

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 covered the roles and responsibilities listed for project management. This month's article will wrap up the series with an overview of project planning controls for systems development.

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/ffiecinfobase/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.

Project Planning

Planning is one of the most critical steps in completing development, acquisition, and maintenance projects. Careful planning, particularly in the early stages of a project, is necessary to coordinate activities and manage project risks effectively. The depth and formality of project plans should be commensurate with the characteristics and risks of a given project.

Primary items organizations should address in formal project plans include:

- **Project Overview** – Project overviews provide an outline of the project plan. Overviews should identify the project, project sponsors, and project managers; and should describe project goals, background information, and development strategies.

- Roles and Responsibilities – Project plans should define the primary responsibilities of key personnel, including project sponsors, managers, and team members. Additionally, project plans should identify the responsibilities of third-party vendors and internal audit, security, and network personnel.
- Communication – Defined communication techniques enhance project efficiencies. Therefore, management should establish procedures for gathering and disseminating information. Standard report forms, defined reporting requirements, and established meeting schedules facilitate project communications.
- Defined Deliverables – Clearly defined expectations are a prerequisite for successfully completing projects. Representatives from all departments involved in, or affected by, a project should assist in defining realistic project objectives, accurate informational, functional, and interface requirements, and objective acceptance criteria.

Management should establish acceptance criteria for each project phase. Management should also establish appropriate review and approval procedures to ensure project teams complete all phase requirements before moving into subsequent phases.

- Control Requirements – An essential part of the planning process involves designing and building automated control and security features into applications. Identifying all required features and exactly where they should be placed is not always possible during initial project phases. However, management should consider security and control issues throughout a project's life cycle and include those features in applications as soon as possible during a project's life cycle.
- Scheduling – Management should identify and schedule major project phases and the tasks to be completed within each phase. Due to the uncertainties involved with estimating project requirements, management should build flexibility into project schedules. However, the amount of flexibility built into schedules should decline as projects progress and requirements become more defined.
- Budget – Managers should develop initial budget estimations of overall project costs so they can determine if projects are feasible. Managers should monitor the budgets throughout a project and adjust them if needed; however, they should retain a baseline budget for post-project analysis. In addition to budgeting personnel expenses and outsourced activities, it is important to include the costs associated with project overhead such as office space, hardware, and software used during the project.
- Testing – Management should develop testing plans that identify testing requirements and schedule testing procedures throughout the initial phases of a project. End users, designers, developers, and system technicians may be involved in the testing process.
- Staff Development – Management should develop training plans that identify training requirements and schedule training procedures to ensure employees are able to use and maintain an application after implementation.

A critical part of a project manager's job is to coordinate discussions between user, audit, security, design, development, and network personnel to identify and document as many functional, security, and network requirements as possible.

Next Month – We will begin a new series of articles on the FFIEC Operations booklet.

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



COMPASS
GROUP CONSULTANTS