Global Information Assurance Certification Paper

Sarbanes-Oxley:
Information Security's Unlikely Advocate

Matt Sorensen
April 12, 2004
GSEC Practical, v. 1.4b
Option 1

Abstract

Sarbanes-Oxley is a law passed in 2002 that calls for improvements and changes to the financial reporting system in the United States. All public companies registered with the SEC must be Sarbanes-Oxley compliant by June 2004. Sarbanes-Oxley requires the executives of public companies to sign off on the effectiveness of internal controls over financial reporting. The internal control structure should include information security measures designed to ensure confidentiality and integrity of financial data. As public companies race to achieve compliance before the appointed deadline, corporate executives are experiencing a heightened awareness and appreciation for general IT controls, including those that mitigate risks to financial data. Current Sarbanes-Oxley compliance efforts have provided an unprecedented opportunity to voice the need for security to the highest levels of management.

It is important that information security practitioners understand the impact of Sarbanes-Oxley, what the law requires, what the penalties are for non-compliance and what the law means to their respective efforts to secure the enterprise. If not already engaged within their respective organizations, information security professionals must act quickly to show that information security should be considered as an important part of the internal control structure within their organizations. With assistance from openly available control standards, IT security can be woven into the fabric of current Sarbanes-Oxley compliance efforts currently underway within many public companies.

Audience & Objectives

The objective of this paper is to provide IT security professionals, including management, with relevant information regarding the Sarbanes-Oxley Act of 2002 that will enable them to make informed decisions on how to increase information security by leveraging Sarbanes-Oxley compliance efforts within their companies. This information will include an introduction to the Act itself, an explanation of the pertinent requirements of the Act and information about the relationship between these requirements and the information security function of an organization. Information will also be presented about how current corporate-wide Sarbanes-Oxley compliance initiatives can be used by the IT security function to improve the state of information security within the organization.

It is a common scenario played out in many companies: the information security function struggles to gain acceptance as a legitimate and crucial entity within an organization. In the face of well-publicized security breaches, company executives voice support that is not reflected in the amount of resources allotted to the security function. Then, after a significant security breach or sustained outage resulting from the latest Internet worm, the security group is held accountable for its "lack of preparedness" and is charged with remediation efforts. This knee-jerk reaction further pushes security efforts away from the proactive to the reactive. As we shall see, proper adherence to Sarbanes-Oxley can lead to a more tightly controlled IT environment with proactive security measures in place. Instead of pushing security initiatives up the chain of command for funding and approval, security controls may actually be *mandated* from the top of the organization in order to fully comply with Sarbanes-Oxley. The challenge lies in spreading awareness of the information security requirements written between the lines of the Sarbanes-Oxley Act.

What is Sarbanes-Oxley?

While serving as chairman of the House Committee on Financial Services, Rep. Michael G. Oxley (OH) participated in various hearings related to several high-profile corporate meltdowns including Enron, WorldCom and Global Crossing (House, 3). As the vast scale of corporate abuse, fraud and malfeasance emerged during the hearings, it must have become clear that changes were needed in the way public companies and their auditors contribute to the stability and trust that form the foundation of our financial markets. These three companies, along with several others, collapsed in the wake of accounting irregularities and fraud. Their self-destruction was like a series of concussion bombs that shattered the investing public's confidence in our country's financial markets and cost investors billions of dollars. As the details of each company's demise came to light, it was clear that the system designed to protect the investing public was not functioning as intended.

President George W. Bush signed the Sarbanes-Oxley Act of 2002 into law on July 30, 2002 (Hurley). The bill, originally known as the "Corporate and

Auditing Accountability, Responsibility, and Transparency Act of 2002", was introduced during the 107th Congress on Feb 14, 2002, by Rep. Oxley (Corporate and Auditing). After several revisions the bill was renamed the "Sarbanes-Oxley Act of 2002" after Rep. Oxley and Sen. Paul Sarbanes (MD).

Financial Reporting

For technologists not well versed in the financial reporting process, the following background may be helpful. Privately owned companies may divest ownership of the company to the general public as a way to raise capital. In return, investors share in the growth and profit of the company by receiving dividends and hopefully experiencing an appreciation in stock value. Initial public offering (IPO) refers to the initial sale of stock to the public. Companies wishing to "go public" must meet stringent requirements overseen by the Securities and Exchange Commission (Securities). One of the requirements of going public includes an annual financial statement audit by a certified public accounting firm. These annual audits are designed to provide the investing public with the piece of mind that public companies are fairly disclosing complete and accurate financial statements: records of revenue, expenses, assets, liabilities and shareholder equity. The decision to buy or sell a specific stock is often based on the financial performance of a company, as reported in the released financial statements, the accuracy of which has been attested to by an independent third-party.

High-Level Overview

The following overview of the Sarbanes-Oxley Act is based on the actual text of the final bill written by the United States Congress (Sarbanes-Oxley Act). The Sarbanes-Oxley Act contains eleven major sections. A brief overview of each section provides not only a general feel for the overall intent and purpose of the law, but also highlights sections relevant to information security. For brevity, some sections have been purposely omitted.

Section I: Public Company Accounting Oversight Board (PCAOB)

This section establishes the PCAOB, (often affectionately referred to as "Peek-a-boo"). The PCAOB ultimately serves as a government watchdog over the public accounting industry. The main functions of the PCAOB include registering audit firms, establishing standards and guidelines for public audit firms to adhere to, investigating and inspecting the work of these firms and, if necessary, levying and enforcing punitive measures against violators.

Section II: Auditor Independence

This section provides definitive guidance on auditor independence, which has long been a hotbed for debate. At the very root of the auditor independence issue lies the question, "Can an external auditor who receives audit fees from a client, every truly be called independent in relation to that client?" It is alleged that in many instances of corporate fraud, the auditor relaxed requirements or even looked the other way in order to preserve long-standing annuity

relationships with audit clients and to preserve very lucrative consulting contracts. Prior to the provisions set forth in the Sarbanes-Oxley Act it was common for firms accused of such behavior to reach large settlements without admitting or denying guilt.

Section II defines exactly what types of consulting services are strictly prohibited for audit firms to provide to their audit clients. Services such as bookkeeping, internal audit outsourcing, and financial information system design and implementation are prohibited. Other provisions included in Section II include: forced audit partner rotation (every 5 years), and audit committee pre-approval of all services provided by the audit firm.

Section III: Corporate Responsibility

Section III attempts to define the responsibilities of all participants in the financial reporting process, including those of audit committees and corporate executives. Section 302 deals with corporate responsibility for financial reports. It has come to light in recent corporate scandals that company executives browbeat audit partners and audit managers into bending ambiguous rules in their favor, essentially lowering the bar by which the company was measured. Exerting this kind of pressure on the external audit is now expressly forbid. Also, according to Section 302, the Chief Executive Officer and the Chief Financial Officer must personally sign an attestation, which asserts to the following:

1. They have reviewed the financial report,
2. The report contains no false or misleading statements,
3. The financial report fairly represents the financial condition of the company for the period covered by the report,
4. They are responsible for establishing and maintaining internal controls, as well as the following:
    a. They are responsible for designing the internal controls to ensure that they are made aware of any *material information*,
    b. They have evaluated the effectiveness of the internal controls within the last 90 days prior to filing the financial report,
    c. They include their opinion on the effectiveness of the internal controls and procedures in place,
5. They have included any significant changes to the internal controls that occurred during the period covered by the report,
6. They have disclosed any significant deficiencies or fraud to the auditors and the audit committee.

The phrase “material information” can be interpreted as meaning any significant event occurring within an organization that may be financial or non-financial in nature, that must be elevated to the attention of management. Failure to do so may violate the provisions of the Act. Examples of the non-financial related events could most certainly include security breaches and compromises, such as those resulting in loss of intellectual property or customer data.

Section 302 makes the law extremely personal for corporate officers. By purposely failing to comply with the above requirements of Section 302, CEOs and CFOs are not only *personally* liable to pay civil penalties; they are also criminally liable as well. In other words, if internal controls over financial reporting are not sufficiently designed and/or working after the corporate officers have signed off, and they are convicted under the Sarbanes-Oxley Act, they will not only personally pay hefty fines but also face jail time. CEOs and CFOs now have a personal stake in internal controls over financial reporting, which include, as we shall see shortly, information security controls.

Section IV: Enhanced Financial Disclosures

This part of the law gets fairly deep into several technical accounting issues, including the treatment of "off-balance sheet entities" made famous by the Enron scandal. At a high-level, Section IV outlines the various new documents required as part of the financial reports and includes:

1. A corporate code of ethics for senior financial officers,
2. Prohibition of loans to corporate officers from the company itself,
3. Disclosure of significant company stock transactions (buy/sell) made by corporate officers within two business days of the transaction,
4. Management's assessment of internal controls, including external audit's validation of management's assessment.

Item #4 above, is found in Section 404 and combined with Section 302, is the crux of all the noise generated by the Sarbanes-Oxley Act. If you only remember one thing about Sarbanes-Oxley from reading this paper, remember this: within public companies, there must exist an internal control structure over financial reporting, it must be effective in preventing, detecting and correcting financial errors, and both corporate officers and the external auditors must, under penalty of law, attest to its effectiveness. Additionally, the internal control structure should include information security controls.

Section V: Analyst Conflicts of Interest

This section seeks to rebuild investor confidence in the research role of analysts by prohibiting certain conflicts of interest.

Section VII: Studies and Reports

This section calls for formal studies to be made on the public accounting and investment banking industries.

Section VIII: Corporate and Criminal Fraud Accountability

This section does indeed have implications for the information security function of an organization. Section 802 is entitled "Criminal Penalties for Altering Documents". The documents covered by this section include any documents under subpoena for a federal investigation, (remember Andersen and the

shredding?) and corporate audit records including work papers, audit findings and reports. Inasmuch as these documents are in electronic form, they must be protected from unauthorized destruction and alteration. Section 802 also makes mention of electronic correspondence and communications, which can be interpreted as email and voice mail. This section was referred to as the "information security sleeper provision" by Denley Chew, at the 2004 RSA Conference (Chew). Section 802 seems to be somewhat overshadowed by compliance efforts related to Sections 302 and 404.

Section IX: White-Collar Crime Penalty Enhancements

This section lays out new and improved penalties relating to white-collar crime, including penalties for violating the various provisions of the Act.

Section XII: Corporate Fraud Accountability

This section outlines additional penalties for fraud and offers a provision protecting corporate whistle blowers.

Summary of the Act

By way of review, we now have a federal law mandating the use of proven internal controls over financial reporting and severe penalties for failing to do so. Corporate executives are now acutely aware of the legal demands to provide sound and assured disclosure of financial health. CEOs and CFOs must ensure that internal controls are present, working, and must certify the effectiveness of internal controls, as well as have their certification validated by a third party. The not-so-obvious link between Sarbanes-Oxley and information security is beginning to be appreciated. In an article posted on SearchSecurity.com, author Edward Hurley writes,

> What the law will likely do is open a dialogue between upper-level management and their security staff on what is needed to ensure that proper and auditable security measures are in place. The executives who have to sign off on the internal controls have a lot to lose if things aren't kosher; they could face criminal penalties if a breach is detected (Hurley).

As information security professionals we now have a clear opportunity to show that information security should also be considered as an important part of internal control. Now, let's examine what is exactly meant by the terms "control" and "internal control".

A Definition Of Control

A control by definition, is "that which serves to check, restrain, or hinder; restraint." (Control). The term "control" is used extensively in the audit community, most always in conjunction with risk management. Information security practitioners may be more comfortable with the term "countermeasure" as opposed to control. For our purposes the term control will have essentially the

same meaning as countermeasure. Whether dealing with information security or financial statements, a control is really any activity or process, whether performed by a human, a computer or a combination of both, which prevents, detects, or corrects the occurrence of a risk condition, (a “bad thing”). A control mitigates a risk. In the case of information security, a bad thing could be any of the following:

- An exploitation of a buffer overflow,
- A Unix box running r-login,
- A three-digit password.

In the case of financial reporting, a bad thing might be:

- A clerk with full access to both the Accounts Payable and the Accounts Receivable systems could easily commit fraud by creating and paying phony invoices to himself.
- A developer with access to modify the production instance of the general ledger system and the payroll system could pay herself and cover her tracks by hiding the fraud in various legitimate general ledger accounts.
- An external hacker exploits a known vulnerability to penetrate a corporate network and from there gains access to a poorly controlled application and alters key financial records.

In the above examples, appropriate controls could include: code reviews for buffer overflow or automated code checkers, Unix operating system configuration baselines, an enforced password policy, access controls, application change controls and patch management.

A Definition Of Internal Control

Now that we are comfortable with the term control, let’s look at how Sarbanes-Oxley uses the phrase “internal control”. All of the control examples used above could potentially be part of a company’s overall internal control framework over financial reporting. This framework should include various types of controls including both manual and automated controls. The accounting firm BDO Seidman defines internal control this way:

> A company’s internal controls over financial reporting represent a process – implemented and monitored by an entity’s board of directors, management, and other personnel – that relates to preparation of financial statements for external purposes that are fairly presented in conformity with generally accepted accounting principles. Internal controls over financial reporting generally include those policies and procedures enabling a company to properly initiate, record, process, and report financial data consistent with the assertions embodied in either the annual or interim financial statements (BDO).

Let's analyze this definition with eye for information security. Note the phrase "policies and procedures" in the last sentence. This could most certainly include information security policies and baselines. Note the phrase "…initiate, record, process, and report financial data" in the last sentence. Imagine trying to initiate, record or process financial data without computer systems! This financial data will most certainly be housed in databases, acted upon by various applications, manually input by users, etc. and is subject to the myriad risks commonly faced by information security practitioners.

For further ammunition in making the case for information security controls being necessary for Sarbanes-Oxley compliance, let's consider a piece of accounting industry guidance. The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) produces statements of Auditing Standards (SAS). CPAs are required to adhere to these standards when performing audits. SAS 94, entitled "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit" was published in 2001. SAS 94 acknowledges the fundamental reliance of financial reporting on IT and requires IT controls to be considered when performing a financial statement audit. The following risks are explicitly mentioned by the ASB in the text of SAS 94 and clearly correlate to information security risks:

IT also poses specific risks to an entity's internal control, including

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.
- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions.
- Unauthorized changes to data in master files.
- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Inappropriate manual intervention.
- Potential loss of data (Accounting, 5).

As a side note, this is why you'll find knowledgeable technologists serving as IT auditors in most, if not all, internal audit departments of public companies. SAS 94 is a lynch pin linking the necessity of well-controlled IT environments, to not only the requirements of Sarbanes-Oxley, but to the financial reporting process in general.

Application vs. General controls

So far, the reader may be tempted to think that only controls over the general ledger and general ledger posting-applications are covered under Sarbanes-Oxley. This is only partly true. IT controls can be classified as

application controls and general controls. Application controls covered under Sarbanes-Oxley are primarily controls that ensure completeness and accuracy of financial data input, processing and output. General controls are those, which if not working properly, will undermine the effectiveness of application controls and other manual, non-IT controls. It may be the general controls that give the information security practitioner the most opportunity to drive security initiatives with Sarbanes-Oxley efforts.

Examples of general controls include: segregation of duties (enforced by access controls), systems development and program change controls, business continuity and disaster recovery, database management, perimeter security, intrusion detection, logical and physical access controls, secure data communications and operating system baselines. General controls are not usually tied to a specific application; they are relied upon by many applications. For example, two applications, one having financial statement impact (payroll system), and one not having any financial statement impact (customer information database) both depend on properly configured operating systems to prevent unauthorized persons from compromising the confidentiality and integrity of data. Both applications also depend on the same perimeter security controls.

Due to the pervasive nature of general controls, the information security practitioner can make strong arguments for improving them in order to fully comply with Sarbanes-Oxley. The end result is a net improvement for the entire IT environment, not just for financial-related systems.

Defense In Depth: A New View

In order to defend against various kinds of blended threats, information security professionals must employ information security in layers, a technique also known as Defense In Depth. In the case of a security breach at one layer, controls at the next layer can still neutralize the threat. Likewise, when thinking about controls protecting an organization's financial reporting, a layered approach is required. When looking for overlap between controls mandated by Sarbanes-Oxley and information security controls, use the Defense In Depth lens to view your organization. A common approach to determining the IT scope for Sarbanes-Oxley is to work backward from the general ledger, identifying communications channels and posting applications. Peel back the layers starting with the General Ledger system and other applications that post to it. Next consider the general controls that support these applications and communications channels in their intended function. Consider the layers of security around them that provide confidentiality, integrity and availability of financial data. Consider threats to the OS, database, network and perimeter, and you'll most likely find common threats across your organization, not just to financial reporting processes. Once the scope has been defined it is time engage your organization's Sarbanes-Oxley compliance process and methodology.

Control Frameworks

When evaluating the constitution and effectiveness of a system of internal controls, it is necessary to measure against a standard or a benchmark. The following are examples of some common standards that can be used as guidance in defining and measuring internal control.

COSO

Sarbanes-Oxley mandated that the SEC provide rules for implementing the provisions of the Act. The SEC released their rules effective August 2003 (Securities). Of particular interest is the SEC's definition of internal control and their requirement that companies declare the use of a common standard for internal control (Moulton). The SEC went further by stating that a commonly known standard for internal control, known as COSO, is acceptable (Securities). Based on this recommendation many organizations are using COSO as a guide for internal control and to assist them in reaching Sarbanes-Oxley compliance.

In 1985, a private-sector initiative was undertaken to examine the financial reporting system in the United States. This initiative was called the National Commission on Fraudulent Financial Reporting, also known as the Treadway Commission (Ibid). Members of the commission represented several financial professional associations. The commission called on its member organizations to work together to produce a common definition and framework for internal control (Ibid). The result was released in 1992 and is known as COSO, which stands for Committee Of Sponsoring Organizations of the Treadway Commission. As noted in the SEC Rules, there are five core elements of an internal control framework as defined by COSO:

1. Control Environment
2. Risk Assessment
3. Information & Communications
4. Control Activities
5. Monitoring (Ibid)

IT controls are not given deep coverage in the COSO model and although COSO does implicate the importance of IT controls, little guidance is given for actual implementation. Therefore, while many organizations have made COSO their guide for internal control, they have turned to alternative control frameworks for additional help in defining and measuring controls over the IT environment.

COBIT

The IT Governance Institute (ITGI), a research arm of the Information Systems Audit & Control Association, produces control Objectives for IT, also known as COBIT (IT). COBIT provides 318 IT-specific control objectives categorized under 34 IT processes. These processes are in turn grouped under four categories:

1. Planning & Organization
2. Acquisition & Implementation
3. Delivery & Support
4. Monitoring (Ibid, 32)

COBIT provides guidance that can be used to augment COSO in developing or evaluating the IT components of internal control. Additionally, to help with the demand for Sarbanes-Oxley compliance, ITGI has released COBIT for Sarbanes-Oxley, which is a subset of COBIT's 318 control objectives most relevant to financial reporting. Even more specific to information security, but not as popularly used in Sarbanes-Oxley compliance efforts, are the ISO 17799 and ITIL standards.

Sarbanes-Oxley Compliance Efforts

Compliance with Sarbanes-Oxley is not a simple task. Most, if not all, public companies are currently well underway in their efforts to comply with Sarbanes-Oxley. The CEO and CFO generally lead the effort with the oversight of the audit committee. The executives typically delegate authority for providing management's assertion down the chain of command, ultimately ending with the management within each operating unit. To determine scope, the financial statements are used as a starting point and each line item is traced back to its source, which is usually a line of business or specific business unit. Often working with management is the CIO organization; again tracing the data feeds into the general ledger system back to the originating applications. External feeds from service providers may be involved. Information security is usually involved with the compliance effort under the authority of the CIO.

Internal Audit (including IT audit) may play a variety of roles that range from assisting management with identifying risks and controls to actually testing controls. Internal audit may choose to remain independent of the process in order to provide their own objective opinion on the state of controls, independent of management's assertion. In this case outside consultants are often brought in to assist management.

Once all the financially relevant business processes and supporting technology systems have been identified, a risk analysis is performed to identify risks to the completeness, accuracy and integrity of the financial data. Flow charts and process narratives are often produced for each process to ferret out the controls typically in place to address each risk. Often control gaps are found and documented.

Once a population of controls has been identified, only the key controls are selected for testing. Determining which controls are key is usually based on which controls are most heavily relied upon by the business unit. Based on the results of testing, each control owner (a representative of management) signs off on the effectiveness of the control, or develops a remediation plan and selects

mitigating controls to test. The sign-offs roll up successively through the chain of command until ultimately, the CFO and CEO, trusting and relying on the validation performed by their subordinates, sign off on the effectiveness of the internal control structure. It is important to remember it should be the CEO and CFO that provide *management's* assertion, and no one else's. Internal audit, external audit, outside consultants, etc. should not be the ones making the final evaluation of the effectiveness of the controls. Management alone should make the final evaluation.

Conclusion

In conclusion, there is now a federal law mandating the use of proven internal controls over financial reporting, which includes severe penalties for non-compliance. Corporate executives are now aware of the demands placed upon them to provide sound and assured disclosure of financial health. CEOs and CFOs must ensure that internal controls are present, working and certified by a third party. Information security professionals now have a clear opportunity to show that information security should also be considered as an important part of internal control.

Most organizations have begun preparing for Sarbanes-Oxley compliance. If the information security function has not been involved with compliance efforts to date, it is critical that they have a voice as soon as possible. Typical involvement starts with a senior information security manager or CISO working in close concert with the CIO organization. Working as a part of a multi-disciplinary team, IT security can assist management in documenting, evaluating, testing and addressing security controls and deficiencies in the IT control environment.

Works Cited

Accounting Standards Board, American Institute of Certified Public Accountants. "Statement on Auditing Standards No. 94, The Effect of Information Technology On the Auditor's Consideration of Internal Control in a Financial Statement Audit". June 4, 2001.

BDO Seidman LLP. "Definition of Internal Controls Over Financial Reporting" 2003. URL: <http://www.bdo.com/about/publications/assurance/fr_mar_2003/def.asp> (April 2004).

Chew, Denley. "Sarbanes-Oxley: The Stealth Information Security Law?". 2004 RSA Conference. Moscone Center. San Francisco. February 24, 2003.

"Control" Webster's Revised Unabridged Dictionary, Electronic Ed., © 1996, 1998 MICRA, Inc. URL: <http://dictionary.reference.com/search?q=control> (April 2004)

House Committee on Financial Services. "Rebuilding Investor Confidence, Protecting U.S. Capital Markets". Financial Executives International. 2003. URL: <http://www.fei.org/news/finrep/files/Sarbanes-Oxley_report.pdf> (March 2004).

Hurley, Edward. "Security and Sarbanes-Oxley." SearchSecurity. Sept. 25, 2003. URL: <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.html> (March 2004).

IT Governance Institute. "IT Control Objectives for Sarbanes-Oxley", April 2004. URL: <http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm> (April 2004).

Moulton, Bruce W. "Sarbanes-Oxley: What it Means To Your Security Program". 2004 RSA Conference. Moscone Center. San Francisco. February 25, 2004.

Securities and Exchange Commission. "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports". 2003. URL: <http://www.sec.gov/rules/final/33-8238.htm> (April 2004).

United States Congress. “Corporate and Auditing Accountability, Responsibility, and Transparency Act”. Thomas, Legislative Information on the Internet. February 14, 2002. URL: <http://thomas.loc.gov/> Search: 107th Congress, Bill Number “HR 3763” (April 2004).

United States Congress. “Sarbanes-Oxley Act of 2002”. House of Representatives Financial Services Subcommittee. July 24, 2002. URL: http://financialservices.house.gov/media/pdf/H3763CR_HSE.PDF (March 2004).