

Control Essentials

Volume I, Issue V

July 2004

Enterprise Risk Management provides the following services:

- Information Security Design and Implementation
- Vulnerability Assessments
- Penetration Testing Studies
- Security Remediation
- Internal Information Systems Audits
- Application Control and Security Services
- Business Continuity Plan (BCP) Services
- Attestation and Assurance
- Compliance with Federal Laws and Regulations

The Clock is Ticking—Are You IT Controls Compliant?

On June 18, 2004 the U.S. Public Accounting Oversight Board (PCAOB) announced the approval of Auditing Standard No. 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements" by the Securities and Exchange Commission (SEC). This standard is applicable for all attestation engagements referred to in Section 404(b) and Section 103(a)(2)(A) of the Sarbanes-Oxley Act.

A key component of compliance within Section 404 of the Sarbanes-Oxley Act and PCAOB rules is the existence of a controlled information technology (IT) environment. The accuracy and timeliness of financial reporting and associated processes is dependent on the design and operating effectiveness of IT key controls as a component of an organization's internal control framework.

The guidelines provided in PCAOB Standard No. 2 are based on the Committee of Sponsoring Organizations (COSO) Internal Control – Integrated Framework. The COSO Framework currently consists of five components including: control environment, risk assessment, control activities, information and communication, and monitoring. The use of IT is apparent in all five components, but most notable in the third component – Control Activities. This component classifies both IT general and application controls as crucial control activities. General controls are the foundation of a well controlled IT environment and directly support the functioning of application controls. Application controls ensure the completeness, accuracy, authorization, and validity of processing transactions for significant accounts identified. To be compliant with Sarbanes-Oxley, all public organizations with a year-end date on or after June 2004 must ensure that IT general and application controls are properly identified, documented, tested, and remediated.

The use of the Control Objectives for Information Technology (COBIT) Internal Control Framework has been widely adopted to demonstrate how IT controls support the COSO Integrated Framework. The COBIT Framework in its entirety consists of 318 control objectives. However, for the purposes of Sarbanes-Oxley compliance, the amount of COBIT objectives were reduced to from 318 to twelve to be aligned with IT general control concepts discussed in PCAOB rules. These concepts include program development, program changes, computer operations, and access to programs and data.

Table 1 below illustrates how the twelve COBIT objectives map to the four PCAOB general control concepts:

COBIT Objectives	Program Development	Program Changes	Computer Operations	Access to Programs and Data
Acquire and maintain application software	X	X	X	X
Acquire and maintain technology infrastructure	X	X	X	
Develop and maintain policies and procedures	X	X	X	X
Install and accredit systems	X	X	X	X
Manage changes		X		X
Define and manage service levels	X	X	X	X
Manage third-party services	X	X	X	X
Ensure systems security			X	X
Manage the configuration			X	X
Manage problems and incidents			X	
Manage data			X	X
Manage operations			X	X

The Clock is Ticking—Are You Sarbanes Oxley Compliant ? (continued)

Benchmarking organizations monitoring Sarbanes–Oxley compliance indicate slippage in the areas of general and application controls documentation, testing, and remediation; specifically in the areas of two COBIT control objectives. These two objectives are Ensure System Security and Manage the Configuration. Requirements within these areas are very technical and require skills that are often not available internally. An example would include the objective of ensuring that the systems infrastructure, including firewalls, routers, switches, network operating systems, and other devices are properly configured to prevent unauthorized access.

Enterprise Risk Management (ERM) is a professional services firm that can assist you with the Sarbanes-Oxley IT compliance process. ERM has specific experience as it relates to the number and complexity of compliance requirements. ERM is positioned to assist you in the following areas:

- identification of application controls including those over initiating, recording, processing, and reporting based upon the identification of significant accounts;
- Identification of general controls as they related to PCAOB general control concepts and COBIT objectives;
- Documentation of applications and general controls design;
- Evaluation of application and general controls design and operating effectiveness;
- Deficiency resolution and remediation;
- Mapping of PCAOB general control concepts to COBIT objectives; and
- Development and/or implementation of COBIT-based controls

ERM specializes in providing risk assessment, information system audit, and security-related services in the U.S. and abroad. ERM professionals have a unique combination of technical and financial backgrounds, supplemented by multiple certifications in the information systems, accounting, and auditing professions; post-undergraduate level educations, and a minimum of ten years practical experience. Our professionals have held high-level IT management and audit positions at numerous prominent organizations in the South Florida area and have worked for the Big Four public accounting firms.

If you are interested in obtaining more information on how ERM can assist you in ensuring compliance with the Sarbanes- Oxley Act, please contact us at (305) 789-6662 or at info@emrisk.com. We would be more than happy to provide additional information on how we can assist in your compliance efforts, the resumes of our professional team members, and a listing of client references. We can also provide you a comparable listing of our billing rates which are significantly lower than those offered by other accounting and consulting firms.

Hope you hear from you soon!

Enterprise Risk Management