

## **FFIEC Information Technology Examination Handbook Executive Summary**

### **Introduction**

The Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook (IT Handbook), which was developed through a collaborative effort of the FFIEC's five member agencies,<sup>1</sup> has replaced the 1996 FFIEC Information Systems Examination Handbook (1996 Handbook).

In 2001, the Information Technology Subcommittee of the Task Force on Supervision (Information Technology Subcommittee) composed of representatives from each of the FFIEC agencies began revising the 1996 Handbook. The FFIEC Agencies determined that the most efficient way to accomplish the revision and to facilitate future revisions would be to release a series of topical booklets, rather than one comprehensive handbook. This approach facilitates the update process as the individual booklets can be revised as needed. Going forward, the FFIEC will update each booklet as warranted by changes in technology or by the evolution of standards related to financial institution IT practices. Additional booklets will be developed as new topics emerge.

### **Revision Process**

The development and review process for each booklet started with one agency assuming responsibility for an IT topic and developing a preliminary draft of the material relating to that topic. The drafts consisted of a comprehensive narrative and, in most cases, a related workprogram, action summaries, a glossary, and a list of related laws, regulations, and guidance. The preliminary drafts then underwent a series of extensive reviews by a working group composed of representatives of the FFIEC agencies, related FFIEC committees and subject matter experts. When ready, the booklets were reviewed and tested by field examiners from the agencies and revised, if necessary, based on examiner feedback. Senior management of each agency performed the final review and approval and then formally released the booklet. Each booklet was released at the time it was completed.

### **IT Handbook**

The FFIEC issued the initial 12 booklets that make up the FFIEC IT Examination Handbook over a period of approximately 18 months ending in August 2004. The topics of these booklets include: Business Continuity Planning; Development and Acquisition; Electronic Banking; Fedline®; Information Security; IT Audit; IT Management; Operations; Outsourcing Technology Services; Retail Payment Systems; Supervision of Technology Service Providers; and Wholesale Payment Systems. The booklets address significant changes in technology since 1996 and incorporate a risk-based examination approach. The 1996 Handbook has been replaced by these booklets.

---

<sup>1</sup> The five member agencies that make up the FFIEC are: the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

Chapters 1 through 23 of the 1996 Handbook were rescinded with the issuance of the various booklets. Chapter 24 and chapters 26 through 30 contained laws and guidance related to the topic of IT issued by various FFIEC agencies. Please refer to the resources section of the FFIEC IT Examination Handbook booklets or to the individual agencies' websites for this information.

### **Rescission of Supervisory Policies**

With the issuance of the new IT Handbook, several Supervisory Policies (SP) found in Chapter 25 of the 1996 Handbook were rescinded. These are: SP-2, Uniform Interagency Rating System for Data Processing Operations, October 1978; SP-3, Joint Interagency Issuance on End-User Computing Risks, January 1988; SP-4, Supervisory Policy On Large Scale Integrated Financial Software Systems (LSIS), November 1988; SP-5, Interagency Policy On Contingency Planning For Financial Institutions, July 1989; SP-6, Interagency Statement on EDP Service Contracts, January 1990; SP-7, Interagency Policy on Strategic Information Systems Planning for Financial Institutions, March 1990; SP-8, Interagency Document on EDP Risks in Mergers & Acquisitions, September 1991; SP-9, Interagency Supervisory Statement on EFT Switches and Network Services, April 1993; and, SP-10, Control And Security Risks in Electronic Imaging Systems, December 1993. The two remaining SPs, SP-1, Interagency EDP Examination, Scheduling, and Distribution Policy, September 1991 Revised, and SP-11, Enhanced Supervision Program (ESP) for Multidistrict Data Processing Servicers (MDPS), January 1995, can be found under Resources in the Supervision of Technology Service Providers Booklet in the FFIEC IT Examination Handbook.

### **Booklet Summaries**

#### **Audit**

The Audit Booklet provides guidance on the risk-based IT audit practices of financial institutions and technology service providers. This booklet builds on the agencies' existing audit guidance and emphasizes the responsibilities of all levels of management and the board of directors for establishing a sound audit program. The booklet incorporates changes to the audit process brought about by the Gramm-Leach-Bliley Act of 1999 and the Sarbanes-Oxley Act of 2002.

#### **Business Continuity Planning**

The Business Continuity Planning Booklet provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services.

Sound business continuity plans allow financial institutions to respond to such adverse events as natural disasters, technology failures, human error, and terrorism. Financial institutions must be able to restore information systems, operations, and customer services quickly and reliably after any adverse event. It is important that business operations be resilient and that customer service disruptions be minimal.

#### **Development and Acquisition**

The Development and Acquisition Booklet provides guidance on development, acquisition, and maintenance projects; project risks; and project management techniques. The booklet

emphasizes the use of standardized policies, detailed plans, and well-structured project management techniques when directing project activities and controlling project risks. Effective development and acquisition should result in sound information systems that provide specific functionality, reliability, and strong security.

### E-Banking

The E-Banking Booklet provides guidance on risks and risk management practices applicable to a financial institution's e-banking activities.

E-banking has created new opportunities for delivering traditional products and services to customers, as well as the potential to offer new products and services. With these opportunities come new challenges, including 24-hour, seven-day-a-week availability; Internet connectivity; increased access to systems and customer information; greater reliance on new service providers; and evolving regulations. These challenges increase threats to the institution's reputation, confidentiality of information, system and data integrity, system availability, and regulatory compliance. E-banking activities require careful planning, coordinated strategies between IT and business units, integrated subject matter expertise, strong controls, and ongoing monitoring and testing. This booklet includes guidance and examination procedures to evaluate the quality of risk management related to these threats and activities in financial institutions and technology service providers.

### FedLine®

The FedLine® Booklet provides guidance on the appropriate control considerations for financial institutions using the Federal Reserve's FedLine® application.

FedLine® provides financial institutions with access to the Federal Reserve's Fedwire services to receive and send payment messages. To protect their access to this system, institutions must ensure its security and availability. The booklet describes policies and procedures necessary to operate FedLine® in a safe and sound manner with detailed guidance on physical security, system configuration, and system parameter settings.

### Information Security

The Information Security booklet provides guidance for examiners and financial institutions to use in identifying information security risks and evaluating the adequacy of controls and applicable risk management practices of financial institutions.

The safety and soundness of the financial industry and the privacy of customer information depend on the security practices of banks, thrifts, credit unions and their service providers. The Information Security Booklet describes how an institution should protect the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers to maintain effective programs tailored to the complexity of their operations.

### Management

The Management Booklet provides guidance on the risks and risk management practices applicable to financial institutions' information technology activities. Sound IT management is

critical to the performance and success of a financial institution. An institution capable of aligning its IT activities to support its business strategies adds value to its organization and positions itself for sustained success. The board of directors and executive management should understand and take responsibility for IT management as a critical component of their overall strategic planning and corporate governance efforts.

### Operations

The Operations Booklet provides guidance on the risks and risk management practices applicable to financial institutions' technology operations. Effective support and delivery from IT operations are vital to a financial institution's performance and success. The role that technology plays in supporting the business function has become increasingly complex. IT operations have become more dynamic and include distributed environments, integrated applications, telecommunication options, Internet connectivity, and an array of computer platforms. The booklet discusses tactical and strategic support and delivery risks, and the controls that should be in place to address those risks.

### Outsourcing Technology Services

The Outsourcing Technology Services Booklet provides guidance on the risks and risk management practices applicable to financial institutions' outsourcing IT activities, including service provider selection, contract issues, and ongoing monitoring of the relationship. The booklet also includes guidance on the risks and risk management issues unique to foreign service providers. Outsourcing an activity does not relieve management and the board of directors of their responsibility to ensure a secure processing environment and the maintenance of data integrity. Thus, ongoing monitoring of the relationship is crucial to ensure the service provider follows the terms of the service level agreements, safeguards the confidentiality of information, and maintains operational stability.

### Retail Payment Systems

The Retail Payment Systems Booklet provides guidance on the risks and risk management practices applicable to financial institutions' retail payment systems activities, including checks, card-based electronic payments, and other electronic payment media such as person-to-person, Electronic Benefits Transfer, and the Automated Clearinghouse.

Financial institutions play an important role in retail payments, and will face many challenges as they implement new products and services. These challenges are a source of increased risk to institutions and require greater diligence to ensure the confidentiality of information, system and data integrity, system availability, and regulatory compliance. Retail payment system activities require careful planning for coordinated strategies between IT and business units, strong internal controls, and ongoing monitoring. The Retail Payment Systems Booklet includes guidance and examination procedures to evaluate the quality of risk management related to these risks and activities in financial institutions and technology service providers.

### Supervision of Technology Service Providers

The Supervision of Technology Service Providers Booklet covers the supervision and examination of services performed for financial institutions by technology service providers. It outlines the agencies' risk-based supervision approach and the examination ratings used for technology service providers.

The guidance stresses that an institution's management and board of directors have the ultimate responsibility for ensuring outsourced activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations.

### Wholesale Payment Systems

The Wholesale Payment Systems Booklet provides guidance on the risks and risk management practices applicable to financial institutions' wholesale payment systems activities, including interbank and intrabank payments, messaging, and securities settlement systems. Financial institutions play an important role in wholesale payments systems. However, they face increasing challenges to meet demands for resiliency and reliability, while continuing to develop and deploy innovative payment solutions to meet expanding global payment processing demands. Because of these challenges, institutions must exercise greater diligence to ensure that confidentiality of information, system and data integrity, system availability, and regulatory compliance are maintained. Wholesale payment system activities require careful planning and coordination between IT and business units, and their operation must include strong internal controls and ongoing monitoring. The Wholesale Payment Systems Booklet includes examination procedures to evaluate the quality of risk management related to these activities in financial institutions and technology service providers.

### Maintenance Process

The Information Technology Subcommittee will continue to oversee the maintenance of the original 12 booklets, and, when appropriate, will introduce additional booklets on new and emerging issues. This maintenance process ensures the FFIEC IT Handbook remains current, establishes an equitable and flexible rotation and update process, provides ongoing tracking and oversight of needed revisions, and keeps the FFIEC website content current.

As stated above, each of the initial 12 booklets was assigned to an "authoring" agency responsible for the development of the first draft and for maintaining the booklet for a designated period of time beginning with the booklet's release. During this time, the authoring agency is responsible for, among other things, tracking, compiling, and reviewing suggested changes to the booklet and recommending to the Information Technology Subcommittee whether to rewrite or update the booklet. After the designated time, the responsibility for most booklets will rotate to a new agency for maintenance.