

SARBANES-OXLEY COMPLIANCE: A TECHNOLOGY PRACTITIONER'S GUIDE

BONNIE A. GOINS

A misstatement of financials — perhaps accidental, perhaps not; it can happen, and it has. People have lost their jobs and their pensions, sometimes their lives' work. Shareholders have lost their investments. Companies have ceased to exist, mired in bankruptcy and scandal. Senior executives have been on display during legal proceedings. Many have fared incredibly well financially, despite losses sustained by the organization's shareholders and employees. You've heard, and read, these stories.

What's all this about? What can be done to remedy and report the problems associated with misstatement of financials? How can companies and their leaders be held accountable? In 2002, the federal government introduced the Sarbanes-Oxley Act (sometimes called "SOX," "Sarbox," or "SOA"). This piece of legislation comprises many sections; however, the section that may best answer the questions above is Section 404, which requires senior management of publicly traded companies to assess whether their organizations have implemented appropriate control structures around financial reporting, and mandates that they report annually to their boards the results of these assessments.

You may be saying to yourself, "Well, that's all well and good, but how can we be sure that everything that has happened in the past can't happen again? After all, what's the incentive for the companies and their leaders to watch for, and guard against, misstatement of financial information?" The Securities and Exchange Commission (SEC), the government body responsible for the regulation of publicly traded equities, has referred to the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in its final ruling that mandates that an appropriate ("recognized") internal control framework be used within an organization. The Sarbanes-Oxley legislation, as stated in the work by the IT Governance Institute, mandates "corporate governance rules, regulations and standards for specified public companies, including SEC registrants," the implementation of which improves corporate accountability.

The *EDPACS* 2005 Ten-Year Index is now available online. Details on page 24.

IN THIS ISSUE

- **Sarbanes-Oxley Compliance: A Technology Practitioner's Guide**
- **Change Management**

Editor
RICHARD O'HANLEY

Editor Emeritus
BELDEN MENKUS, CISA



AUERBACH

It is important to note that the Sarbanes–Oxley legislation does not, at this time, apply to privately held companies; however, the principles of sound corporate governance map well onto any organization, regardless of its size, which may result in private organizations being added to the compliance expectation at some time in the future. Additionally, the legislation does not take into account aspects of an organization’s business function outside of financial reporting; however, it is clear that organizations can reap significant benefits by applying proper internal controls to the remainder of their business functions. I will return to this theme periodically throughout this article.

*A COMMON THEME
IS THE NOTION
THAT SENIOR
MANAGEMENT
IS RESPONSIBLE
FOR MEETING
COMPLIANCE
OBJECTIVES
AND HELD
ACCOUNTABLE
WHEN COMPLIANCE
OBJECTIVES
ARE NOT MET.*

SENIOR MANAGEMENT RESPONSIBILITIES

A common theme in this legislation is the notion that senior management is responsible for meeting compliance objectives and, conversely, is held accountable when compliance objectives are not met. This precludes the ability of senior management to “fingerpoint” to a subordinate in the event the organization is found to be not in compliance. As stated previously, senior management is required to produce an annual report on the state of internal controls. This report must contain the following:

- A statement of senior management’s responsibility to create, implement, maintain, monitor, and enforce an appropriate internal control structure around financial reporting for the organization
- A statement indicating the method(s) used to assess whether the organization has placed effective internal controls around the financial reporting environment
- Assessment results for the last fiscal year, detailing the state of the organization’s internal controls surrounding the financial reporting environment, along with senior management’s statement regarding the effectiveness of the internal controls in use
- A statement that the organization’s auditing partner (i.e., registered public accountancy) for the financial reporting environment for the fiscal year has attested (through an attestation report) to the effectiveness of internal controls within the

If you have information of interest to EDPACS, contact Richard O’Hanley, Editor, Auerbach Publications, 270 Madison Avenue, 4th Floor, New York, NY 10016 (rich.ohanley@taylorandfrancis.com). EDPACS (ISSN 0736-6981) is published monthly by Auerbach Publications, Taylor & Francis Group, 6000 Broken Sound Pkwy NW, Suite 300, Boca Raton, FL 33487. Periodicals postage is paid at Boca Raton and additional mailing offices. The subscription rate is \$245/year in the U.S. Prices elsewhere vary. Printed in USA. Copyright 2005. EDPACS is a registered trademark owned by Taylor & Francis Group. All rights reserved. No part of this newsletter may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. Requests to publish material or to incorporate material into computerized databases or any other electronic form, or for other than individual or internal distribution, should be addressed to Auerbach Publications, Editorial Services, 6000 Broken Sound Pkwy NW, Suite 300, Boca Raton, FL 33487. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and the Pan American Copyright Convention. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients may be granted by Taylor & Francis, provided that \$20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 0736-6981/05/\$20.00+\$0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. POSTMASTER: Send address change to EDPACS, Auerbach Publications, Taylor & Francis Group, 6000 Broken Sound Pkwy NW, Suite 300, Boca Raton, FL 33487.

organization, as stated in senior management's assessment of the effectiveness of its internal control environment

The Act further requires that senior management provide this report in written format, with an *explicit* statement of the effectiveness of its internal controls. Senior management may *not* assert that internal controls surrounding financial reporting are effective if one or more "material weaknesses" (i.e., instances of required internal controls that are ineffective or absent) has been identified during the assessment of the control environment. Senior management is required to disclose all material weaknesses found within the internal control environment surrounding financial reporting as of the end of the fiscal year. The only allowable exception is if senior management designs and implements an effective internal control to remediate the material weakness prior to the end of the reporting cycle and has sufficiently tested the implemented control over a period of time, such that it can be determined that the newly implemented control is effective for financial reporting.

THE ROLE OF INFORMATION TECHNOLOGY WITHIN SARBANES-OXLEY LEGISLATION

It is clear that this important legislation applies to the accounting principles and environment within publicly traded organizations; however, it cannot be denied that appropriately controlled and protected information technology also plays a major role in the reliability of financial reporting within organizations. As such, IT resources must be present on the Sarbanes-Oxley compliance team to assure that compliance objectives are supported by the organization's infrastructure and application environments. IT resources can be used in any of the following activities:

- Tying systems and infrastructure that provide internal controls around financial reporting to the organization's financial statements; this can be done in tandem with an accounting resource.
- Identifying threats to these identified systems and the infrastructure.
- Conducting a risk analysis that, at least, measures the likelihood the threat will be realized, the impact on the organization in that event, and the calculation of risk based on these two metrics. If the organization is more sophisticated in its measurement of risk, probability and frequency can be added to the analysis.
- Creating, implementing, maintaining, monitoring, and enforcing effective internal controls that protect the organization, including systems, software, and infrastructure.
- Creating, implementing, maintaining, monitoring, and enforcing policies, procedures, and appropriate documentation that detail the effective internal controls that protect the organization, including systems, software, and infrastructure.
- Performing ongoing, periodic testing of the implemented internal controls to assure they maintain their effectiveness.

*IT RESOURCES
MUST BE PRESENT
ON THE
SARBANES-OXLEY
COMPLIANCE TEAM
TO ASSURE THAT
COMPLIANCE
OBJECTIVES ARE
SUPPORTED BY THE
ORGANIZATION'S
INFRASTRUCTURE
AND APPLICATION
ENVIRONMENTS.*

- Updating or adding appropriate internal controls as the environment surrounding financial reporting changes.
- Reporting progress and remediation efforts to senior management and the board, as required.

Information technology and security practitioners can take on the role of IT auditor (if from a third party), providing assistance to senior management during the assertion phase, or these professionals can assist the organization in the remediation of material weaknesses discovered during assessment and assertion testing phases. These roles will be discussed in detail in the material that follows.

*THE COMMITTEES
THAT INTERPRET
THE SARBANES-
OXLEY LEGISLATION
RECOGNIZE THAT
NO ONE SET OF
RECOMMENDATION
S FITS EVERY
ORGANIZATION.*

“Information Technology” Is Pretty Broad – Where Should I Begin?

In March 2004, the U.S. Public Company Accounting Oversight Board (PCAOB) approved an important auditing standard, known as Auditing Standard No. 2 and titled, “An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.” For those of us who are not professional auditors, this standard, as stated in *IT Control Objective for Sarbanes–Oxley* (by the IT Governance Institute), “define(s) the IT systems that are involved in the financial reporting process and, as a result, should be considered in the design and evaluation of internal control.” These systems include any technology involved in financial transactions, such as servers, databases, network infrastructure, and financial applications. Technology categories used by the PCAOB as audit areas include program development, program changes, computer operations, and access to programs and data.

Each of the PCAOB audit areas can be broken down into further detail through the use of the COBIT framework. The relationship between the PCAOB auditing standards and the corresponding COBIT control objectives can be seen in [Tables 1 through 5](#).

Each of the twelve COBIT control objectives used for Sarbanes–Oxley compliance also has detailed specifications that it must meet. These specifications can be obtained through the IT Governance Institute at www.itgi.org. A sample of the level of detail in one of the COBIT control objectives follows in [Table 6](#).

The committees that interpret the Sarbanes–Oxley legislation recognize that no one set of recommendations fits every organization because organizations vary by complexity, size, and other demographics. As such, the sponsoring committees urge the organization to apply internal controls appropriate to its environment. It is also highly recommended that the organization thoroughly document all its decisions regarding internal control design, implementation, and maintenance, but particularly in the case where senior management decides *not* to implement a control, based on business case, lack of resources, or other reasons. An auditor required to attest to the current state of financial reporting will certainly be looking for these documents during the course of an audit.

Table 1 PCAOB Audit for Program Development: COBIT Mapping

Acquire or develop application software
 Acquire technology infrastructure
 Develop and maintain policies and procedures
 Install and test application software and technology infrastructure
 Define and manage service levels
 Manage third-party services

Table 2 PCAOB Audit for Program Changes: COBIT Mapping

Acquire or develop application software
 Acquire technology infrastructure
 Develop and maintain policies and procedures
 Install and test application software and technology infrastructure
 Manage changes
 Define and manage service levels
 Manage third-party services

Table 3 PCAOB Audit for Computer Operations: COBIT Mapping

Acquire or develop application software
 Acquire technology infrastructure
 Develop and maintain policies and procedures
 Install and test application software and technology infrastructure
 Define and manage service levels
 Manage third-party services
 Assure systems security
 Manage the configuration
 Manage problems and incidents
 Manage data
 Manage operations

Table 4 PCAOB Audit for Access to Programs and Data: COBIT Mapping

Acquire or develop application software
 Develop and maintain policies and procedures
 Install and test application software and technology infrastructure
 Manage changes
 Define and manage service levels
 Manage third-party services
 Assure systems security
 Manage the configuration
 Manage data
 Manage operations

Table 5 COBIT Control Objectives at a Glance

IT General Controls (COBIT Process)	Control Objective	Applicable PCAOB General Control
Acquire or develop application software	Controls exist to reasonably assure that software that is either acquired or developed effectively supports financial reporting.	Program development Program changes Computer operations Access to programs and data
Acquire technology infrastructure	Controls exist to reasonably assure that technical infrastructure in the organization supports financial reporting applications.	Program development Program changes Computer operations
Develop and maintain policies and procedures	Controls exist that reasonably assure that policies, procedures, and documents exist and are maintained that instruct in proper use and support the financial reporting environment.	Program development Program changes Computer operations Access to programs and data
Install and test application software and technology infrastructure	Controls exist that reasonably assure the infrastructure performs as advertised and is able to properly support the financial reporting environment; infrastructure must be tested and validated for proper function before being put into production.	Program development Program changes Computer operations Access to programs and data
Manage changes	Controls exist that reasonably assure that significant system changes to the financial reporting environment are authorized, tested, and validated before being put into production.	Program changes Access to programs and data
Define and manage service levels	Controls exist that reasonably assure that there is a common definition of "service levels," and quality, and that support for financial systems will be appropriately maintained.	Program development Program changes Computer operations Access to programs and data
Manage third-party services	Controls exist that reasonably assure that third-party services are appropriately documented contractually; that these services are "secure, accurate and available," as contracted; and that these services properly support the integrity of financial reporting.	Program development Program changes Computer operations Access to programs and data
Assure systems security	Controls exist that reasonably assure that financial reporting systems and subsystems are properly secured.	Computer operations Access to programs and data
Manage the configuration	Controls exist that reasonably assure that all IT components are properly secured and would prevent any unauthorized changes; controls should also help to document the current state of the configuration (i.e., a configuration management plan).	Computer operations Access to programs and data
Manage problems and incidents	Controls exist that reasonably assure that problems are identified as events or incidents and are properly investigated, addressed, resolved, and recorded.	Computer operations
Manage data	Controls exist that reasonably assure that any financial reporting data that is recorded, processed, and reported stays intact (i.e., is complete, accurate, and valid) throughout the processing, transmission, and storage process.	Computer operations Access to programs and data
Manage operations	Controls exist that reasonably assure that any authorized programs are executed as planned and deviations from any scheduled processing are identified and thoroughly investigated.	Computer operations Access to programs and data

Now That I Know the IT Control Objectives, What Do I Do with Them?

Translating the IT control objectives to real-world remediation activities is not always an easy endeavor. Fortunately, there are tools that can help the security practitioner translate the legislative recommendations to a security-oriented framework. The ISO 17799 or the National Security Agency Information Assurance Methodology (NSA IAM) can be used to facilitate this process.

**Table 6 COBIT Control Objectives:
Acquire or Develop Application Software***

Control	Evidence of Control
Security, availability, and processing integrity requirements are included in the organization's formal process for development and acquisition of software (i.e., the system development life cycle).	Review the organization's formal process for development and acquisition to determine whether requirements are included for security, availability, and processing integrity for financial reporting.
Formal policies and procedures exist for development or purchase of new systems, as well as for changes made to existing systems.	Review the organization's formal process for development and acquisition to determine whether formal policies and procedures for additions or changes are included for financial reporting.
The organization's process provides for appropriate integrity controls (i.e., accuracy, validation, authorization, and completion of transactions).	Review the organization's formal process for development and acquisition to determine whether formal application controls are included for financial reporting.
The acquisition and development process should be aligned with the organization's strategic planning process.	Review the organization's formal process for development and acquisition to determine whether senior management reviews, acknowledges, and approves all acquisition and development projects, based upon the direction of the company and approved technology, for financial reporting.
End users are involved in the acquisition and development process, as well as the testing of the end products, to assure resilience and reliability of the result.	Review the organization's formal process for development and acquisition to determine whether end users are included in each appropriate step.
Postmortems are conducted at the end of the acquisition or development process to determine whether controls are operating effectively.	Evaluate a sample of the organization's formal postmortems to determine if they adhere to the stated formal process.
The process is monitored and all relevant acquisition and development efforts adhere to the formal process.	Review multiple acquisition and development projects to determine if they adhere to the stated formal process used by the organization.

* Goal: System software, whether purchased or built in-house, must provide "reasonable assurance" that it effectively supports the organization's financial reporting requirements.

Another method to map remediation activities to compliance requirements is to use the COBIT control objectives to identify like activities already taking place within the organization. This process will require interviews with business units, IT, and senior management to uncover details about business function as it exists on a day-to-day level within the organization. A good baseline questionnaire is included in Appendix B of the IT Governance Institute document referenced at the end of this article.

Typically, business functions that are keyed to compliance are considered to be "critical business functions" within the organization. Evaluation of the procedures used to complete these critical business functions may shed light on the function's mapping to COBIT control objectives. One approach is to develop "process narratives" that can be mapped one-to-one with the control objectives.

MANY ORGANIZATIONS UNDERSTAND THE VALUE OF DOING MORE THAN THE MINIMUM NECESSARY TO MEET LEGISLATIVE REQUIREMENTS.

Here's an example: let's say you have interviewed the resident security team and discovered how it responds to and reports security incidents within the organization. You find out the following details related to this response:

- Senior management has been involved with the response team and approves any deliverables the team produces.
- Senior management views the incident response effort as pivotal to the success of the organization, not just as a means to comply with Sarbanes–Oxley.
- As such, the organization, with the approval of senior management, has purchased an incident tracking system and has implemented it.
- There is a formal process documented for reporting and responding to an incident in the organization; it is available on the corporate intranet and all staff have been trained on its use and their responsibilities for reporting incidents.
- The incident tracking system provides an audit trail on every event or incident that is logged (note that an event, such as a hard drive malfunctioning, is not necessarily a security incident; however, inventory, replacement time, and other demographics may still be tracked if entered into a system such as the one described previously); logs are retained for seven years in a secure off-site storage facility.
- The organization contracts with outside experts to assist in response that is outside the skill set of internal staff; these experts are accounted for in the incident response and reporting process.
- Senior management is provided with reports of all security incidents; senior management, in turn, reports all security incidents to its board, along with response specifics and the resolution to the security incident.

Upon review of the COBIT control objectives for “Manage Problems and Incidents,” you see that the organization has exceeded the requirements listed in the control objectives. You must corroborate all the information received during this interview and gather evidence necessary to support the statements; however, if everything is in order once the validation is completed, you may assume that this particular COBIT control objective has no material weaknesses; only 11 to go!

You may be asking yourself why the organization would want to exceed the requirements for Sarbanes–Oxley compliance. Many organizations understand the value of doing more than the minimum necessary to meet legislative requirements. Often, there is substantive business value in exceeding legislative requirements. Let's take another look at the second-to-the-last item in the incident response process just discussed; that is, the organization utilizes third-party experts to assist in response and reporting that is outside the skill set of internal resources engaged in this “critical business function.” Can you see what might happen if these expert resources were not available to the organization in time of need? Imagine that the organization is breached by a knowledgeable insider and that information is being copied and disclosed from critical systems. Without experts to assist in containment of the incident, eradication of any tools

or malicious software that may have been used for the exploit, recovery of the system to normal working order, and *preservation of any evidence throughout the incident that could lead to the perpetrator and possibly the method of attack*, the organization may have no method for recovering critical data or systems nor the evidence required for successful prosecution, if necessary. Let's take this a step further; let's say that some of the data represents personally identifiable data and this organization does business around the world, with its corporate headquarters and largest customer base located in California. The disclosure alone mandates that everyone whose information was affected must be notified (SB 1386); if one of these affected parties goes to the press ...

Many organizations have come to understand that security and compliance objectives are valuable to the organization as a whole and, as such, the fulfillment of these objectives is applied to the business case, in general, not just to the narrow interpretation of a particular piece of legislation. Fulfilling these objectives may, in some cases, exceed the requirements for the legislation but will nearly always reap rewards (in the scope of protection) for the organization itself. That said, it is also important for the organization to periodically assess its internal controls so that controls applied in areas of low risk, whether they are applied simply to financial reporting or to the organization as a whole or are "overapplied" to any area, can be "right sized" to save the organization resources, dollars, and time.

*MANY
ORGANIZATIONS
HAVE COME TO
UNDERSTAND THAT
SECURITY AND
COMPLIANCE
OBJECTIVES ARE
VALUABLE TO THE
ORGANIZATION
AS A WHOLE.*

THE ASSERTION AND ATTESTATION PROCESS

Step One: Document the Financial Reporting Environment

Individuals in an IT or security role may work as part of a team with a financial resource. This approach works well because a team focus provides comprehensive coverage of the financial reporting environment. In addition to the previously mentioned tasks that may be assigned to an IT resource on a Sarbanes-Oxley project, the IT or security professional must also provide sufficient documented information and evidence around the control environment, as it relates to the technology that supports financial processing. This can be accomplished by either diagramming or documenting the IT processes currently used in the organization and merging this information with processes diagrammed or documented by the financial resource. Here's an example: a financial resource is documenting the process by which a particular financial application performs its critical business function. This person is very familiar with the accounting processes that occur within, or are facilitated by, the application; however, because he or she is unaware of the IT processes that support the application, that part of the documentation is filled with a black box labeled, "Something happens in IT." It is then the IT or security resource's job to properly document the functions and controls that live inside the "black box." Performing the documentation of the financial reporting environment in this way assures that the financial and IT functions are tied together from

the beginning of the documentation process. Other mechanisms are available to accomplish this task; however, a Sarbanes team should never lose sight of the fact that the IT results should correspond, and lend support, to the financial functions that rest upon the technology. Once both the financial resource and the IT or security resource complete the documentation, a joint report or separate reports can be issued to the organization, along with documentation that supports the effort and outlines the work done to date.

*THE ORGANIZATION
USES TESTING
RESULTS TO
REMEDiate
ANY MATERIAL
WEAKNESSES
FOUND IN THE
INTERNAL CONTROL
ENVIRONMENT
SURROUNDING
FINANCIAL
REPORTING.*

Step Two: Work with the Management Assertion Team to Uncover Any Material Weaknesses

When an organization is prepared for assertion, it typically contracts with an outside auditing partner to facilitate the testing of its internal environment. That distinction is important; this auditing partner is considered an *internal resource*. The organization uses testing results to remediate any material weaknesses found in the internal control environment surrounding financial reporting. The IT or security resource may assist the internal auditing team in a number of ways:

- The resource may provide details about the current state of IT, security, and internal controls within the financial reporting environment of the organization. These details can be obtained through a survey based on the PCAOB standards or the 12 COBIT control objectives cited for Sarbanes–Oxley compliance, and is typically provided to the IT or security resource for completion. Although auditors may be more comfortable using the PCAOB standards, organizations may find the COBIT control objectives easier to understand and marry with compliance objectives. Either approach can work in an organization.
- The resource may provide evidence for the assertion team to test.
- The resource may serve as a liaison between the assertion team and the organization's IT departments.
- The resource may assist in remediating material weaknesses as the assertion progresses; this saves the organization and the assertion team time and effort later.
- The resource may be called upon to provide appropriate documentation of the effort in IT.
- The resource may be asked to participate in meetings with the attestation (external auditing) partner, to keep the partner abreast of ongoing activities and to adapt deliverables, if requested by the attestation team, so that the attestation phase is not lengthened.

Step Three: Work with the Assertion and Attestation Teams to Facilitate Attestation of the Organization's Financial Reporting Environment

Not all IT or security resources will be asked to participate with the assertion and attestation teams; however, they may be called upon at any time to participate in any function the team(s) require, with the exception of performing as an auditor. In this case, segregation of duties and, as such, independence, would be

violated. IT or security resources, who may be called upon to perform IT audits as a third party, will likely not be called upon to serve as a remediation resource.

Attestation teams function much like assertion teams; that is, they test the internal controls environment surrounding financial reporting to determine if any material weaknesses can be found. They also prepare an attestation report detailing their findings. This report is provided to senior management and their designees. The team uses PCAOB Audit Standard No. 2 to perform this attestation.

THE COMPLIANCE “ROADMAP”

Achieving compliance is a highly interdependent, business-oriented endeavor. To have any hope of successfully navigating the compliance and control objectives detailed here, IT must align itself with the business goals of the organization.

As stated in *IT Control Objectives for Sarbanes–Oxley*, steps in developing a proper roadmap include:

- Planning and scoping
- Performing a risk assessment
- Identifying significant accounts and controls
- Formalizing and documenting control design
- Evaluating the control design
- Testing the control design for effectiveness
- Identifying and remediating control deficiencies
- Documenting process and results
- Building sustainability

For the practicing security professional, this roadmap should look familiar. Indeed, it is similar to the design, implementation, and maintenance of sustainable security within an environment. As such, it is appropriate to utilize industry best practice tools to conduct these tasks. For example, the NIST Special Publication 800:30 can be used to facilitate the risk assessment within the organization. Identifying significant accounts and controls is akin to identifying criticality within the environment (hence, “significant”). This process likely will be familiar to any IT professional with “life-cycle” knowledge. That said, it is clear that this path can also be taken to implement proper control environments within the organization in areas outside of financial reporting.

References

- International Standards Organization (ISO) 17799/British Standard (BS) 7799
- Information Systems Audit and Control Association (ISACA) www.isaca.org
- IT Governance Institute, *IT Control Objectives for Sarbanes–Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting*, www.itgi.org
- National Institute of Standards and Technology (NIST), www.nist.gov

IDENTIFYING
SIGNIFICANT
ACCOUNTS AND
CONTROLS IS AKIN
TO IDENTIFYING
CRITICALITY WITHIN
THE ENVIRONMENT.

For more on Sarbanes–Oxley:

William Brown and Frank Nasuti, *Sarbanes–Oxley and Enterprise Security: IT Governance and What It Takes to Get the Job Done*, EDPACS, August 2005, pp. 1–20.

Mario Damianides, *Sarbanes–Oxley and IT Governance: New Guidance on IT Control and Compliance*, EDPACS, April 2004, pp. 1–14.

Frederick Gallegos, *Sarbanes–Oxley Act of 2002 (PL 107-204) and Impact on the IT Auditor*, EDPACS, November 2003, pp. 10–20.

Vasant Rasal, *Guidelines for Compliance with Sarbanes–Oxley*, EDPACS, January 2004, pp. 14–20.

National Security Agency Information Assurance Methodology (NSA IAM), www.nsa.gov
Sarbanes-Oxley Act, www.aicpa.org

Bonnie A. Goins, MSIS, CISSP, NSA IAM, ISS is a Senior Security Strategist at Isthmus Group, Inc.. She has over fifteen years of experience in the areas of: information security; secure network design and implementation; risk, business impact and security assessment methods; project management; executive strategy and management consulting; and information technology. She is a coauthor of the Digital Crime Prevention Lab and a contributing reviewer for SANS' HIPAA Step-by-Step.

CHANGE MANAGEMENT

WILLIAM A. YARBERRY, JR.

Change management is a core IT general control required to support the business functions of the enterprise. Although change control is conceptually simple, the mechanics of implementation and monitoring require attention to detail as well as support from IT, users, and business unit management.

At its most basic level, change management is a control system that ensures programs, systems, and infrastructure modifications are authorized, tested, documented, and monitored. One layer below these simple objectives is a plethora of details that challenge even the most procedurally oriented IT organization. As a first step toward good practices, the enterprise needs to set up objectives at the policy level. Examples include:

- Application and infrastructure changes are properly approved, both for work initiation and later migration to production.
- Proposed changes are prioritized based on business needs.
- Changes are auditable and can be traced “up and down” the process. For example, a variation in the size of an executable module can be traced backwards to the documentation authorizing a change; conversely, an authorization for a specific change can be linked to detailed code modifications.
- Failed changes can be rolled back.
- Changes to application code and configurations are tested and approved prior to implementation in production.
- Users participate in application-related testing of changes.
- Segregation of duties is maintained: developers do not promote code into production and “move specialists” do not have access to source code/libraries.
- Procedures exist to ensure urgent/emergency changes are implemented in a controlled and auditable manner.
- Changes are “sized” so that the level of testing and review is appropriate, given the financial/operational impact of the change.