Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Security and Section 404 of the Sarbanes-Oxley Act

In response to the corporate accounting scandals of 2001 the Public Company Accounting and Investor Protection Act of 2002 was passed. Also called the Sarbanes-Oxley Act, it is broken down into eleven titles containing sixty-six sections which cover everything from establishing the Public Company Accounting Oversight Board (PCAOB) to making it illegal to retaliate against an informant. Probably the most talked about and the most important part of the Sarbanes-Oxley Act for information technology professionals is sectio...

Copyright SANS Institute
Author Retains Full Rights

AD

Table of Contents 1
Reed_Warner_GSEC.doc 2

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Information Security and Section 404 of the Sarbanes-Oxley Act

Reed Warner
GSEC Practical 1.4c, Option 1
Submitted December 16, 2004

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Abstract

In response to the corporate accounting scandals of 2001 the Public Company Accounting and Investor Protection Act of 2002 was passed. Also called the Sarbanes-Oxley Act, it is broken down into eleven titles containing sixty-six sections which cover everything from establishing the Public Company Accounting Oversight Board (PCAOB) to making it illegal to retaliate against an informant. Probably the most talked about and the most important part of the Sarbanes-Oxley Act for information technology professionals is section 404, which deals with internal controls.

This paper will summarize section 404 and recently released items relating to it, such as the Public Accounting Oversight Board's release of the Auditing Standard #2 on March 9, 2004[1] and the Security and Exchange Commission's Final Rules related to section 404, released on May 27, 2003[2]. It will then discuss the how an information security team can help an organization stay compliant with Section 404.

The Sarbanes-Oxley Act, Title IV Section 404

Section 404 of the Sarbanes-Oxley Act requires the executives of publicly traded companies to confirm that they have effective internal controls around the financial reporting. An internal control can be a process or procedure that provides reasonable protection that the financial reporting is accurate. Section 404 also requires that the company assess its internal control structure to verify that all controls are effective[3]. The second part of Section 404 deals with the evaluation and reporting of the internal control structure by a registered public accounting firm. The act itself is uses very broad language and does not say specifically what the management of a company needs to do to make sure that its testing and evaluation of the internal control structure is adequate. The same can be said for the assessment of the public accounting firms as well. Looking at the act itself offers no specific guidance on how to evaluate or test any of the internal controls designed to protect the processes and data that contribute to the financial reports. The deadlines for compliance with section 404 have been pushed back, probably due to this lack of specific guidance on how to comply. The deadline for compliance with section 404 is now the date of the first annual report after April 15, 2005, the exception being a company that has market capitalization of $75 million or more and is on an accelerated filling deadline has to comply by the date of its first financial report released after November 15, 2004[4].

---

[1]Deloitte, URL: http://www.deloitte.com/dtt/article/0,1002,sid%253D2002%2526cid%253D43641,00.html
[2] United States Securities and Exchange Commission, URL: http://www.sec.gov/news/press/2003-66.htm
[3] United States Securities and Exchange Commission, URL: http://www.sec.gov/news/press/2003-66.htm
[4] Gartner, URL: http://www4.gartner.com/DisplayDocument?doc_cd=119939

© SANS Institute 2005

Author retains full rights.

In order to understand Section 404 completely it is very useful to read the actual text of the law. Below is the entire text of the Sarbanes-Oxley Act Section 404[5]:

> **SEC.404. MANAGEMENT ASSESSMENT OF INTERNAL CONTROLS.**
>
> (a) RULES REQUIRED- The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall--
> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
> (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
>
> (b) INTERNAL CONTROL EVALUATION AND REPORTING- With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Securities and Exchange Commission's final rules related to Section 404

The Securities and Exchange Commission's final rules related to section 404 include a number of important items. These rules include a list of items that must be included in the internal controls report, they are[6]:

- management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year
- a statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting
- a statement that the registered public accounting firm that audited the company's financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting

Along with these components that must be included there are several

[5] Findlaw, URL: http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
[6] Securities and Exchange Commission, URL: http://www.sec.gov/rules/final/33-8238.htm

© SANS Institute 2005

Author retains full rights.

other important items included in these rules. One of the most important rulings also included is an official definition of the term "internal control over financial reporting."[7] The definition says that the management team (the executive team and board or others filling those roles) will put into place certain policies and procedures that pertain to the financial statements. These policies and procedure should follow generally accepted accounting principles and should include three main points. The first main point is that the policies and procedures will maintain the accuracy of the financial reports. The second is that they will allow the preparation of financial reports using "generally accepted accounting principles"[8] and that "receipts and expenditures"[9] are being entered only if authorized. The final main point is that they provide for the prevention or detection of unauthorized use of assets that would have "a material effect on the financial statements."[10]

The PCAOB's Auditing Standard #2

The Public Company Accounting Oversight Board's release and adoption of its auditing standards are key to complying with the Sarbanes-Oxley Act. The framework to be used in auditing the internal control structure is the auditing framework release by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission in the document *Internal Control – An Integrated Framework.* The COSO organization is "…a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance."[11] The Treadway Commission is the common name for The National Commission on Fraudulent Financial Reporting which was derived from the last name of former SEC Commissioner James C. Treadway.[12] The Securities and Exchange Commission approved this auditing standard on June 17, 2004[13].

The PCAOB will accept other standards, but any other standard must contain the general principles that are included in the COSO framework.[14] There are five main components of the COSO framework: Control Environment. Risk Assessment, Control Activities, Information and Communication, and Monitoring. I will cover each section of this in detail later in this paper.

---

[7] Securities and Exchange Commission, URL: http://www.sec.gov/rules/final/33-8238.htm
[8] Securities and Exchange Commission, URL: http://www.sec.gov/rules/final/33-8238.htm
[9] Securities and Exchange Commission, URL: http://www.sec.gov/rules/final/33-8238.htm
[10] Securities and Exchange Commission, URL: http://www.sec.gov/rules/final/33-8238.htm
[11] IT Governance Institute URL:
http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf
[12] The Institute of Chief Risk Officers, http://riskinstitute.ch/00013184.htm
[13] Securities and Exchange Commission, URL http://www.sec.gov/rules/pcaob/34-49884.htm
[14] Public Company Accounting Oversight Board, URL:
http://www.pcaobus.org/Rules_of_the_Board/Documents/Rules_of_the_Board/Auditing_Standard_2.pdf

© SANS Institute 2005

Author retains full rights.

Corporate Information Security Programs

Creating effective internal controls and putting them into practice will have a large effect on the information security program. Effective controls can be included in a number of different things that an information security team is responsible for, from an intrusion detection system to monitor for malicious network activity to reviewing log files on a periodic basis. A good way to look at the relationship between the Sarbanes-Oxley Act Section 404 and an information security program is to look at each of the five elements of the COSO framework.

Control Environment

The control environment element sets the overall tone of internal controls in a company[15]. For an information security program, this can mean having the right support from senior management to be able to carry out its functions relating to the internal control structure and everyday information security tasks. There are a number of things that an information security professional will have indirect contact with that fall under the element of control environment. For example, an employee may be required to sign a code of conduct[16]. This is usually not something an information security team creates directly, but most likely will be required to sign. The structure of how the information security team and its managers report up to the management of the corporation also falls under the element of Control Environment.

Control Activities

The element of control activities is where the information security team can play the most active role in compliance with Sarbanes-Oxley Section 404. This element contains a lot of the things that information security professionals are used to doing in their everyday duties. The control activities element breaks down into two separate control types, general controls and application controls[17].

Control Activities: General Controls

General controls include the policies and procedures that ensure that the data coming out of IT systems that is used in preparation of the financial statements is accurate. General controls can be broken down into four types,

---

[15] IT Governance Institute URL: http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf

[16] PriceWaterhouseCoopers URL: http://www.pwcglobal.com/extweb/service.nsf/8b9d788097dff3c9852565e00073c0ba/62672b99f219016085256f0e005c14fa/$FILE/SOActSection404Pract37AC61.pdf

[17] IT Governance Institute URL: http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf

© SANS Institute 2005 Author retains full rights.

data center operational controls, system software controls, access security controls, and application system development and maintenance controls.[18] The key to the role information security plays in making these controls effective is the creation, implementation and enforcement of an information security policy. This policy contains "rules and regulations that must be met."[19] The security policy can contain elements of all of the types of general controls.

Control Activities: General Controls: Data Center Operational Controls

One of the elements of the data center operational controls is a physical security policy which will define who physically has access to the systems that data resides on. This is necessary to ensure that the data has not been manipulated from the console of the system or copied off of that system. Other elements of the data center operational controls are policies that outline batch process scheduling. The information security team should make sure there are proper policies regarding the scheduling and running of batch jobs. They should verify regularly that these policies are being followed and document it in an auditable form.

Another key element of this piece of the IT general controls is that of data backup and recovery planning. A good security policy should contain a section on data backup and recover planning. Along with establishing a policy for data backup and recovery, the information security team should regularly test the restoring of critical systems. After performing regular backup and recovery tests, the results should be documented and communicated to all appropriate individuals.

Control Activities: General Controls: System Software Controls

The system software element of IT general controls is very broad and can cover many different things. The role of information security should be to set policies that affect the maintenance and implementation of systems. System administrators should follow these policies when implementing new systems and software. The information security team should spot check systems to verify compliance with the policies. The results from these checks should be monitored and tracked to make sure that future implementation to not fail compliance with policies. System software can cover a very broad range of services that are maintained by an organization. Database software, operating system software and other systems that provide underlying infrastructure to an organization's information systems should be taken into consideration by the information security team when creating policies and procedure as controls around them.

---

[18] IT Governance Institute URL: http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf
[19] SANS Institute, http://www.sans.org/resources/policies/

© SANS Institute 2005

Author retains full rights.

This is where a policy for antivirus software would fall in the COSO framework. With a record number of viruses and worms that made their way around the Internet and private networks this year, the implementation and maintenance of a good antivirus system is a key control for maintaining system software. The information security team should maintain the antivirus system and ensure that all systems that are threatened by current worms or viruses are protected. Regular and random checking of systems to ensure that system administrators have not purposely or inadvertently disabled the antivirus software and that the software is up to date with the latest virus signatures is very important to maintaining the protection of that system.

Control Activities: General Controls: Access Security Controls

Access security controls prevent the unauthorized use of systems or unauthorized access to data. Making sure appropriate policies exist for the review of user IDs and access levels is an important item for the information security team to consider. Procedures for the removal of access for terminated employees or employees that may have transferred to another part of the company and no longer have the business need to access certain applications or data is also an important piece to effective access security controls. The creation of these procedures can fall within the duties of an information security professional. The information security team should also be checking that these policies are followed and that no inappropriate access exists. The use of passwords is very prevalent in today's applications, so a password policy should be developed. The password policy should include things like the length and complexity level of acceptable passwords. The information security team should also check the passwords of systems on a regular basis to ensure that system administrators and users are in compliance with the policy. They should also verify the settings of applications and operating systems to make sure that the password restrictions and other settings comply with the approved security policy. Again, documenting the results is key to providing evidence of an effective internal control structure.

Control Activities: General Controls: Application System Development and Maintenance Controls

The Information Security team's role in the application system development and maintenance control is not unlike the other controls. Policies should be created and implemented to ensure that only approved changes are implemented into existing software and that the development life cycle of new application development projects is a well defined process. The Information Security team should also play an active role in designing new applications or major changes to existing application to make sure that the policies are followed and the data or processes remain as secure as possible. For example, if a new application is being developed to transfer data to a customer via the Internet, information security personnel should be involved to make sure the data is

© SANS Institute 2005

Author retains full rights.

encrypted during the transfer.

Control Activities: Application Controls

Application controls differ from general controls in that they are contained within the software that is creating and/or manipulating the data that is used in the financial statements. An example of this is a check in accounting software that may trigger an email to an appropriate person if a transfer of an unusual amount of money amount is requested. The best way for information security to make sure application controls work effectively is to make sure that the controls cannot be changed without proper approval and documentation. Protecting the system infrastructure from unauthorized use or access is another way to keep the integrity of application controls consistent.

Risk Assessment

An information security risk assessment is defined as "An initiative which identifies the nature and value of the Information Assets or Business Assets, the threats against those assets, both internal and external, the likelihood of those threats occurring and the impact upon the organization."[20]A well planned risk assessment program is key part of an information security program. Identifying key systems and data is the first step. A vulnerability assessment can then be performed on these to identify where each system has weaknesses. An information security team should regularly perform vulnerability assessments to determine the threats against that system as a part of a risk assessment program. Often the most difficult part of a risk assessment program is determining the probability of these threats being exploited and what may happen as a result of exploitation. Information security professionals should spend time researching exploits to their systems and incorporating that information into the vulnerability assessment program.

Monitoring

Monitoring should be very familiar to information security professionals. It plays an important part in maintaining a secure environment. The purpose of monitoring is to detect if something has gone wrong. One of the main principles of information security is "prevention is ideal but detection is a must."[21] Monitoring also plays a very important part in maintaining proper internal controls. It can help detect when data has been altered and therefore prevent it

[20] Information Security Glossary, http://www.yourwindow.to/information-security/gl_informationsecurityriskassessment.htm
[21]Computer World, http://www.computerworld.com/securitytopics/security/story/0,10801,82515,00.html

© SANS Institute 2005 Author retains full rights.

from becoming part of a financial report. There are two main types of monitoring, continuous monitoring and separate evaluations.[22]

Monitoring: Continuous Monitoring

Continuous monitoring is the type of monitoring with witch the information security team will be more familiar. The information security team can assist in implementing continuous monitoring by implementing technology. Services such as a network intrusion detection system to watch the perimeter networks to detect if entities external to the company have gained access to resources can be implemented. Host based intrusion detection tools can be set up on servers to monitor critical files to ensure that they are not modified by people who are not authorized to do so. A syslog server can act as a central repository for all the monitoring tools that are set up. This will make it easy to check for any unauthorized access. A syslog server can also be set up to automatically alert anybody who needs to be notified if certain resources are accessed or modified. Policies should be defined to determine how long each log should be kept. It is also the responsibility of the information security team to report any unauthorized access or modification of critical data to the management team, and to make sure that each event is properly documented for review.

Monitoring: Separate Evaluations

A separate evaluation is a type of monitoring that is usually done by a third party. While the information security team does not take part in the actual evaluation, one type of separate evaluation that information security will be involved in is the external vulnerability assessment or penetration tests. This is a test performed by qualified individuals who, upon being given very little information, try to gain access to the systems of a company. An information security team can take the results of such an evaluation and create an action plan for system administrators to follow. The remediation of problems discovered by this type of separate evaluation should be tracked, documented and communicated by the information security team.

Information and Communication

The information and communication element of COSO is really the element that ties all of the rest of them together. When generating the financial reports, much information is communicated within a company. In part, this element of is designed to provide controls over the information and the communication of it. At this level there are five things that the information needs to be and therefore, the controls need to protect, they are: appropriateness, timeliness, currency, accuracy, and accessibility[23]. Information security can

[22] IT Governance Institute URL: http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf
[23] IT Governance Institute URL:

© SANS Institute 2005

Author retains full rights.

protect these things by making sure the systems that provide for the communication of this information are stable and secure. Policies and procedures should be written to protect the data while it is being communicated and while it is at rest. If the information security team has implemented the internal controls of the other element of COSO, these five properties should be well protected.

The other level of information and communication that would involve the information security program is the communication of the security policy, any security violations and awareness. It is the responsibility of the information security professionals to make the company employees and management aware of the policies it has developed to make sure that they are followed. For example, if the policy states that no financial information should be sent via email and the employee is never told that such a policy exists, then the policy and the internal controls it is implementing would be ineffective. The information security team should report to management any security violations as soon as possible. They should also develop an awareness program that is designed to inform employees about current information security topics such as how to spot an Internet Virus in an email or friendly reminder not to write down their passwords on paper and slip in underneath their keyboard.

Conclusion

The Sarbanes-Oxley Act was written and adopted into law to protect the investors and employees of large public companies. Section 404 deals with the internal controls that need to be in place around the companies Information Technology systems. The PCAOB was established by the Sarbanes-Oxley Act and has recommended the COSO framework for outlining the internal control structure. The COSO framework does not have to be used directly, but all the elements addressed in the COSO framework should be addressed in whatever method is used. Information security in an organization plays a very important role in Sarbanes-Oxley section 404 compliance. Through the four elements of COSO, I have touched on a number of things an information security team can do to establish the internal control structure and ensure compliance with section 404.

References

http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf

"Highlights of the PCAOB Auditing Standard No. 2." Deloitte 15 Dec. 2004. <http://www.deloitte.com/dtt/article/0,1002,sid%253D2002%2526cid%253D43641,00.html >

"SEC Implements Internal Control Provisions of Sarbanes-Oxley Act; Adopts Investment Company R&D Safe Harbor." United States Securities and Exchange Commission. 8 Dec. 2004. <http://www.sec.gov/news/press/2003-66.htm>

Oxley, Michael and Sarbanes, Paul, "The Sarbanes Oxley Act of 2002." 8 Dec. 2004 <http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf>

"Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports." United States Securities and Exchange Commission. 14 Dec. 2004 <http://www.sec.gov/rules/final/33-8238.htm>

Bace, John, Caldwell, French, Logan, Debra, Leskela, Lane and Mogull, Rich. "New Sarbanes-Oxley Deadlines Give Big Firms a Break." Gartner. 3 Mar. 2004. 14 Dec. 2004 <http://www4.gartner.com/DisplayDocument?doc_cd=119939>

"IT Control Objectives for Sarbanes Oxley." IT Governance Institute. 14 Dec 2004.<http://www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives%282%29.pdf>

"Public Company Accounting Oversight Board; Order Approving Proposed Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements ("Auditing Standard No. 2")." United States Securities and Exchange Commission. 14 Dec 2004 < http://www.sec.gov/rules/pcaob/34-49884.htm>

"Treadway Commission.", The Institute of Chief Risk Officers. 14 Dec 2004. <http://riskinstitute.ch/00013184.htm>

"Sarbanes Oxley Act: 2004 Practical Guide for Management." PriceWaterHouseCoopers. 14 Dec 2004 <http://www.pwcglobal.com/extweb/service.nsf/8b9d788097dff3c9852565e00073c0ba/62672b99f219016085256f0e005c14fa/$FILE/SOActSection404Pract37AC61.pdf>

"Security Policy Project." SANS Institute. 14 Dec 2004 <http://www.sans.org/resources/policies>

References

© SANS Institute 2005 Author retains full rights.

"Information Security Risk Assessment." Information Security Glossary. 14 Dec 2004 <http://www.yourwindow.to/information-security/gl_informationsecurityriskassessment.htm>

Cole, Eric. "How to Secure Your Comapany." Computerworld. 26 Jun. 2003. 14 Dec. 2004 <http://www.computerworld.com/securitytopics/security/story/0,10801,82515,00.html>

© SANS Institute 2005, Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced