

**Stephen Tonn,**  
**Compass Group Consultants, LP**

## **System Development and Acquisition**

We recently finished a series of articles summarizing recently released FFIEC Business Continuity Planning guidance. This month's article will be the first in a series focusing on the System Development and Acquisition Booklet that was published by the FFIEC in April, 2004.

## **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](http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html)

## **Introduction**

Development and acquisition is defined as, "an organization's ability to identify, acquire, install, and maintain appropriate information technology systems. The area includes internal development of software applications or systems as well as purchase of hardware, software, or services from third parties. These processes include numerous risks, and effective project management influences a bank's operational risks (also referred to as transactional risks). These risks include the possibility of loss resulting from inadequate processes, personnel, or systems. Losses can result from errors or fraud, or from an inability to deliver products and services, maintain a competitive position, or effectively manage information.

The Development and Acquisition Booklet describes common project management activities and emphasizes the benefits of using well-structured project management techniques. The booklet details general project management standards, procedures, and controls. It also discusses various development, acquisition, and maintenance project risks, and provides action summaries to highlight the primary considerations within each section.

## **Examination Objectives**

Examiners' primary objectives for reviewing development, acquisition, and maintenance activities are to:

- Identify weaknesses or risks that could negatively impact an organization
- Identify entities whose condition or performance requires special supervisory attention
- Effect subsequent corrective action, if needed

Examiners plan to conduct risk-focused reviews that assess the overall effectiveness of an organization's project management standards, procedures, and controls. The guidance does not

require organizations to employ elaborate project management techniques in all situations. However, the booklet encourages organizations to employ project management standards, procedures, and controls commensurate with the characteristics and risks of their software development, acquisition, and maintenance projects.

## **Standards**

The critical importance of technology to financial institutions dictates the use of appropriate development, acquisition, and maintenance standards when new systems are implemented. Standards do not guarantee that organizations will appropriately develop, acquire, and maintain technology systems. However, consistent utilization of appropriate standards will enhance management's control over projects, thereby decreasing project risks. Well-defined standards also help ensure that systems are obtained in an efficient manner, operate in a secure and reliable environment, and meet business and end-user needs. Therefore organizations that routinely complete projects should establish comprehensive standards, policies, and procedures that meet project and organizational needs to reduce project risks.

## **Accounting for Software Costs**

In addition to effectively implementing systems, organizations must correctly account for the costs associated with the acquisition and development of software for internal use. The American Institute of Certified Public Accountants' Statement of Position (SOP) 98-1 requires organizations to capitalize or expense various costs associated with obtaining and developing internally used software. Management should become familiar with SOP 98-1 and other applicable accounting standards and discuss specific capitalization and expense issues with its accountants.

## **Information Security**

Information security is a critical part of internally and externally developed software. Financial institutions should consider information security requirements and incorporate automated controls into internally developed programs, or ensure the controls are incorporated into acquired software, before the software is implemented. For additional details, please refer to the *IT Handbook's* "Information Security Booklet" and additional industry standards such as *Security Considerations in the Information System Development Life Cycle* published by the National Institute of Standards and Technology.

**Next Month – We will continue with our series of articles on the recent FFIEC System Development and Acquisition booklet with a discussion on Project Management.**

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](mailto:stonn@thecompassgrp.net).

