FARM CREDIT ADMINISTRATION ★ ESTABLISHED 1933 ★

OPERATIONS

October 2007

Essential Practices for Information Technology Examination Manual IT Section

FCA Essential Practices for Information Technology

Based on Industry Standards and FFIEC Examination Guidance

Table of Contents

Page

Operations

Operations

Introduction:
This section encompasses general operations and network operations. General operations involve maintaining and protecting assets and controlling legal liability. Network operations involve maintaining ongoing integrity, efficiency, and availability of the institution's network. Responsibilities and procedures for the management and operation of all information process facilities should be established.

Management should ensure that stored and transmitted information is protected from damage, loss, or misappropriation. Failure to do so could result in legal liability as well as severe damage to an institution's professional and business reputation. Once the latter is damaged or lost, an institution could find it nearly impossible to continue as a going concern. Therefore, reputation risk can pose a more certain and sudden danger to an institution's existence than the financial liability that can result from more time-consuming legal action.

Examination Objectives:
Determine if the board and management have established and maintained effective IT operation controls and oversight. This is accomplished through the following examination objectives:

- **General Operating Controls** – Evaluate the adequacy of management's controls for IT operations (e.g. inventories, software licensing and compliance, hardware disposal, etc.).
- **Network Operating Controls** – Assess management controls for maintaining network integrity, efficiency, and availability.

Examination Procedures:
Examination activities should be based on the criticality and complexity of the business functions present at the institution. The examination should begin with a review of audit activities and the risk assessment for IT operations. At a minimum, the Essential Practices for IT Operations should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the *FFIEC Operations Booklet*) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

Operations

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
1. General Operations		
Hardware and Software Inventories		
Maintain current hardware and software inventories. ***Reason*:** *Hardware inventories should be maintained to identify assets. Inventories should be used to facilitate:* • *resource sharing,* • *software distribution and maintenance,* • *asset control,* • *hardware security, and* • *repair or replacement of hardware.* *Software inventories should be maintained to identify assets. Inventories should be used to identify:* • *software for replacement or upgrades,* • *authorized users,* • *license compliance, and* • *unauthorized software.*	ISO/IEC 27002:2005, Section 5.1.1, "Inventory of Assets."	Operations Booklet (Jul. 2004) pp. 6-9. Information Security Booklet (Jul. 2006), p. 10. E-Banking Booklet (Aug. 2003), p. 28. Business Continuity Planning Booklet (Mar. 2003), p. 14.
Software Licensing		
Maintain current software licensing and enforce compliance with licensing agreements. ***Reason*:** *Software licensing and compliance with licensing requirements minimizes the legal and financial risks associated with using unlicensed software. As noted above under inventories, an inventory of all software is a key component to controlling this issue, as are detection and protection techniques.*	ISO/IEC 27002:2005, Section 10.4, "Protection against Malicious and Mobile Code"; Section 15.1.2. "Intellectual Property Rights(IPR)."	Operations Booklet (Jul. 2004), p. 9. Development and Acquisition Booklet (Apr. 2004) p. 14.
Equipment Removal/Data Destruction		

Establish formal procedures and controls for the secure removal and disposal of information assets. Essential controls include:
• **Requiring authorization for removal of equipment, information, or software.**
• **Ensuring all data and software are removed or destroyed prior to equipment disposal.**
• **Ensuring information and equipment to be removed or destroyed is stored in a secure area.**
***Reason*:**
	ISO/IEC 27002:2005, Section 9.2.7, "Removal of Property";
	Section 10.7.2, "Secure Disposal or Re-use of Equipment";
	Section 8.6.2, "Disposal of Media."
		Operations Booklet (Jul. 2004), p. 30.
		Information Security Booklet (Jul. 2006), pp. 53.
		Information Security Booklet (Jul. 2006), pp. 74-75.

Operations

Element Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Information can be compromised through careless disposal or re-use of equipment. Therefore, storage devices containing sensitive information, as defined by the institution’s data classification system, should be physically destroyed or securely overwritten. These actions help protect the institution from liability by providing security for confidential information, as well as compliance with licensing agreements.		
2. Network Operations		
Intrusion Detection		
Establish processes to detect, correct, and report unauthorized system access. Essential elements of the process include: • **Detecting external and internal intrusions,** • **Logging incidents,** • **Real-time monitoring,** • **Reporting to management and FCA,** • **Conducting an impact analysis,** • **Establishing an intrusion response process and team, and** • **Updating and maintaining the system.** ***Reason:*** *Using an Intrusion Detection System (IDS) enhances an institution’s ability to determine if its preventive and protective measures are performing as expected. An IDS also provides some protection against legal liability as it can show an institution took “reasonably” expected steps to prevent damage, loss, or theft of privileged information.*	ISO/IEC 27002:2005, Section 13.2, “Management of Information Security Incidents and Improvements”; Section 10.10.2, “Monitoring System Use”; Section 15.2.2, “Technical Compliance Checking”; ”	Information Security Booklet (Jul. 2006), pp. 83-87. E-Banking Booklet (Aug. 2003), pp. 28-29.
Web Site Monitoring		
Review the web site to detect unauthorized changes and implement corrective action if necessary. ***Reason***: *Ensure the web site is available and its integrity is maintained and reputation risk is minimized.*		E-Banking Booklet (Aug. 2003), p. 8.
Internet Use Monitoring		
Establish, monitor, and enforce Internet Usage policies and procedures. ***Reason***: *Ongoing monitoring of internet usage allows management to:* • *Protect corporate resources (e.g., employee time, network resources);*	NIST Special Publication 800-44, “Guidelines on Securing Public Web Servers” pp. ES-2 and 3.	E-Banking Booklet (Aug. 2003), p. 30.

Operations

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
- *Prevent inappropriate use (e.g., gambling, pornography, stock trading, downloading files, etc.);* - *Limit legal liability; and* - *Minimize reputation risk.*		
Internet Data Transmissions		
Identify and classify all internet transmissions. Secure data transmissions of confidential and sensitive information as defined in the institution's data classification system. ***Reason***: *Unless encrypted, information sent via the internet is exposed to disclosure, theft or modification and creates potential legal exposure and reputation damage. To address these concerns FCA issued Regulation 609.950(c) – Electronic Communications in May 2002. This regulation requires institutions to ensure electronic communications represent "good business practices."*	FCA Regulation 609.950(c). ISO/IEC 27002:2005, Section 7.2, "Information Classification."	Operations Booklet (Jul. 2004), pp. 27-29.
Network Traffic Monitoring		
Monitor network faults, performance, configuration, security, and accounting management. ***Reason***: *The network system is an integral part of communications infrastructure. Problems affect many or all users quickly and visibly. Projections of future capacity requirements should be made to ensure that adequate processing power and storage are available. A network administrator should monitor network efficiency statistics, ensure that files are backed up regularly and stored off-site, establish and maintain adequate virus protection, review network activity reports, and react to network alerts and alarms.*	ISO/IEC 27002:2005, Section 10.3.1, "Capacity Planning."	Operations Booklet (Jul. 2004), p. 40. Management Booklet (Jun. 2004), p. 31.
Monitoring Network and Firewall Exploits		
Regularly review the technical alerts/advisories and recommended solutions provided to monitor new threats and implement timely corrective measures to firewalls, network operating systems, and applications. ***Reason:*** *In order to protect the confidentiality, integrity, and availability of data and systems, network administrators must constantly monitor new exploits and ensure that measures to protect against them are applied to systems. Computer hackers and intruders continue to exploit newly discovered holes in firewalls*	FCA Informational Memorandum, "Network Security—Support Web Sites" (Sept. 7, 2000). ISO/IEC 27002:2005, Section 10.4, "Controls Against Malicious and Mobile Code."	E-Banking Booklet (Aug. 2003), p. 28. Operations Booklet (Jul. 2004), p. 26. Information Security Booklet (Jul. 2006), pp. 68-69.

Operations

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
and network systems and devise new attacks.		Development and Acquisition Booklet (Apr. 2004), pp. 55.
Patch Management		
Implement a patch management program that includes: • **Monitoring vulnerabilities and patches for all software identified in the systems inventory,** • **Evaluating the impact of the patches on the institution's information technology systems and environment,** • **Testing the patches to validate expected functionality, and** • **Installing the patches throughout the network.** ***Reason:*** *Inadequate patching of software vulnerabilities exposes an institution to significant risk. Although software vendors often develop an update or "patch" to correct identified weaknesses, it is the software user's responsibility to update systems or install patches in a timely manner. Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from web site defacement to taking control of entire systems, and thereby being able to read, modify, or delete sensitive information, destroy systems, disrupt operations, or launch attacks against other organizations' systems.*	FDIC FIL-43-2003, "Guidance on Developing an Information System Patch Management Program to Address Software Vulnerabilities" (May 29, 2003).	Operations Booklet (Jul. 2004), p. 26. E-Banking Booklet (Aug. 2003), p. 28. Information Security Booklet (Jul. 2006), pp. 68-69. Development and Acquisition Booklet (Apr. 2004), pp. 55.
Network Architecture		
Maintain current diagram of network architecture. ***Reason***: *The network diagram depicts the current network layout and design. It is a tool that the network administrator uses to identify inter-relationships, enforce security, detect problems, minimize risk, and help restore operations.*		Operations Booklet (Jul. 2004), pp. 9-11. E-Banking Booklet (Aug. 2003), p. 28. Information Security Booklet (Jul. 2006), pp. 10.