-11—34
Products and Services.....	III-11—35
Customers and Entities .....	III-11—35
Using NAICS Codes.....	III-11—36
Geographic Locations .....	III-11—37
Customer Due Diligence (CDD) .....	III-11—38
Customer Due Diligence Guidance.....	III-11—39
Customer Risk .....	III-11—39
Enhanced Due Diligence for High-Risk Customers .....	III-11—40
Obtaining and Retaining Beneficial Ownership Information .....	III-11—41
Exhibits .....	III-11—41
Exhibit III-11.1: Sample Customer Identification Program.....	III-11—42
Exhibit III-11.2: Sample Bank Secrecy Act Policy .....	III-11—45
Exhibit III-11.3: Risk-Based Analysis for CIP Programs.....	III-11—50
Exhibit III-11.4: CIP Sample Audit Worksheet.....	III-11—56
Exhibit III-11.5: FBI Testimony on Matrícula Consular Cards .....	III-11—59
Exhibit III-11.6: OCC BSA/AML Quantity of Risk Summary Form (RSF).....	III-11—62
Exhibit III-11.7: NAICS Code Chart .....	III-11—66
Exhibit III-11.8: Top 10 Questions and Answers for BSA/AML.....	III-11—67
Exhibit III-11.9: Customer Risk vs. Due Diligence and Suspicious Activity Monitoring....	III-11—70