SYSTEM DEVELOPMENT

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

Systems Development

Systems Development

Introduction:

Systems development is the process of defining, designing, testing, and implementing a new software application or program. It could include the internal development of customized systems, the creation of database systems, or the acquisition of third party developed software. Written standards and procedures must guide all information systems processing functions. The organization's management must define and implement standards and adopt an appropriate system development life cycle methodology governing the process of developing, acquiring, implementing, and maintaining computerized information systems and related technology.

Examination Objectives:

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

- **Board and Management Oversight** – Assess the adequacy of systems development oversight by examining related policies, procedures, and methodology.
- **Risk Assessment**—Determine the level of systems development activities existing within the institution. If systems development activities for mission-critical systems are handled primarily through a service provider, evaluate management's due diligence to ensure appropriate documentation and controls exist within the service provider's development processes. Assess the adequacy of the institution's risk assessment process for systems development.
- **Internal Controls**—Evaluate the effectiveness of preventive and detective controls designed to identify material deficiencies on a timely basis. The internal audit function should identify systems development as an area for evaluation and review.

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 internal and external audit activities and risk assessments for systems development. At a minimum, the ***Essential Practices*** for Systems Development should be clearly documented and functioning within the internal control environment. More in-depth examination procedures (such as those found in the *FFIEC Development and Acquisition Booklet*) should be evaluated and incorporated into the examination scope as an institution's size, risk, and complexity increases.

Systems Development

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
Systems Development Life Cycle (SDLC) Standards and Procedures		
Establish written standards and procedures for systems development and maintenance for the systems to be developed, acquired, implemented, and maintained. Review SDLC methodology to ensure that its provisions reflect current generally accepted techniques and procedures. ***Reason:*** *SDLC documented standards and procedures ensure a consistent approach and controls are maintained throughout a systems or application development process.*	Handbook of IT Auditing, Section B3; Coopers & Lybrand, 1998 edition. COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, PO11.5-11.7.	Management Booklet (Jun. 2004), pp. 25-32. Development and Acquisition Booklet (Apr. 2004), pp. 2, 15-38, 51-57. Information Security Booklet (Jul. 2006), pp. 63-70.
SDLC Management and Controls		
Ensure adequate SDLC management processes and controls exist. Essential management processes and controls over the system development (project) process include: • **Appropriate strategic planning for projects within the IT short- and long-term plans, including authorization and reporting requirements from senior management to the board;** • **Periodic reporting to the board on project status and target completion dates (including budget variance reports);** • **Requirements for internal audit involvement in mission critical projects; and,** • **Requirements for security officer/team involvement regarding security controls.** ***Reason:*** *Appropriate management processes and controls over the systems development process ensures efficient use of resources and minimizes risk(s) within systems development and programming activities. A general systems development or project management framework defines the scope and boundaries of managing projects, as well as the SDLC or project management methodology to be adopted and applied. Automated project planning, monitoring, and production software aids help control and facilitate the systems development process. Periodic reporting to senior management and the board as well as auditor and security officer involvement enables controls to be considered during the development process prior to implementation into production.*	COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, PO11. ISO/IEC 27002:2005, Section 12.1, “Security Requirements of Systems.”	Management Booklet (Jun. 2004), pp. 5-12 & 25-32. Development and Acquisition Booklet (Apr. 2004), pp. 2, 15-38, 51-57. Audit Booklet (Aug. 2003), pp. 18-19. Information Security Booklet (Jul. 2006), pp. 63-70.

Systems Development

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
SDLC Documentation		
Develop and maintain a well-documented SDLC for all system and application development processes. At a minimum, the SDLC documentation will include: • **Project initiation (planning);** • **Requirements definition (analysis);** • **System design;** • **System development;** • **Testing;** • **Implementation and support;** ***Reason**:* *Minimum SDLC standards should ensure that project development is sufficiently controlled to ensure the integrity of the system and IT infrastructure. The development process may differ depending on the method used (prototyping, rapid application development, waterfall, etc.). The process should be flexible while providing maintenance of system integrity and internal controls.*	Handbook of IT Auditing, Section B3. Coopers & Lybrand, 1998 edition.	Development and Acquisition Booklet (April 2004), pp. 15-38.
Testing Standards		
Document testing standards and procedures. Standard testing procedures include: • **A documented test plan;** • **Types of tests to be used (e.g., unit, parallel, user test, regression);** • **A restriction of the use of live files in testing to prevent destruction or alteration of live data;** • **Simulated error conditions to ensure that the program effectively handles all situations; and** • **Independent verification, documentation, and retention of test results.** ***Reason:*** *Testing standards and procedures must be documented to ensure consistency and data integrity during the testing process. The testing phase is designed to prove the reliability of the application or system. Testing is performed in an isolated environment to ensure that new programs do not adversely impact existing production systems. Testing ensures that data will be processed correctly and reliable output will be produced in the desired format.*	ISO/IEC 27002:2005, Section 12.4.2 and 12.2.4 “Systems Development – Change Control”	Development and Acquisition Booklet (Apr. 2004), pp. 29-30.

Systems Development

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
Change Control Approval		
Document standards for managing changes (Change Control) to an existing information systems infrastructure. The Change Control process includes: - **Management and business unit approval of the change request;** - **Specification of change;** - **Approval for access to source code;** - **Programmer completion of change;** - **Request and approval to move source code into the test environment;** - **Completion of acceptance testing by business unit owner;** - **Request and approval for compilation and move to production; and** - **Determination and acceptance of overall and specific security impact.** ***Reason*:** *Change management procedures must be documented and followed in order to minimize the likelihood of system disruption, unauthorized alterations, and errors to the existing IT infrastructure.*	COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, AI6. ISO/IEC 27002:2005, Section 12.5.1, “Change Control Procedures.”	Development and Acquisition Booklet (Apr. 2004), pp. 51-57. Information Security Booklet (Jul. 2006), p. 69 - 70.
Change Control Documentation		
Document the process for modifying information systems programs. Change Control documentation includes: - **Change request date;** - **Person(s) requesting;** - **Change request approval;** - **Change request approval and acceptance (Management and business users);** - **Documentation revision date;** - **Quality assurance approval;** - **Final business unit owner acceptance and approval; and** - **Date moved into production.** ***Reason*:** *Change control documentation is necessary to ensure management and users are aware of changes being made to the existing IT infrastructure. Documentation is also necessary to ensure appropriate segregation of duties between*	COBIT: Control Objectives for Information and related Technology. 4.1 ed. 2000, AI6. ISO/IEC 27002:2005, Section 12.5.1, “Change Control Procedures.”	Development and Acquisition Booklet (Apr. 2004), pp. 51-57. Information Security Booklet (Jul. 2006), p. 69 - 70. Operations Booklet (Jul. 2004), p. 26.

Systems Development

Element		
Essential Practices Statement	**Industry Standard Reference**	**FFIEC IT Examination Handbook Reference**
production, application, and operation staff.		
Emergency Change Control Procedures		
Document and control Emergency Program Changes. Control procedures include: - **Approval by supervisory personnel;** - **Review of changes by a knowledgeable supervisor if the source code is changed;** - **A form used to identify the change, indicate the reason(s) for the emergency change, identify who made the change, record the date the change was made, and document the authorization signature(s); and** - **Completion of normal management procedures after the emergency change is made (see Change Control Essential Practice Statements above).** ***Reason*** *Occasionally the need for program change arises that must bypass normal change procedures. Such a change might be required to restore production processing. These immediate (emergency) changes are usually called patches, quick fixes, program temporary fixes, or temporary program changes. The use of such techniques should be strictly controlled to prevent unauthorized changes and to ensure that approved changes are made correctly.*		Development and Acquisition Booklet (Apr. 2004), pp. 54.