FARM CREDIT ADMINISTRATION ★ ESTABLISHED 1933 ★

MANAGEMENT

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

Management

Management

Introduction:

The board and executive management (management) actions and philosophy affect all areas of an organization, including management of information technology. Therefore, management must create a framework for the use of information technology (IT) by integrating technology strategic planning into the overall corporate plan, developing applicable policies and procedures, and establishing an internal control system to safeguard data. As part of business planning, management should complete a risk assessment to identify potential risks to institution information and information systems, the probability that these risks will occur, and the expected loss if potential risk becomes reality. Then they can determine what guidelines are required to mitigate the known risks, formulate appropriate policies and procedures, and implement controls. The formality of the information technology plan and policies should be commensurate with institution size, risk, and complexity.

Examination Objective:

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

- **Board and Management Oversight** – Evaluate board and management's planning and oversight of the IT environment. The board remains ultimately accountable for managing its IT functions even though some services may be outsourced.
- **Internal Controls** – Assess the overall adequacy of the board and management's internal control systems (e.g. IT policies and procedures, plans, segregation of duties, reporting structure, personnel qualifications).

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 management. At a minimum, the Essential Practices for IT Management should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the *FFIEC Management Booklet*) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

Management

Element

Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Policies and Procedures		
Adopt policies and procedures to ensure the institution's safety and soundness and compliance with law and regulations. ***Reason*:** *Policies provide the basis for establishing and maintaining proper information technology controls. Policies also translate the development, maintenance and use of management information systems into practical and usable user rules and aid in training new employees. As the operating environment changes, the institution needs to keep pace through updates of policies, procedures, and other operating guidelines. The lack of policy and procedural direction has the potential to cause credit, financial, and other operational problems.*	FCA Regulations 609.930; 618.8430(b). FCA Informational Memorandums, "Guidance for Weblinking Relationships" (Sept. 19, 2002); "Guidance on Authentication in an Electronic Banking Environment" (July 2, 2002); "E-Commerce and Security Risks" (Oct. 2, 2000); "Web Site and Internet Guidelines" (Nov. 8, 1999); "Threats to Information Management Systems" (Aug. 30, 1999). FCA Examination Manual, Section 520, "Policies and Procedures." COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, PO6. ISO/IEC 27002:2005, Section 5.1.1, "Information Security Policy Document."	Management Booklet (Jun. 2004), pp. 13, 25. Audit Booklet (Aug. 2003), pp. 4-5, 18. Business Continuity Planning Booklet (Mar. 2003), p.3. E-Banking Booklet (Aug. 2003), pp. 21, 30. FedLine Booklet (Aug. 2003), pp. 4, 10. Information Security Booklet (Jul. 2006), p. 5. Development and Acquisition Booklet (Dec. 2004), p.2. Outsourcing Technology Services Booklet (Jun. 2004), p. 3. Operations Booklet (Jun. 2004), pp. 15-17.
Technology Plan		
Develop short- and long-range information technology plans and budgets that support the organization's mission and goals. Incorporate the information technology plan into the overall corporate plan. ***Reason*:**	FCA Regulation 609.935. FCA Examination Manual Section 515, "Business Planning."	Management Booklet (Jun. 2004), pp. 16-24.

Management

Element

Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
Information technology is an integral part of institution operations. Therefore, the successful development and maintenance of information technology requires board commitment and planning, as well as appropriate oversight. Because major investments in IT resources have long-term implications on both the delivery and performance of automated products and services, IT resources must be integrated into the overall business planning process. While the complexity of the technology plan will depend on the size and operations of the institution, each technology plan should consider the following critical areas, at a minimum: hardware, software (commercial and in-house development), personnel, and budgets. Operational planning focuses on short-term actions (e.g., annual planning). The operational plans should flow logically from the strategic plan and be revised at least annually.	COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, PO1-PO2.	
Data Integrity		
Ensure data is complete, accurate, and has not been altered in an unauthorized manner (i.e., use appropriate controls such as: edit checks, reasonableness tests, limit tests, common definitions, etc.). ***Reason*:** *Data integrity ensures that data remains complete, accurate, and valid during its input, update, and storage. It will also provide management with accurate information for decision-making.* *Measures taken to ensure integrity include controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining rigorous authentication.*	COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, DS11. ISO/IEC 27002:2005, Introduction, p. viii; Section 0.1, "Information Security—Integrity."	Information Security Booklet (Jul. 2006), p. 2.
Data Classification		
Classify data and information according to the importance assigned during the risk assessment process. ***Reason*:** *Data classification and the allocation of responsibility for its ownership are important to ensure that the value of information is properly recognized. It is the first step towards ensuring that the most valuable information assets have the highest level of protection. Classifying information can help ensure the correct level of protection will be defined and implemented. Information identification should be done at a high level and identify broad categories of information. For example:* • ***Public****—non-sensitive information available for external release* • ***Internal****—information generally available to employees*	ISO/IEC 27002:2005, Section 7.2, "Information Classification."	Management Booklet (Jun. 2004), p. 21.

Management

Element

Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
and approved non-employees • ***Confidential***—*sensitive information intended for use only by specified groups of employees* • ***Restricted***—*extremely sensitive information intended for use only by named individuals*		
Job Descriptions		
Document general and specific security roles and responsibilities for all employees within their job descriptions. ***Reason:*** *All employees, officers, and contractors should comply with security and acceptable use policies as documented in the organization's information security policy. Describing the systems and processes that employees will protect and the control processes for which they are responsible increases accountability for security.*	ISO/IEC 27005:2005, Section 8.1.1, "Roles and Responsibilities."	Information Security Booklet (Jul. 2006), p. 72. Management Booklet (Jun. 2004), pp. 5-14.
Personnel Screening		
Verify job application information on all new employees and contractors. Confirm the applicant's: • **Character references;** • **Prior experience, academic record, and professional qualifications; and** • **Identity using government-issued identification.** ***Reason:*** *Due to their internal access levels and knowledge of the organization's processes, authorized users can pose a threat to systems and data. Performing appropriate background checks should reduce the risks of theft, fraud, or misuse of facilities and information. The sensitivity of a particular job or access level may warrant additional criminal background and credit checks. Management should remain alert to changes in employees' personal circumstances that could increase incentives for system misuse or fraud.*	ISO/IEC 27002:2005, Section 8.1.2, "Screening."	Information Security Booklet (Jul. 2006), p. 71.
Confidentiality and Non-disclosure Agreements		
Obtain signed confidentiality agreements before granting new employees and contractors access to information technology systems. ***Reason:*** *Confidentiality agreements put all parties on notice that the organization owns its information, expects strict confidentiality,*	ISO/IEC 27002:2005, Section 8.1.3, "Terms and Conditions of Employment" and Section 6.1.5, "Confidentiality Agreements".	Information Security Booklet (Jul. 2006), p. 71. E-Banking Booklet (Aug. 2003), p. 30.

Management

Element

Essential Practices Statement	Industry Standard Reference	FFIEC IT Examination Handbook Reference
and prohibits information sharing outside what is required for business needs. A breach in confidentiality could violate regulatory requirements, disregard customer privacy and associated rights, increase fraud risk, disclose competitive information, and damage the organization's reputation.		
Segregation of Duties		
Organize and segregate management and staff assignments to reduce opportunities for unauthorized modification of data, misuse of information, or fraud. ***Reason:*** *Segregation of duties is a basic internal control procedure and is the best deterrent against employee dishonesty or external harm to equipment, documentation or records. For instance, the duties associated with the requisition, approval, execution, and recording of a particular transaction should not be assigned to the same person. Failure to implement and maintain such a system with respect to business activities and information security administration, including maintenance of individual security profiles, constitutes a potentially dangerous practice that may lead to a compromise of system integrity.*	FCA Examination Manual, Section 525, "Internal Controls." COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, PO7. ISO/IEC 27002:2005, Section 10.1.3, "Segregation of Duties."	Information Security Booklet (Jul. 2006), pp. 6, 47, 64. E-Banking Booklet (Aug. 2003), p. 35. FedLine Booklet (Aug. 2003), p. 4, 7, 9. Operations Booklet (Jun. 2004), p. 25. Development and Acquisition Booklet (Dec. 2004), pp. 5, 19.