

# Lessons Learned

## COSO, COBIT and Other Emerging Standards for SOX Compliance

BY ROBERT PUTRUS, PE, CMC

**After nearly three years**, many companies still are coming to grips with the Sarbanes-Oxley Act, specifically Sec. 404, and other new compliance laws, such as HIPAA and Gramm-Leach-Bliley.

And even now, there are lessons to learn regarding tools and methodologies used during these early stages of Sec. 404 compliance.

Although SOX is relatively new, the compliance methodologies that companies employ are well-established and are direct outgrowths of established best practices.

Adopted frameworks used in rendering Sec. 404 compliance services include The Committee of Sponsoring Organizations' Internal Control-Integrated Framework and Control Objectives for Information and Related Technologies.

### THE COSO REPORT

The most commonly used framework for evaluating financial reporting internal controls is COSO's, Internal Control-Integrated Framework, which established a broad definition of internal control extending to all objectives of an organization.

The report establishes three categories of controls: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with laws and regulations.

COSO also identifies five, inter-related components that must be functioning to have an effective internal control system, as well as describes the criteria for effective internal control mechanisms.

### THE COBIT STANDARD

COBIT is a 1996 IT control framework published by the IT Governance Institute and the Information Systems Audit and Control Association. It's built, in part, upon COSO's framework and provides a comprehensive approach for managing risk and control of information technology. COBIT comprises four domains, 34 IT processes and 318 control objectives.

The framework has been adopted worldwide by leading companies, financial

institutions and governments as a consistent approach to complying with SOX.

COBIT is considered a gold standard because it indicates good practices for the management of IT processes in a manageable and logical structure. This structure bridges the gaps between business risks, technical issues, control needs and performance measurement requirements.

### LESSONS LEARNED

**No. 1: Automated Software Tools Aren't the Solution.** In response to SOX, many software companies and enterprise resource planning vendors sought to develop software that could document company processes, identify risks, develop test procedures, track the test results and document project status.

At first, the concept seems appealing. However, companies considered these compliance tools an additional cost to an already expensive government mandate. Such software solutions require companies to purchase the software license and database, additional hardware and network equipment; pay annual maintenance fees; and invest time and money in staff training.

The complexity added by new tools made it more difficult for companies to complete the project on time, in part, because the addition of a software package risked shifting the CFO's compliance project to an IT project.

As a result, many companies are using standard office automation tools, such as basic word processing software, spreadsheets and project management software, to document and report SOX compliance.

**No. 2: Everyone Participates.** SOX projects require participation from many levels of an organization, and for Sec. 404 compliance projects to succeed, companies must make their staff an active participant on the integrated project team.

People need to prepare for compliance consultants or auditors, and companies



must commit staff and resources to make efficient use of outside consultants.

**No. 3: SOX Soul Searching.** For best results, SOX projects should be seen as an opportunity for the company to identify and eliminate or mitigate weaknesses, as well as to build upon identified strengths.

SOX compliance can have multiple outcomes, ranging from the introduction of new initiatives to implementing business processes and business enablers throughout the company.

When looking into SOX compliance efforts, publicly held companies must articulate the following:

- Management of the company is responsible for establishing and maintaining adequate internal controls and procedures for financial reports.
- Management's assessment of the effectiveness of the company's internal control over financial reporting, based on management's year-end evaluation, including the disclosure of any material weakness.

Proper SOX compliance will enable all business functions within the company to propose, debate and negotiate what the company's priorities and business initiatives ought to be.

### APPROACHES TO COMPLIANCE

Although Sec. 404 compliance projects are intended to be comprehensive, they don't need to be overwhelming. Companies ought to use the opportunity to re-engineer and streamline their business processes.

As a rule, companies should consider the following when they embark on a Sec. 404 compliance project:

1. Make staff available to the SOX project team.

2. The project team must include company management, company functional staff and members of the consulting team.

3. The team will apply the COSO framework for the business processes.

4. The team will apply the COBIT framework for its IT area.

5. The project must have program and project managers who are accountable.

A well-planned Sec. 404 project may be segmented into seven phases:

*1. Project Planning and Orientation*—Through interviews with company management and internal subject matter experts, consultants will gain an understanding of the company's business practices, policies and procedures; code of ethics; and complaints-handling process.

*2. Corporate Level Control Assessment*—Consultants interview company executives and board members to understand the company's internal controls and its commitment to its board of directors and audit committee; integrity


and ethics; competence; anti-fraud policy; and other related governance issues.

*3. Process Documentation and Narratives*—Project team leaders develop narratives (describing how tasks are accomplished) of the key processes, which are deemed "high" and "medium" complexity. The documentation and narratives address outstanding issues, risks and any initial design remediation that may be required.

*4. Develop Individual Control Matrix*—Consultants develop a control matrix for each of the identified processes. The matrix is part of the COSO framework and includes, but is not limited to, cycle identification; financial statement assertions; control objectives; control risks; control activities; control type; control frequency; control owner; test procedures; test results; gaps; and remediation needed.

*5. Develop Early Remediation Plan*—Consultants develop an early remediation matrix for the identified processes. The team then prioritizes and implements the remediation.

*6. Develop Test Procedures and Test Performance*—Consultants develop test procedures and determine the type of test to be performed for each of the control activities identified in Phase 4. After the tests are developed, the integrated project team performs the test procedures using specialized test templates. Any gaps or failed tests will be identified and evaluated, and a determination made as to whether or not the gap or failure is significant enough to constitute a material weakness.

*7. Identify and Implement Remediation, then Re-test*—The integrated project team recommends actions to close the gaps and pass the tests. This remediation plan prioritizes the agreed upon remediation. The integrated project helps implement the remediation suggestions. Finally, the remediated processes have to be tested. 

**Robert Putrus, PE, CMC** is president of Institute of Management Consultants—San Diego Chapter. You can reach him at (760) 550-2160 or [president@imcsd.org](mailto:president@imcsd.org).