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,[1] 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 aseries 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

[1] 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) In October 2006, the Chairman of the State Liaison Committee was added as a voting member to the FFIEC

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. 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[2]

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 (Revised 2008)

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.

The revised booklet, which updates the March 2003 Business Continuity Planning Booklet, includes enhancements to the business impact analysis and testing discussions and addresses

[2] In 2009, the FedLine® booklet was deleted from the FFIEC IT Handbook InfoBase because that booklet is no longer applicable. Several years ago, the FedLine DOS application was terminated. When that happened, the FedLine® booklet became obsolete.

emerging threats and lessons learned in recent years. The booklet also stresses the responsibilities of each institution's board and management to address business continuity planning with an enterprise-wide perspective by considering technology, business operations, communications, and testing strategies for the entire institution.

Key elements of the FFIEC's December 2007 Interagency Statement on Pandemic Planning have been added to the booklet. A pandemic outbreak would present unique business continuity challenges. The methodologies detailed in the booklet provide a framework for financial institutions to develop or update their pandemic preparedness plans. All financial institutions should have plans that address how the institution will function during a pandemic event.

Other changes in the booklet highlight the importance of business continuity planning for all financial institutions, regardless of whether their systems are provided in-house or through third-party service providers, as well as the lessons learned from financial institutions that suffered damage from hurricanes Katrina and Rita.

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.

Information Security (Revised 2006)

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 revised booklet, which updates the 2002 Information Security Booklet, addresses changes in technology, risk assessments, mitigation strategies, and regulatory guidance. The discussion of risk assessment has been expanded to reflect the maturation of that process related to information security. New or revised material is included regarding authentication, monitoring programs, and software trustworthiness. Many additional topics including malware, wireless, remote access, and trust services have also been incorporated or revised.

The security of financial institutions' systems and information is essential to maintaining the privacy of customer information and safe and sound operations. The revised booklet describes how an institution should protect and secure the systems and facilities that process and maintain information. The booklet calls for financial institutions and technology service providers (TSPs) to maintain effective security 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 (Revised 2010)

The Retail Payment Systems Booklet provides guidance on the risks and risk management practices applicable to financial institutions' retail payment systems activities.

The revised booklet, which updates the March 2004 Retail Payment Systems Booklet, addresses changes in technology and provides guidance on the Check Clearing for the 21st Century Act of 2004. This booklet also provides expanded guidance on merchant card processing and ACH activities. It provides a more in-depth discussion of the increased risks posed by these activities and some of the risk management tools that financial institutions can use to mitigate them. In addition, there is an increased emphasis on risk management practices related to third parties in the payments arena, such as Third-party-senders in ACH, or merchant processors in credit card networks. There is also a brief discussion on emerging technologies in retail payment systems. The booklet includes information on remotely created checks and electronically created payment orders, both of which are being used more frequently as payment devices. Lastly, the booklet addresses remote deposit capture and provides examination procedures for use in conjunction with the FFIEC guidance, *Risk Management of Remote Deposit Capture* (January 14, 2009).

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 IT Handbook 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.