

Stephen Tonn,
Compass Group Consultants, LP

System Development and Acquisition

Our last article in the series related to the April 2004 FFIEC System Development and Acquisition regulatory guidance outlined concepts for project management methodologies. This month's article will continue the series with a discussion of project management roles and responsibilities.

Background

The "Development and Acquisition Booklet" is one in a series of booklets updating the 1996 *Federal Financial Institutions Examination Council (FFIEC) Information Systems Handbook* (FFIEC IS Handbook). The booklet, which rescinds Chapter 12 of the 1996 *FFIEC IS Handbook*, provides examiners and financial institutions with guidance for identifying and controlling development and acquisition risks.

The FFIEC agencies plan to distribute these books electronically via the Internet through the FFIEC's InfoBase application. The InfoBase includes each booklet in Adobe Acrobat file format as well as an online version with links to various resource materials and an orientation to the handbook update process. The new documentation can be found at:

http://www.ffiec.gov/ffiecinfolbase/html_pages/it_01.html

Action Summary for Management

Financial institutions should establish appropriate development, acquisition, and maintenance project management methodologies. The methodologies should match a project's characteristics and risks and include appropriate:

- Project plans;
- Definitions of project requirements and expectations;
- Project management standards and procedures;
- Quality assurance and risk management standards and procedures;
- Definitions of project roles and responsibilities;
- Involvement by all affected parties; and
- Project communication techniques.

Project management in its basic form involves planning and completing a task. Technology-related tasks include ongoing operational activities and one-time projects. A project's impact on operations must be a key consideration when assessing development, acquisition, and maintenance activities.

Roles and Responsibilities

The size and complexity of a project dictates the required number and qualifications of project personnel. Duties may overlap in smaller organizations or lower-risk projects; however, all projects should include appropriate segregation of duties or compensating controls.

Primary project management roles and responsibilities include:

- *Corporate Management* – Corporate managers are responsible for approving major projects and ensuring projects support, not drive, business objectives.

- *Senior Management* – Senior managers are responsible for approving and promoting projects within their authority and ensuring adequate resources are available to complete projects.
- *Technology Steering Committee* – Technology steering committees are responsible for establishing and approving major project deliverables and coordinating interdepartmental activities. The committees often include the project manager, a board member, and executives from all organizational departments. Large organizations often establish project management offices to coordinate multiple projects.
- *Project Manager* – Project managers are responsible for ensuring projects support business objectives, project goals and expectations are clearly defined, and project tasks are identified, scheduled, and completed. Project managers are also responsible for monitoring and reporting a project's status to senior management.
- *Project Sponsor* – Project sponsors are responsible for developing support within user departments, defining deliverables, and providing end users for testing purposes. Project sponsors often provide financial resources to a project.
- *Technology Department* – The technology department is responsible for maintaining the technology resources used by project teams and assisting in the testing and implementation phases. Department members should assist in defining the scope of a project by identifying database and network resources and constraints.
- *Quality Assurance* – Quality assurance personnel are responsible for validating project assumptions and ensuring the quality of phase deliverables. Quality assurance personnel should be independent of the development process and use predefined standards and procedures to assess deliverables throughout project life cycles.
- *User Departments* – User departments assist project managers, designers, and programmers in defining and testing functional requirements (system features). End-user involvement throughout a project is critical to ensuring accurate definitions and adequate tests. Large projects may include a subject matter expert or data analyst responsible for communicating user information and functional requirements to project teams.
- *Auditors* – Auditors assist user departments, project managers, and system designers in identifying system control requirements and testing the controls during development and after implementation.
- *Security Managers* – Security managers assist user departments, project managers, and system designers in identifying security requirements and testing the features during development and after implementation.

Clearly community banks will be challenged to provide staff resources for all of the roles outlined above, but Bank management should separate as many of the defined functions as possible and consider increased levels of supervisory oversight as part of the compensating controls for major technology projects.

Next Month – We will continue with our series of articles on the FFIEC System Development and Acquisition booklet with an overview of controls for systems development.

Stephen Tonn is the Managing Partner of Compass Group Consultants, LP, an independent Internal Audit & IT Security Solutions provider. You can reach him at 210.601.9710 or by email at stonn@thecompassgrp.net.