Global Information Assurance Certification Paper

SARBOX for Dummies

Sans Institute
GIAC Security Essentials Certification (GSEC)

Practical Assignment
Version 1.4c
Option 1

Submitted by
Garry Shaner
1/11/05

SARBOX for Dummies

Abstract

An Act of Congress was passed in 2002. The Act originated out of a need to protect stockholder interests in publicly traded companies and in the purist sense, to make sure that financial reporting to the SEC (Securities and Exchange Commission) were, in effect, reliable and accurate. The Act is known as the Sarbanes-Oxley Act and is often referred to as SARBOX or SOX. A very small section of the 66 page Sarbanes-Oxley Act (Sec. 404) has taken on a life of it's own and has effected IT security with more power than any other single issue.

As technology has evolved, so has the financial reporting structure and the controls that support it. So here we are - IT Security is at the forefront. One of the most difficult tasks that we may have as IT professionals is explaining technical processes in easy to understand logic that the rest of the organization can understand. The discussion that follows will explain in simple terms what Section 404 means, the basic concerns of Section 404, things that should be included to become compliant to Section 404, and its' effects on a company's organization.

Introduction

We should start with a review of Section 404. Read it carefully and pay close attention to the lack of specific detail. The lack of specific detail creates an atmosphere of subjectivity and potentially conflicting interpretation.

Section 404 of the Sarbanes–Oxley Act

"Sec.404. Management Assessment of Internal Controls

(a) Rules Required – The Commission shall prescribe rules requiring each annual report required by section 13(a) of 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."[1]

That's it? How does this affect IT? First of all Section 404 must be interpreted. Interpretation is subjective and creates the problem of everyone agreeing to the same interpretation. Interpretation is ultimately left to the registered accounting firm which is hired by the publicly owned company to attest to the accuracy of its' financial reporting.

Still confused? Let's work through it. First of all, publicly traded companies must file regular financial reports to the SEC. These reports must be reviewed and approved by a third party registered public accounting firm. The accounting firm must interpret the new Act and attest to the fact that the company is in compliance. The accounting firm is accountable to, and assisted by, the PCAOB (Public Company Accounting Oversight Board) and COSO (Committee of Sponsoring Organizations of the Treadway Commission). COSO is an older organization formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting[2]. It studied broad factors that could contribute to fraudulent financial reporting, and developed recommendations for the SEC and various other regulators. The PCAOB was created by the SARBOX ACT to oversee auditors of public companies.[3] The PCAOB is a non-profit private sector corporation that was created to establish auditing and related attestation, quality control, ethics, and independence standards and rules to be used by registered public accounting firms in the preparation and issuance of audit reports as required by the Act or the rules of the Securities and Exchange Commission.[4]

Let's not forget that the intention of the Act was to protect the accuracy and reliability of financial statements to protect public interests. Years ago, financial books consisted of pencils, paper ledgers, and adding machines. Today financial reporting is done almost completely relying on some sort of IT-related hardware or software. The accounting firm must now audit this financial trail and find proof that it is complete and secure.

Now let's cloud the issue again. Remember the phrase "assessment made by

[1] Sarbanes-Oxley Act of 002
http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf
[2] The Committee of Sponsoring Organizations of the Treadway Commission
http://www.coso.org/
[3] Public Company Accounting Oversight Board
http://www.pcaobus.org/
[4] American Institute of Certified Public Accountants
http://www.aicpa.org/info/sarbanes_oxley_summary.htm

the management of the issuer" from the ACT Section 404b? The term "management" means the company itself or someone hired by the company to perform work on their behalf. That means that the company must first conduct its' own assessment or hire another third party to conduct an assessment for them, which is reviewed by the original accounting firm. This entire process must be completely documented, reviewed, and approved in writing.

"If you want to understand Sarbanes-Oxley, go back to the Securities and Exchange Act of 1934. Markets were melting down; people didn't trust Wall Street or their banks. To restore order and confidence, they came out with the most sweeping legislation that Wall Street had ever seen. Sarbanes-Oxley is volume two of the Securities and Exchange Act. It's a shot across the bow to tell CEOs and CFOs that, yes, we will send you to prison and, yes, we will fine the heck out of you if we catch you doing something illegal. It's penance paid by the corporations because of certain CEOs using their corporations as personal piggy banks. The problem with Sarbanes is the way they wrote the law. In terms of records management, what's a record? A record is anything a litigator or the federal government says it is. The SEC is not going to be so stupid as to push themselves into a box and say, "You will do A, B and C." They say you will do certain things, such as an internal controls scenario. You will have the CFO sign off on the quarterly statement. You will have to restate your earnings if they are found to be not correct, things like that. Then they kind of leave it to you and your lawyers to interpret. Sarbanes-Oxley says you will do these things. It doesn't say how you will do these things."[5]

Basic Concerns

Compliancy to the Act is not optional for publicly traded companies. Companies failing to perform management self-assessment of internal control risks are subject to large penalties, potential prosecution, and may also jeopardize the publicly traded stock value.[6]

Processes and procedures of internal controls must be fully documented pursuant to subjective interpretation. Thousands of IT groups have spent the last couple of years scrambling to document and provide a history trail suitable for the auditors. Historically many of these departments have taken the backseat on the budget bus. IT does not generally generate revenue and has in many cases been a support department and viewed as overhead. Many IT groups have taken this in stride over the years and have still been able to develop reliable systems with adequate security systems while working within minimal budget restraints. The basic backbones are in place, the systems are running

[5] Web Extra: Sarbox Puts CIOs "On the End of the Spear" CIO Insight, May, 2004 by Debra D'Agostino
http://www.findarticles.com/p/articles/mi_zdcis/is_200405/ai_ziff127017
[6] "Feds Reach Out and Touch IT" July 10, 2003 By Sean Doherty
http://www.networkcomputing.com/1413/1413f17.html

and, at the least, minimal security is in place. However, many of these same groups have never had the resources to thoroughly document and authenticate their systems, processes and procedures. It should also be stressed that compliancy is not a one-time pass or fail but will be a continual process subject to annual audits.

There is an obvious dilemma that has been created that puts major pressure on the IT organization. IT security must have evidential documentation of compliancy with perhaps little or no historical financial support to provide it.

The basic areas of concern for compliancy to SARBOX 404 compliance are:

Documentation
Full documentation of company policies and procedures is required. This becomes the basis of compliance audits. Policies and procedures must address specific detail of the issues detailed below in regards to who, what, when, how and why. In addition to the written documentation, evidential matter must also exist that supports compliance to the policies and procedures. Documentation of unwritten policies and procedures is rather easy to develop. The historical evidential documentation of compliance to them is the difficult part if paperwork has not been an integral part of the security landscape.

Network Security
A basic network security backbone must exist and be fully documented. This would be comprised of, as a minimum, a firewall and a secure user authentication process. Documentation should consist of hardware, firmware, configuration file backups, and schematic details of logical connection controls.

Application Security
Application controls must be documented and reviewed regularly. User permissions to specific applications must be properly authorized and documented verification must be archived and regularly reviewed.

Antivirus Protection
The entire network must be protected from the ever-growing number of viruses. This includes remote users. Documentation must provide proof of effectiveness of virus definition updates and automated proactive protection.

Program Change Control
Controls must protect the reliability and authenticity of data. Proper authentication and verification of program changes such as version upgrades or service packs must be documented. Testing must exist and test results must be properly approved before changes can be released into the live data environment.

Password Security
User authentication should consist of complex passwords that cannot be

cracked by “brute force” within a reasonable amount of time. Cracking techniques and frequency must be documented and archive logs must be maintained and reviewed regularly. Procedures must be documented on user non-compliance issues and follow-up action.

Remote Access Security

Remote access privileges must be documented for proper authorization. This includes contractors who may only need random access. Modems, if used, must be documented and fully controlled. Wireless access, both locally or remotely, must be fully documented and securely controlled.

Application Program Change Control

Controls must protect the reliability and authenticity of data. Proper authentication and verification of program code changes must be documented. Testing must exist and test results must be properly approved before changes can be released into the live data environment.

Computer Equipment Security

Physical security systems must exist. Server rooms must be restricted to a business need basis. A history log must be available for review of access activity. The equipment must also be protected properly from other exposures such as fires, water damage and various other types of exposure.

Review of logs (Security, Application, and System) should be done on a regular basis and archived for evidential matter. Manual review of a large number of servers could easily consume a full time position. Automated collection and filtering of these logs is the key to not only the key to better utilization of IT personnel but also can provide security alerts via automated e-mail notification.

Segregation of Duties

Segregation of duties reviews most likely need to be split among the specific owner/managers of specific applications (i.e., order entry, accounts payable, accounts receivable, purchasing, payroll, etc). This is no small chore in many organizations that use legacy systems that are broken down into hundreds, if not thousands, of program objects. Specific owner/managers must be assigned to each program object.

A segregation of duties review of user access to sensitive information must be performed regularly and documented. Users should not have access to application functions that could potentially create a situation of fraudulent activity. This would vary greatly depending on the type of applications that are applicable to the business. In smaller organizations with limited resources it may make sense to have mitigating controls in place rather than hire additional personnel. Mitigating controls would consist of additional checks and balances that compensate for a deficiency in another area.

Training

Training is extremely important both for both IT personnel and the end user. Someone who has a complete understanding of their job function and the processes and procedures that are commensurate with the position must administer each layer of the security blanket. A simple typing mistake in a firewall configuration file, or a permission box checked wrong while setting up a user could easily become a security breach. End users must also be trained on the logic and ramifications of simple things such as taping their username and password on their keyboard.

Communication

Organizational structure should be communicated throughout the organization in a timely manner to provide for proper authorization approvals from appropriate individuals.

User profiles should be maintained in a timely manner. Employee terminations and responsibility changes must be communicated to IT in a timely manner so that unauthorized access potential is minimized.

Security violations should be thoroughly investigated and documented. This should encompass all aspects of security. Violations are a symptom of a process or procedure that may need adjustment.

Backups

Backup processes & procedures must be thorough and consistent to ensure original data state could be reinstated if circumstances require. Historical logs must be maintained as evidential matter. Safe storage at an offsite location is required. Historical backup reconstruction needs should be defined by conducting a Business Impact Analysis. The findings from the analysis will determine what an acceptable risk may be.

Business Impact

Again, we should keep in mind that our goal in this case is two-fold. We need to do our part to be in compliance with the Act but we must also bear in mind the impact on the organization. [A business impact analysis is usually quite simply, if something happens, what is the impact to the business?] The impact works both ways. Processes and procedures must ensure financial reporting data and related supporting IT systems are secured in such a fashion that the shareholder interests are protected and the probability of fraudulent access or catastrophic loss are minimized. But on the other hand, we must also be good stewards by creating logical and efficient safeguards that are cost effective. The cost of security must not outweigh the benefit of decreased probability. If you don't understand why something is being done ask enough questions so that you understand. If it doesn't make sense after you understand then you shouldn't be doing it.

Defense In-Depth
As we are all taught, defense in layers is quite effective. That seems to be the emphasis applied to the Section 404 compliance standards.

Tools
Numerous security and network monitoring tools will be needed to assist in compliance. These tools will become a daily part of your daily security routine. Specific tools will depend on your specific needs. Automation of the monitoring tasks should be implemented whenever possible. It is important to remember that documentation must be maintained so automated e-mail notifications or log generation leave an adequate evidential trail. In many instances a simple logbook with manual entries works just as well. Remember to use the good old common sense approach.

Platform Span
All processes and procedures should encompass the full spectrum of OS platforms. System base changes should not necessitate a change in process.

Process Flow
When you have completed your compliance structure step back and review the "total" process. It should have continuity of security assurance from cradle to grave. It is a good idea to use flow charts whenever possible.

Progress Tracking and Follow-up
Tracking and documentation must take place throughout the entire process of any issues that arise as being non-compliant. These issues must be collected from the start of the first audit and history of progress of the non-compliant issue must be tracked. This serves as a summary at the end of the process similar to a score card. Non-compliant issues may be minor or what is termed as a "Material Deficiency" or "Operational Deficiency".

Effects on the Organization

Effects on the company's organization could tend to have a great impact depending on prior processes and documentation requirements. Top-level management support will be necessary for needed process and procedure implementation and additional funding that may be required. User education will be required to explain documentation needs and requirements. Informal requests and changes regarding security issues will have to be replaced with documented authorization trails. Ongoing internal audits (Management Testing) will shift valuable resources. There are also those who subscribe to a darker theory in which the CFO now has the opportunity to seize greater control away from the CIO.[7] Any way that you look at it there may be a need for change. We must be aware of how the changes will effect the organization and plan

[7] "The Sarbox Conspiracy" by Christopher Koch, CIO 12/07/2004
http://www.cio.com.au/index.php/id;911250668;fp;2;fpid;2

accordingly.

Conclusion

Compliance to Section 404 of the Act can be condensed down to one simple statement - Use common sense and keep it simple. IT security can appear to be overwhelmingly technical, but each piece can be broken down and logically digested.

Processes must include attention to social engineering. Global communication is commonplace in this day and age. Long gone are the times when a local operator manually patched your call through across a shred "party-line" and you quickly recognized the voice on the other end. In today's fast paced world we need to be ever aware of the potential security breaches that can occur through someone falsifying their identity. Consider this example. The IT help desk receives a call from someone stating that he/she is the newly hired National Sales V.P. (a remote user) and that they are having problems connecting into the network remotely. The caller asks if his/her account has been accidentally locked out. The VP was just hired. The help desk person most likely will not recognize the voice. When the account is checked it is not locked out. The caller then responds with: I've been trying for over an hour to logon and I have some files that I need urgently, can we verify that I have the correct username and password? The Help Desk person will of course want to help the new V.P., so the username is given to the caller for verification. The caller responds with a confirmation that that is correct so it must be the password and then requests that it be reset while he is on the phone. What just happened here? Executive level data access was just handed over to your competition. The potential is also there for the caller to not only view and copy any data but to also erase any data that the real V.P. may need. This could easily go unnoticed. So what is the take-away here? Make sure that your security processes and procedures include steps to include identity verification.

Our job as security professionals is broad in scope and must include attention to these various arenas. Stopping a potential hack from the outside world is great but as we have heard for years, the greatest threat is from behind the firewall. It that respect, SARBOX 404 compliance makes perfect sense in that it primarily targets just those issues.

Being in the spotlight can be both good and bad. The good piece that Section 404 compliance brings to IT is that executive management may better understand additional benefits that comprehensive security brings to the business. An article in e-Week[8] reports that an AMR Research (an IT research company) survey reports that 85 percent of companies surveyed will require changes in IT and application infrastructure for compliance. Corporate spending

[8] "SarbOx: Chance to Advance" By eWEEK Editorial Board 3/1/2004
http://www.eweek.com/article2/0%2C1759%2C1542555%2C00.asp

to meet compliance standards is predicted to exceed $5.5B in 2004[9;10], this amount of spending alone will get the CEO and CFO's attention. IT projects that be have been previously shelved because of lack of funding and resources may fit nicely into the complete compliance package.

The bad piece that Section 404 compliance brings is the potential for Executive management to delegate compliance responsibility to the CIO / IT department without adequate understanding of the entire process and unwillingness to support necessary changes and additional funding that may be required.

Compliance to the Act will bring change to IT security sector that we have never seen before. How we manage that change is up to us.

Additional References and good reading:

"Sarbanes-Oxley Information Center", PricewaterhouseCoopers – CFO Direct Network®
http://www.cfodirect.com/

"Sarbox Puts CIOs "On the End of the Spear"", CIO Insight May, 2004 by Debra D'Agostino
http://www.findarticles.com/p/articles/mi_zdcis/is_200405/ai_ziff127017

"Sarbanes-Oxley SEC Rules & Regulations – Rule 404", Sarbanes-Oxley Financial and Accounting Disclosure Information
http://www.sarbanes-oxley.com/section.php?level=1&pub_id=SEC-Rules

"Sarbox" TheFreeDictionary.com, by Farlex
http://encyclopedia.thefreedictionary.com/Sarbox

"Sarbox 404 results in new fees for firms", by Leo John and Lee Weisbecker, From the September 10, 2004 print edition of Triangle Business Journal
http://www.bizjournals.com/triangle/stories/2004/09/13/story4.html

"Sarb-Ox Docs Cost a Lot More ..." Opinion by Mark Hall 9/13/2004
http://www.computerworld.com/softwaretopics/software/story/0,10801,95859,00.html

[9] "2004 Sarbanes-Oxley Spending and Project Planning Trends" 2/11/2004 By John Hagerty, Heather Keltz, Shawn Fitzgerald
http://www.amrresearch.com/Content/View.asp?pmillid=16705&docid=810

[10] "Still Sweating Over Sarbox" By Pam Baker CIO Today 8/9/2004
http://cio-today.newsfactor.com/story.xhtml?story_title=Still-Sweating-Over-Sarbox&story_id=26233

"The Sarbanes-Oxley Act of 2002", Sox-Online
http://www.sox-online.com/

"Summary of Sarbanes-Oxley Act of 2002 -- Section 404: Management Assessment Of Internal Controls.", AICPA (American Institute of Certified Public Accountants)
http://www.aicpa.org/info/sarbanes_oxley_summary.htm

"Sarbanes-Oxley: A Funny Thing Happened on the Way to Compliance", by Ben Worthen, Reprinted From: CIO 1/30/2004 article ID: 3266
http://enterprisesecurity.symantec.com/content.cfm?articleid=3266&EID=0