An Overview of Sarbanes-Oxley for the Information Security Professional

GSEC Practical Assignment
Version 1.4b, option 1

Gregg Stults
May 9, 2004

Table of Contents

Abstract
The Sarbanes-Oxley Act of 2002 has dramatically affected overall awareness and management of internal controls in public corporations. Responsibility for accurate financial reporting has landed squarely on the shoulders of senior management, including the potential for personal criminal liability for CEOs and CFOs. Since modern accounting systems are computer based, accurate financial reporting depends on reliable, and secure, computing environments.

Information security professionals are being asked to understand and comply with Sarbanes-Oxley in short time frames and with limited budgets. It is important that they learn as much as they can and create realistic compliance strategies. This paper will describe Sarbanes-Oxley, discuss some of the current strategies for compliance and address some specific guidelines for typical security topics.

Introduction
Information security professionals today face a complex and growing array of government regulations that can affect they way they do their job. Federal and state legislation such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA) and California Senate Bill 1386 can substantially impact the information security requirements for a company. Information security professionals are expected to be aware of, understand, and ensure that their company is in compliance with these laws.

For companies that must report to the Securities and Exchange Commission (SEC), the Sarbanes-Oxley Act of 2002 (SOX) has recently gone into effect. This law was passed as a result of a series of financial scandals in the 1990s, and is intended to mandate better controls and accountability for corporations. Information security professionals will play a key role in a company's ability to comply with this new law. An understanding of the scope and potential issues with SOX is critical to successfully implementing the changes required by SOX.

What is Sarbanes-Oxley?
On July 30, 2002, the Sarbanes-Oxley Act of 2002 was signed into federal law. The stated purpose of the law is *"To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the security laws, and for other purposes."*[1] The effect of the law is sweeping, long term changes in the way publicly traded companies manage auditors, financial reporting, executive responsibility and internal controls. While numerous laws and regulations governing the conduct of public companies already exist, SOX is considered the most substantial piece of corporate regulation since the securities laws of the 1930's.

The creation of SOX followed one of the most turbulent periods in US corporate history. The very public collapse of corporate giants like Enron and WorldCom damaged the fundamental trust in US corporations and cost investors billions of dollars. It also led to the demise of one of the nation's largest public accounting

[1] PCAOB, "Sarbanes-Oxley Act of 2002"

firms, Arthur Anderson.[2] SOX was the government's response. By mandating the requirements for reliability and usefulness of financial reporting, SOX is designed to renew investor's trust and understanding of public corporation financial reporting.

The effect of SOX on information security

To understand how SOX affects information security, an examination of two specific sections of the act is helpful: section 302, titled "Corporate responsibility for financial reports", and section 404, titled "Management assessment of internal controls".

Section 302

Section 302 states that the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) must personally certify that financial reports are accurate and complete. They must also assess and report on the effectiveness of internal controls around financial reporting.[3] This section clearly places responsibility for accurate financial reporting on the highest level of corporate management. CEOs and CFOs now face the potential for criminal fraud liability.[4] It is noteworthy that section 302 does not specifically list which internal controls must be assessed.

Section 404

Section 404 states that a corporation must assess the effectiveness of its internal controls and report this assessment annually to the SEC. The assessment must also be reviewed and judged by an outside auditing firm.[5] The impact of section 404 is substantial in that a large amount of resources are needed for compliance. A comprehensive review of all internal controls related to financial reporting is a daunting task. As with section 302, the wording of section 404 is broad and does not provide specific guidance as to which controls must be assessed.

While the topic of information security is not specifically discussed within the text of the act, the reality is that modern financial reporting systems are heavily dependant on technology and associated controls. Any review of internal controls would not be complete without addressing controls around information security. An insecure system would not be considered a source of reliable financial information because of the possibility of unauthorized transactions or manipulation of numbers. Sections 302 and 404 indirectly force the scrutiny of information security controls for SOX compliance.

PCAOB aka "Peek-A-Boo"

To assist in implementation and oversight of SOX, the act also created the Public Company Accounting Oversight Board (PCAOB).[6] The role of PCOAB is to oversee and guide auditors as they assess a company's compliance with SOX. One aspect

[2] AICPA, "Bird's Eye View of the Enron Debacle"
[3] PCAOB, "Sarbanes-Oxley Act of 2002", Sec. 302
[4] Clayton
[5] PCAOB, "Sarbanes-Oxley Act or 2002", Sec. 404
[6] PCAOB, "Sarbanes-Oxley Act of 2002", Sec. 101

of this guidance is the creation of Proposed Auditing Standards[7] that provide more detailed guidance for assessing compliance with the intent of SOX. The latest release of the standards (on March 9, 2004) states that management assessment of internal controls should include the following element:

> *Determining which controls should be tested, including controls over all relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include: ... Controls, including information technology general controls, on which other controls are dependent.*[8]

The essence of this statement is that information technology (IT) general controls form the foundation for many other types of financial reporting controls and, therefore, must be assessed for SOX.

While the standards proposed by PCAOB address IT controls specifically, they still provides very little practical guidance for an information security professional. This is appropriate, however, considering the substantial range in size and complexity of information systems in public corporations. The PCAOB standard specifically states:

> *Internal control is not "one-size-fits-all," and the nature and extent of controls that are necessary depend, to a great extent, on the size and complexity of the company. Large, complex, multi-national companies, for example, are likely to need extensive and sophisticated internal control systems.*[9]

In addition to some flexibility, it is also important to note that most corporations will already have many or all the necessary controls. Most Information security professionals are well aware of the risks associate with poor security controls and compliance with SOX may consist of simply ensuring that existing practices are documented and working consistently.

COSO

For the purpose of internal control guidance, PCAOB has selected a control framework created by the Committee of Sponsoring Organizations (COSO). The COSO framework provides a structured and comprehensive set of guidelines for creating and implementing internal controls.[10] The use of the COSO framework is not required for SOX compliance, but it is safe to assume that any other framework selected will be similar in scope. An important factor in the selection of COSO was the wide acceptance it already enjoys in US corporations.

---

[7] PCAOB, "Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements"

[8] PCAOB, "Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements" p. A-21

[9] PCAOB, "Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements" p. 9

[10] COSO, http://www.coso.org

COSO provides general guidance regarding information security controls, addressing higher level topics such as control environment, risk assessment, control activities, information and communication and monitoring.[11] COSO, however, still does not provide the specific information that an information security professional would need. Another, more specific, guideline is needed for actual security operations control.

COBIT

The final piece of the puzzle is Control Objectives for Information and related Technology (COBIT). The COBIT framework was created by the Information Systems Audit and Control Association (ISACA) to provide specific guidance for creating and assessing IT controls. COBIT is best described with its mission statement:

> *The COBIT Mission: To research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals.*[12]

COBIT addresses 34 IT processes, ranging from strategic planning to implementation, production support and monitoring. The processes are grouped into 4 domains:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring

Within each of these domains are detailed guidelines for the assessment of every major IT process. By mapping these processes to the more general COSO framework, a roadmap for SOX compliance can be created.

ITGI

The Information Technology Governance Institute (ITGI) is a group created to assist corporations with governing their IT and ensuring IT efficiently supports business mission and goals. ITGI has used COSO and COBIT to create a set of specific IT control objectives for SOX.[13] These control objectives are designed to assist personnel responsible for control assessment. They provide specific guidance in identifying and assessing IT controls. While the COBIT control objectives encompass all IT processes, the focus of this discussion is security.

General guidelines on COBIT information security topics

Within the ITGI general control objectives, the topic of security can be further broken down into specific sub-topics:

[11] COSO, http://www.coso.org
[12] COBIT, http://www.isaca.org/cobit
[13] ITGI, http://www.itgi.org

- Security Policy
- Security Standards
- Access and Authentication
- Network Security
- Monitoring
- Segregation of Duties
- Physical Security

This list may not cover every possible area, but does provide a good starting point for addressing SOX compliance and IT security controls.

Security Policy

What is a policy? *"A policy is typically a document that outlines specific requirements or rules that must be met."*[14] *"…information security policies are 'the bottom line'... they set the boundaries of acceptability across the organization."*[15] For information security, a policy would typically address a specific topic such as acceptable use of company e-mail, or wireless communications. For SOX compliance, policies can be a key piece of documentation for demonstrating compliance to an external auditor. The PCAOB Auditing Standard states *"Documentation might take many forms, such as paper, electronic files, or other media, and can include a variety of information, including policy manuals…"*[16] Comprehensive security policies form the foundation of information security and should drive standards and processes to ensure IT systems are secure. When reviewing security policy for a company consider the following:

- Do policies exist for the appropriate information security topics?
- Have the policies been approved by the appropriate management level?
- Are policies effectively communicated to employees?

There are many sources for guidance on the creation of security policies. The International Organization for Standardization (ISO) includes a section on policy in their ISO17799 standards.[17] The SANS Institute has also gathered a set of guidelines for security policies.[18]

Security Standards

The existence of appropriate security standards should be considered necessary for SOX compliance. According to the SANS institute: *"A standard is typically collections of system-specific or procedural-specific requirements that must be met by everyone."*[19] An example of a security standard would be the Windows 2000

[14] The SANS Security Policy Project, http://www.sans.org/resources/policy
[15] Information Security Policy World, http://www.information-security-policies-and-standards.com
[16] PCAOB, "Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements"
[17] ISO, http://www.iso.org
[18] The SANS Security Policy Project, http://www.sans.org/resources/policy
[19] The SANS Security Policy Project, http://www.sans.org/resources/policy

Benchmark provided by the Center for Internet Security (CIS).[20] This benchmark provides specific guidance for configuring security on a Windows 2000 server. While the CIS benchmark may be adequate for many Windows 2000 installations, they should typically be used as a baseline that will be customized to the specific needs of an organization.

Examples of areas that commonly have security standards include:

- Workstation and server configurations
- Physical security
- Network infrastructure administration
- System access controls
- Data classification and management
- Application development and maintenance

In addition to the standards, policy driven processes should exist for review and maintenance of the standards as well as methods for communicating standards to appropriate personnel.

Access and Authentication

A fundamental control for financial reporting systems is ensuring that only people who are authorized to use the system can access it. Methods to validate that only authorized personnel can access systems should be employed. These could include unique user ID's and passwords or more sophisticated authentication mechanisms such as SecureID[21] or even biometric authentication (fingerprint or retinal scanning).[22]

If passwords are used, they should be forced to meet appropriate requirements including, aging, length, complexity, and limiting the reuse of old passwords. There should also be clear policies regarding safeguarding passwords and sharing of login information.

User Account Management

User account management generally encompasses the processes used for creating, changing and deleting user accounts. When accounts are used to access systems that support financial reporting, these procedures should be formal and documented. Key controls include:

- Account creation and change requests should be documented and require formal approval from the appropriate level of management.
- Terminated employees should have their access promptly removed. A process should exist to ensure that account administrators are notified in a timely manner of employee terminations.
- There should be a regular review process that examines the access

[20] The Center for Internet Security, http://www.cisecurity.org/index.html
[21] RSA Security Inc. URL: http://www.rsasecurity.com/products/securid/
[22] O'Shea

privileges for existing users and verifies they are appropriate. Employee roles change over time and it is a common problem for new access to be granted while old access is never reviewed or deleted.

Network Security

Since most IT systems are connected to a network and probably have some form of access to the internet, it is important that the network infrastructure have appropriate security. Perimeter security should be controlled with firewalls and monitored with intrusion detection systems. In large and geographically diverse networks, using firewalls to segment financial systems from other internal systems may be appropriate.

Encryption may be another appropriate tool to secure sensitive information. SSL or similar encryption methods should be used to secure IP connections whenever passwords or other sensitive data may traverse the link. Digital certificates and other forms of encryption such as PGP[23] should be used when financial information must be moved between systems.

The use of antivirus protection should also be considered mandatory. Recent high profile viruses and worms such as SQL Slammer, and Blaster, can degrade or disable a network as well as open holes for unauthorized access to infected systems. Companies such as Symantec[24] and McAfee[25] provide comprehensive virus scanning tools for a wide range of applications.

Wireless security should also be given specific consideration in an assessment of overall network security. The nature and increasing popularity of wireless network access makes it inherently risky and vulnerable to attack. If wireless access points exist anywhere on a network used by financial systems, special efforts should be considered to secure them. Dedicated firewalls or strong controls around authentication and encryption should be considered. Also, clear policies and standards should exist including processes to identify and track wireless access points and clearly define requirements that must be met before they can be installed.[26]

Finally, an independent assessment of network security may also be appropriate to test the security controls. This may include ethical hacking,[27] or penetration testing from a third party service.[28]

Monitoring

Monitoring of logs and security events is related to many areas of information

[23] PGP Corporation URL: http://www.pgp.com/
[24] Symantec, http://www.symantec.com
[25] McAfee Security URL: http://us.mcafee.com/default.asp
[26] Karygiannis
[27] Levitt
[28] Kurtz

security. Invalid login attempts, port scans, and requests for inappropriate access are all examples of security events that should be monitored. Depending on the size and complexity of IT infrastructure, a very large amount of security event information may be generated. Effective monitoring may require the use of analysis tools.[29]

Regardless of the scope of security monitoring, the result should be identification of security issues and the creation of action plans to address those issues.

Segregation of Duties

Where appropriate, the capabilities required to initiate, carry out, and review transactions should be segregated so that no one person has control over the process from start to finish. What does segregation of duties mean in the context of information security? A definition provided by The Information Security Glossary:

> *A method of working whereby tasks are apportioned between different members of staff in order to reduce the scope for error and fraud. For example, users who create data are not permitted to authorize processing; Systems Development staff are not allowed to be involved with live operations.*[30]

Another example would be: one administrator can create a user, but cannot grant them any access. A different administrator can grant access, but cannot create users. This would prevent one individual from being able to create a new user ID for the purpose of unauthorized access.

In smaller IT departments, segregation of duties may be difficult and operationally inefficient. Where appropriate preventative controls such as segregation cannot be achieved, detective controls, such as monitoring and review of administrative activities, may be appropriate.

Physical Security

Physical access to IT infrastructure systems supporting financial reporting should be restricted. Mechanisms to control access could be as simple as a lock and key or as sophisticated as biometric systems such as facial recognition or retinal scanners. Establishing the physical boundaries can be difficult in today's distributed computing environments. A data center supporting a large enterprise resource planning (ERP) system may have very strong security controls, but a departmental SQL Server may simply be located under someone's desk in the office. In either case, physical access to the systems should be restricted to authorized personnel only, and that access should be monitored and reviewed on a periodic basis.

---

[29] Smith

[30] The Information Security Glossary URL: http://www.yourwindow.to/information-security/index.htm

Conclusion

The job of an information security professional has never been easy. Constant change, management desire for bleeding edge technologies, and limited resources are standard operating procedure today. The recent advent of government regulation has added another layer of complexity to an already complex environment. Words like “control” and “compliance” have crept into the IT vocabulary. To effectively do their job, information security professionals need to stay abreast of the latest government regulations as well as technology.

The Sarbanes-Oxley Act of 2002 has dramatically increased senior management’s awareness of information security as it supports financial reporting controls. This can substantially increase workload and stress on IT personnel, but it can also provide the justification for resources to address security issues that may have previously been given a lower priority. Despite the initial added cost of SOX compliance, the overall improvement in internal controls should result in more efficient operation and ultimately cost savings.

The approach to meeting the challenges of SOX should be similar to other technology challenges: get educated, make a plan and monitor progress toward compliance.

References

Public Company Accounting Oversight Board (PCAOB) “Sarbanes-Oxley Act of 2002” URL: http://www.pcaobus.org/rules/Sarbanes_Oxley_Act_of_2002.pdf

American Institute of Certified Public Accountants (AICPA) “A Bird’s Eye View of the Enron Debacle” URL: http://www.aicpa.org/info/birdseye02.htm

Public Company Accounting Oversight Board (PCAOB) “Release No. 2004-001: An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements” URL: http://www.pcaobus.org/rules/Release-20040308-1.pdf

Committee of Sponsoring Organizations of the Treadway Commission (COSO) URL: http://www.coso.org/index.htm

Information Systems Audit and Control Association (ISACA), Control Objectives for Information and related Technology (COBIT) URL: http://www.isaca.org/cobit

Clayton, Richard D. and Mackintosh, Trip. "Corporate Governance: Avoiding Criminal Liability under Sarbanes-Oxley" Holland & Hart, LLP 2002 URL: http://library.lp.findlaw.com/articles/file/00318/008546/title/Subject/topic/Corporations%20%20Enterprise%20Law_Director%20%20Officer%20Liability/filename/corporationsenterpriselaw_1_114

The SANS Institute URL: http://www.sans.org/resources/policies/

Information Security Policy World URL: http://www.information-security-policies-and-standards.com/

International Organization for Standardization (ISO) URL: http://www.iso.org

Symantec URL: http://www.symantec.com

The Information Security Glossary URL: http://www.yourwindow.to/information-security/index.htm

The Center for Internet Security URL: http://www.cisecurity.org/index.html

RSA Security Inc. URL: http://www.rsasecurity.com/products/securid/

O'Shea, Timothy and Lee, Mike. "Biometric Authentication Management" Network Computing December 27, 1999 URL:http://www.networkcomputing.com/1026/1026f2.html

PGP Corporation URL: http://www.pgp.com/

McAfee Security URL: http://us.mcafee.com/default.asp

Karygiannis, Tom and Owens, Les. "Wireless Network Security 802.11, Bluetooth and Handheld Devices" National Institue of Standards and Technology (NIST) Nov. 2002 URL: http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Levitt, Jason. "Ethical Hacking Made Simple: Satan's Legacy" InformationWeek February 5, 2001 URL: http://www.informationweek.com/author/internet44.htm

Kurtz, George and Prosise, Chris. "PENETRATION TESTING EXPOSED" Information Security Sept. 2000 URL: http://infosecuritymag.techtarget.com/articles/september00/features3.shtml

Smith, Billy. "Thinking about Security Monitoring and Event Correlation" November 3, 2000 URL: http://www.securityfocus.com/infocus/1231