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.

The Impact of the Sarbanes Oxley Act on IT Security

This paper goes on to define the Sarbanes-Oxley Act and its requirements, a framework for compliance, and specific IT security areas that must be considered during compliance efforts. According to the Deloitte and Touche Information Security and Privacy Group, "there is a lack of clarity on the impact of multiple governance initiatives (including Sarbanes-Oxley) on information security".4 By not specifically addressing IT security, the Act leaves room for interpretation.

Copyright SANS Institute
Author Retains Full Rights

AD

GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b
October 18, 2003
Scott Byrum

The Impact of the Sarbanes-Oxley Act on IT Security

Abstract

As if organizations needed another reason to be more cognizant of the importance that IT security plays in a successful business operation. The recent Blaster worm outbreak, the blackout in the Northeastern United States in August 2003, and other similar events have helped solidify IT security's spot on the corporate map[1]. Yet, another event, the Sarbanes-Oxley Act of 2002, will be responsible for further promoting the significance of security to corporate executives. When drafted, the writers of the Act did not have IT security in mind.[2] As time has passed, and compliance efforts have been initiated, organizations have begun to realize that without a certain level of assurance regarding IT security controls[3], compliance is not possible.

This paper goes on to define the Sarbanes-Oxley Act and its requirements, a framework for compliance, and specific IT security areas that must be considered during compliance efforts. According to the Deloitte and Touche Information Security and Privacy Group, "there is a lack of clarity on the impact of multiple governance initiatives (including Sarbanes-Oxley) on information security".[4] By not specifically addressing IT security, the Act leaves room for interpretation. The information presented below is based on the research I conducted and represents my interpretation of the effects of the Sarbanes-Oxley Act on IT security. In the near future, as compliance efforts progress, new standards and best practices relating specifically to IT security controls in a Sarbanes-compliant environment will be released. This paper is not intended to provide reference to all the controls that should be considered during compliance efforts. Its purpose is to help you, the reader, become more familiar with Sarbanes requirements and their potential affect on the IT security control structure. Regardless of whether the IT security controls mentioned below are required of your organization by the Act, their existence can lead to more secure business processes and ultimately, a better bottom-line.

The Sarbanes-Oxley Act of 2002

The purpose of the Sarbanes-Oxley Act of 2002 (SOA) is to restore confidence in the integrity of the financial reporting process at publicly traded companies. Its adoption

[1] Roberts, p.1.
[2] Regan, p.1.
[3] Defined as a policy, procedure, or practice whose purpose is to ensure that a desired goal or objective will be achieved. ISACA, 2003 CISA Review Manual, p.30.
[4] Power, p.12.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

into law was influenced by recent high profile accounting scandals at firms such as Enron and WorldCom. In Section 302 of the Act, the SEC requires that executive officers at each publicly traded company, usually the CEO and CFO, certify all financial reports that are required by Section 13(a) or 15(d) of the Securities Exchange Act of 1934 before disclosure to the public. By certifying, the executives are stating that they have reviewed the filing for accuracy and that they have disclosed any significant deficiency in the internal control structure and/or any fraud perpetrated by any individual with a significant role related to internal controls at the organization. The requirements of the section went into effect for quarterly financial reports filed on or after August 12, 2003. Penalties of misstatement may include executive jail time and/or personal fines.[5] There is no wonder why the act has caused such a buzz and influenced executives to begin spending substantial dollars on SOA compliance.

To comfortably certify the financial statements, executives will require assurance that the data used in the company's financial reports is accurate. All organizations rely on controls to promote sound business processes including those that affect financial reporting data. Section 404 of the Act, which goes into effect as early as June 14th, 2004, requires executive management to file an internal control report with its annual report on Form 10-K, the form that provides an annual overview of the company's business. Within the control report, management is required to make judgments regarding the effectiveness of the internal control structure over financial reporting. This includes the identification of any significant deficiencies in controls over the financial reporting process. Prior to public disclosure, the company's external auditor must confirm the validity of the assertions that management makes in the report.[6] Exhibit 1 illustrates the required sections of the internal controls report. With a strong control structure in place and functioning properly, executive management can feel confident that the data it reports in the financial statements is accurate and truly reflects actual operations. Only then can certification occur and compliance be achieved.

IT Security's Role

Each organization that is affected by the Sarbanes-Oxley Act has some level of reliance on automated information systems to process and store the data that is the basis of financial reports. The Act requires these organizations to consider the IT security controls that are in place to promote the confidentiality, integrity, and accuracy of this data. Specific attention should be given to the controls that act to secure the corporate network, prevent unauthorized access to systems and data, and ensure data integrity and availability in the case of a disaster or other disruption of service. Also, each application that interfaces with critical financial reporting data should have validation controls such as edit and limit checks built-in to further minimize the likelihood of data inaccuracy. A properly designed IT security control structure that is operating effectively is a critical piece to the Sarbanes-compliance puzzle. Its existence will

[5] Bolles, p.1.
[6] Protiviti, p.13.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Exhibit 1[7]

Articulates management's responsibilities to establish and maintain adequate internal control over financial reporting.

XYZ Company
Internal Control Report
for fiscal year 2004

To ensure accuracy of the data reported to the public, it is XYZ management's responsibility to establish and maintain an effective internal control structure over all processes that affect financial reporting data.

Defines framework used by management for evaluating internal control structure.

To evaluate the current control structure at XYZ, management has worked closely with the Internal Audit department to ascertain the design and operational effectiveness of all relevant controls. A web-based tool has been deployed to assist with compliance efforts and serves as repository for required documentation.

Overall, the control structure at XYZ is very effective. Listed below are specific assertions regarding the control structure. Following the assertions, are the material weaknesses that were noted during management's assessment.

Assertions (as of 12/01/04):

- Access to data assets through computer applications and systems is adequately controlled.
- Data availability is ensured by a thoroughly tested contingency plan.

Management's assessment of control structure as of a point in time (in this case 12/01/04). Includes assertions and material weaknesses.

Material Weaknesses in Control Structure (as of 12/01/2004):

- Limit checks are not used by AP system to validate input data.

Attestation of external auditor.

XYZ's external auditors, 123 Public Accountants, have attested to and reported on the assertions and material weaknesses noted above.

Note: the purpose of Exhibit 1 is to illustrate the different sections required in the internal controls report. It may serve as a guide but should not be used in actual practice without further research.

[7] Section descriptions are taken from Protiviti, Guide to the Sarbanes-Oxley Act, p.13.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

provide the certifying officers piece of mind when signing off on the accuracy of financial reports.

Complying with Sarbanes-Oxley[8]

Before examining specific IT security controls, it is critical that an organization have an approach to guide overall Sarbanes compliance efforts. In many cases, this involves the Internal Audit department taking the lead and working alongside business process owners from each process that has a direct effect on financial reporting data. Results are communicated to a steering committee, which acts as a governing body over compliance efforts.

Initially, an entity-level assessment should be performed to assess the control environment at the corporate level. This assessment should focus on controls that are funneled down from atop the organization with the purpose of ensuring the integrity of financial reporting data. In terms of information security, the entity-level assessment should focus on areas such as corporate network security and disaster recovery planning. The results of the entity-level assessment have bearing on the scope of the next phase, analyzing process-level controls. If testing reveals that the control environment at the entity-level is strong, it is likely that the control structure at the process-level will also be strong. Thus, less analysis may be required at the process-level. For example, if a disaster recovery plan exists and sufficiently covers all critical systems, less analysis and testing is required at the process-level to ensure that specific data, i.e. the payroll file or the accounts receivable file, can be recovered after a disaster.

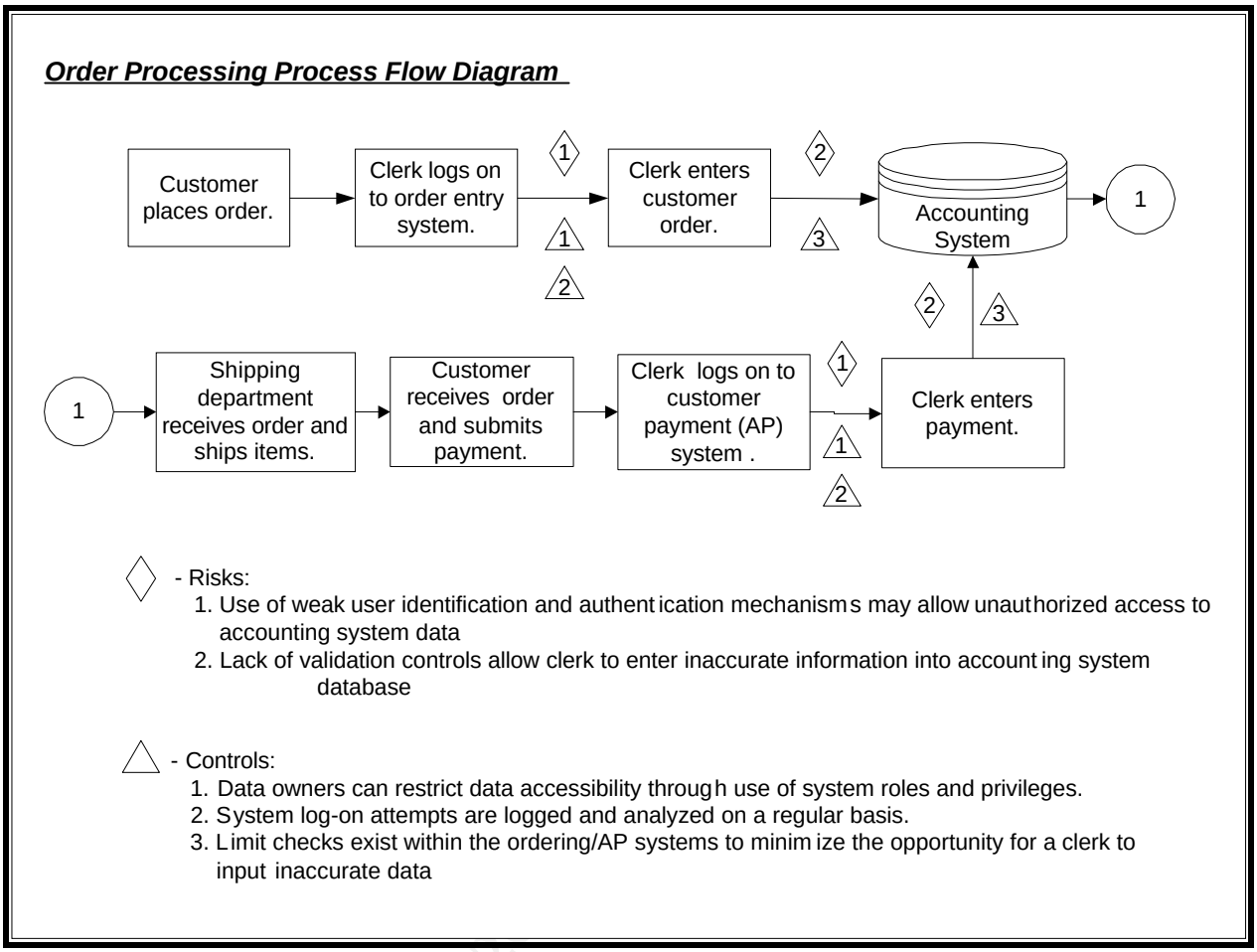
During the process-level assessment, the control structure of all processes that have a significant influence on financial reporting data must be documented and analyzed for effectiveness. Business process owners are relied upon to share process knowledge, which serves as the basis for documentation. At the process-level, documentation involves creating diagrams and/or narratives that outline the process steps, as well as the individuals, applications, and databases that are involved. Once the process has been defined, risks and controls can be plotted. Exhibit 2 represents a process-flow diagram for a typical order processing process.

After all critical processes, and the corresponding risks and controls, have been diagramed, the system of controls must be tested for design and operational effectiveness. It is important that the controls are considered in unison rather than on an individual basis. It is possible for the strength of one control to compensate for the weakness of another control. Exhibit 2 identifies three IT security controls that are in place to ensure the integrity of data involved in the order processing process. Respectively, controls 1 and 2 refer to access controls at the application level and the logging and monitoring of system log-on attempts. If, at the entity-level, the organization has strong access and logging controls, detailed testing may not be required to confirm the effectiveness of controls 1 and 2 at the process-level.

[8] Protiviti, pgs.53-78.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Exhibit 2



Conversely, control 3, limit checks, is not relevant at the entity-level and will require testing to confirm its operating effectiveness. To test for design effectiveness, the auditor may compare the design of the control to standards and/or industry best practices. For example, if the accounting system in question were SAP, the auditor would compare control 3, the organizations implementation of an SAP limit check, to the best practice for SAP limit checks. If the control is properly designed, it is then tested to ensure that it is operating effectively. This test would involve accessing the ordering/AP systems and ensuring that the limit checks actually do validate a clerk's input based on an established set of criteria. If the control passes both the design and operational tests, it may be deemed effective in terms of minimizing the organizations exposure to the corresponding risks. In this case, the limit check (control 3) minimizes the risk (risk 2) that a clerk will enter inaccurate data into the ordering/AP systems.

In most cases, the assessments at the entity and process-level will reveal that some controls are designed and operating effectively and others are not. Controls that have a significant deficiency that is not overcome by the presence of a compensating control are included in a remediation plan. This plan includes information such as the control name, the corresponding process and responsible party, the issue that is causing the control deficiency, an action plan for remediation, and a deadline. The organization

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

should prioritize the remediation plan so that the most important control gaps are addressed first. By fixing these controls, each of which is in place to guarantee the integrity of financial reporting data, the executives can be fully confident when certifying the accuracy of the public financial statements. If no material control weaknesses exist, investors will favorably receive management's internal control report. And, voilà, the organization is compliant with Sections 302 and 404 of the Sarbanes-Oxley Act!

IT Security Controls – Standards and Best Practices

To measure the effectiveness of the existing control structure during the entity-level assessment, some standard is needed to act as a benchmark. Several best practice frameworks can assist in compliance efforts including the COSO (Committee of Sponsoring Organizations) Integrated Framework, the COBIT (Control Objectives for Information and related Technologies) framework, the ISO 17799 standard (Code of Practice for Information Security Management), and the ITIL (Information Technology Infrastructure Library). The COSO framework has been identified by the SEC as a good starting ground for Sarbanes compliance. It addresses accounting controls over business operations and the financial reporting process; however, it does not make specific reference to IT controls. COBIT, which is published by ISACA (the Information Systems Audit and Control Association), was created to address IT controls not specifically mentioned in the COSO framework.[9] Currently, it is the standard of choice in terms of a driving guideline for the entity-level assessment focusing on IT security controls. The COBIT framework defines several IT control objectives in each of four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. Recently, ISACA has realized the need to integrate other standards, including ISO 17799 and ITIL, into COBIT to create a framework specifically designed to address IT controls in the post-Sarbanes-Oxley world. The projected completion date for this guideline was the second quarter of 2003[10].

Entity-Level IT Security Controls

At every organization, regardless of size, the data that is the basis for financial reporting relies on information systems for processing and storage and the corporate network infrastructure for accessibility. Hence, it is important that a proper control structure is in place at the entity-level to support all business processes. Each organization will have a unique control structure based on its reliance on information technology and on the business environment in which it operates. Although there is no right or wrong answer as to the IT security controls that must be in place at the entity-level, there are several areas that all organizations must address during SOA compliance efforts. Three of these areas are infrastructure security, access control, and contingency planning[11].

[9] Hoffman, p.1.
[10] ISACA, COBIT Mapping, p.1.
[11] Barrett & Stanek, p.1.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Infrastructure Security

The corporate network is responsible for the transport of financial reporting data and the transactions that affect this data to and from network hosts. In many environments, the corporate network extends to customers, business partners, and suppliers. To ensure that critical data is not intercepted, altered, or accessed during transmission requires a strong control structure around the corporate network infrastructure. COBIT defines several controls related to network security in control objective 5, Ensure Systems Security, of the Delivery and Support (DS) domain:

> **5.16 Trusted Path**
> *Control Objective*
> Organizational policy should ensure that sensitive transaction data is only exchanged over a trusted path. Sensitive information includes security management information, sensitive transaction data, passwords, and cryptographic keys. To achieve this, trusted channels may need to be established using encryption between users and systems, and between systems.[12]

In the context of Sarbanes-Oxley, the data used for financial reporting is sensitive information. Preventative and detective controls need to be established to ensure that this data is secure as it is transferred from source to destination. It is necessary for the organization to have a clear understanding of the physical topology of its network as well as the protocols used for communication. A network diagram is an effective approach to defining all network access points and the breakdown of the network into public, semi-public, and private domains. In terms of SOA compliance, private network resources are of the greatest concern.

Any transfer of financial reporting data from an internal database server to a requesting host should occur over a secure channel. Preventative controls should act to secure the network infrastructure and prevent unauthorized access. The first line of defense is an effective password management program that requires the use of strong passwords (discussed thoroughly in access control section below). Any access granted to private network resources over the Internet should occur over a properly configured VPN that utilizes encryption. Encryption may also be used for internal transfers, depending on the sensitivity of the information. Third-party access to private resources via a modem introduces several security issues and should be used with caution. Another essential preventative control is the use of firewalls, which filter traffic between the private network segment and the semi-public and public segments (see control objective 5.20 below). Finally, physical security controls should exist to prevent outsiders from gaining access to an internal network connection or to the data center.

In case the firewall fails to prevent unauthorized access, it is critical that detective controls are in place to detect inappropriate traffic. An intrusion detection system should log activity and be regularly monitored to identify suspicious network traffic in a

[12] This and each COBIT control objective to follow was taken from ISACA, COBIT Control Objectives 3rd Edition, pgs.96-103.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

timely manner. At the application-level, the organization should also consider logging traffic to the database servers that store financial reporting data. Logs can be analyzed to detect fraud, including fraud by individuals who have internal control responsibilities, which must be disclosed according to Section 302 of the SOA. Combined together, these preventative and detective controls ensure the existence of a trusted path over which financial reporting data can be securely exchanged.

5.20 Firewall Architectures and Connections with Public Networks

Control Objective

If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of service attacks.

As stated earlier, many organizations provide access to financial reporting data to outside entities via a VPN over the Internet. A firewall at the front door of the internal corporate network is an effective way to limit access to this data. Filtering rules, based on IP address, port number, and protocol can be implemented to determine who can access which resources. For example, an organization may want to provide its major suppliers access to its order data but not to other critical systems such as accounts payable, inventory, etc. A way to implement these sorts of access constraints is via a firewall's filtering rules.

Firewalls offer additional functionality that is relevant to a Sarbanes-Oxley compliant control environment. For instance, most firewalls have a logging capability that is the basis for intrusion detection and is critical in investigating fraud.[13] Logs can reflect network traffic that was permitted as well as traffic that was denied. Firewalls are also capable of data encryption, which can further promote data confidentiality, integrity, and nonrepudiation. Data on its way to a supplier via the Internet can be encrypted by a firewall, making it unintelligible to an unauthorized party. Finally, a properly configured firewall is capable of blocking viruses and worms at the front door, which helps ensure the availability and accuracy of critical data. While firewalls are a very powerful and very necessary piece of a secure network, even they can be defeated. But, by following a 'Defense-in-Depth' strategy, which involves adding other controls to complement the firewall, the organization can further ensure the accuracy of financial reporting data.

Access Control

If designed and implemented effectively, access controls will assist in governing which users are able to view and/or edit financial reporting data. An effective access control program restricts access to critical data to only those users with a legitimate need. The program should address each of the following areas: user account provisioning, account maintenance and monitoring, account revocation, and password management. At the entity-level, the access control program applies to logging on to the corporate network

[13] Cole, p.673.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

and to mission critical systems such as an Enterprise Resource Planning (ERP) system. In control objective 5, Ensure Systems Security, of the Delivery and Support (DS) domain, COBIT defines several controls related to access control/user management:

> **5.2 Identification, Authentication, and Access**
> *Control Objective*
> The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication, and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-on's. Procedures should also be in place to keep authentication and access mechanisms effective (e.g., regular password changes).

For accountability purposes, the scheme used for user ID's should be consistent across the organization and should clearly identify the user. A common example of such a scheme is an individual's first initial of his/her first name followed by his/her last name and department ID. Based on the principle of least privilege, the user should be authorized to access and transact with only the data necessary to complete his/her duties. Also, to reduce the opportunity for fraud, segregation of duties should be considered when determining user authorization. For instance, a system administrator should not be responsible for monitoring system log files. Access to these files would allow the admin to cover his tracks in the case of fraud.

Authentication of users is also a big concern that should be addressed in an effective access control program. As mentioned previously, a user authentication mechanism requiring the use of strong passwords can act as the first line of defense against unauthorized access. Corporate policy and password filters should enforce a password length requirement, often eight characters, and should necessitate the use of a mix of alpha and numeric characters as well as symbols and other special characters. Users should be required to change their passwords after a certain time period and should not be able to revert back to recently used passwords. Also, users should be cautioned about disclosing passwords and about the risks of storing written passwords at their desks. Finally, it is critical that the file containing the passwords of a system's users is stored in ciphertext and that passwords are encrypted as they traverse the network. By implementing strong identification, authentication, and authorization controls, the organization has added another layer of protection for financial reporting data. To complement these controls, an effective means of user account provisioning and revocation should exist.

> **5.4 User Account Management**
> *Control Objective*
> Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending, and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls, and procedures for information systems and contracts between the parties.

The organization should define a standard approach for data owners to follow when provisioning users. One of the more popular, the role-based approach, requires that the data owner assign a user to a group based on the duties he/she is responsible for. Initially, the user inherits all privileges associated with the group, although the data owner may be able to further restrict access at the local (user) level. Regardless of the approach used, the organization should ensure that the provisioning process is effective at giving users the appropriate access.

Equally as important as effective provisioning, are the monitoring and revocation processes. The monitoring process involves logging and analyzing access attempts to identify unusual situations including failed log-on attempts and log-on attempts during non-business hours. As mentioned previously, effective monitoring can help identify and prevent fraudulent activity. It is also critical that the organization have a revocation process in place by which user access to critical systems may be quickly disabled. The speed of the revocation process is important in certain situations such as when dealing with terminated employees or compromised user accounts. In both cases, individuals with unpleasant intentions may attempt to access and deface financial reporting data.

Business Continuity Planning

A major purpose of a business continuity plan is to ensure the integrity and availability of crucial data after a disaster or other disruption of service. In many environments, thousands of transactions that affect financial reporting data occur each day. It is critical that the organization protects stored financial reporting data in the case of a disruption as well as guarantee that transactions that occur during downtime are properly accounted for. COBIT defines several controls related to contingency planning in control objective 4, Ensure Continuous Service, of the Delivery and Support (DS) domain:

> **4.1 IT Continuity Framework**
> *Control Objective*
> IT management, in cooperation with business process owners, should establish a continuity framework which defines the roles, responsibilities and the risk-based approach/methodology to be adopted, and the rules and structures to document the continuity plan as well as the approval procedures.

Developing a business continuity plan involves several steps including the identification of threats, the prioritization of assets based on criticality, and the development of a detailed plan. When creating the disaster recovery plan (DRP), the IT component of the business continuity plan, there are certain items that must be addressed. First and foremost, the DRP should address the steps necessary to effectively restore critical

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

systems after an interruption with minimal impact on data integrity and availability. Specific consideration should be given to backup procedures for critical data, and to network and server recovery. Depending on the magnitude of the event, the organization may have to move to a new site and/or procure new hardware and software. The logical and physical security in each of the possible post-disaster operating environments should be addressed. Finally, the DRP should identify the specific responsibilities of each team involved in the recovery including, but not limited to, the damage assessment team, the network recovery team, and the relocation team[14]. After a plan has been established, it must be tested for adequacy and maintained to reflect changes in the organization's business environment.

4.5 Maintaining the IT Continuity Plan

Control Objective

IT management should provide for change control procedures in order to ensure that the continuity plan is up-to-date and reflects actual business requirements. This requires continuity plan maintenance procedures aligned with change management and human resources procedures.

Changes in technology including system upgrades and network changes may alter the requirements of the DRP. Management should define a procedure for updating the business continuity plan in a timely manner to reflect all relevant changes. The procedure should hold specific individuals responsible for initiating and carrying out the changes and should identify the means by which changes will be communicated across the organization.

4.6 Testing the IT Continuity Plan

Control Objective

To have an effective continuity plan, management needs to assess its adequacy on a regular basis or upon major changes to the business or IT infrastructure; this requires careful preparation, documentation, reporting test results and, according to the results, implementing an action plan.

It is critical that the effectiveness of the continuity plan be validated through regular testing. Testing should ensure that the plan accomplishes its objectives and allows the organization to recover in a timely manner. Specifically, testing should ensure that all involved individuals are aware of and are able to carry out their responsibilities, that critical systems and the supporting infrastructure can be efficiently restored, and that off-site storage of data and software is synchronized with the current live environment. Test results should be maintained and referred to during subsequent tests to ascertain whether previously identified problems have been resolved.

[14] ISACA, 2003 CISA Review Manual, pgs.281-283.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Process-Level IT Security Controls

During the process-level control assessment, processes that affect financial reporting data are documented in flow diagrams and/or narratives. The documentation will identify the applications that are involved in critical processes. In many environments, these applications are a component of an ERP system such as SAP, Oracle, Peoplesoft, or J.D. Edwards. Several IT security controls should exist at the application level to ensure the integrity of financial reporting data. These include preventative access controls, which allow data owners to restrict user privileges, detective access controls, such as the logging of unsuccessful log-on attempts, validation controls, including edit and limit checks, and the encryption of certain data and transactions.[15] Strong controls at the application level will complement the entity-level control structure and act to further ensure the accuracy of financial reporting data.

The COBIT framework does not refer to specific application controls. As a result, an alternative framework is required to analyze the security controls around existing applications. The System Development and Maintenance section of the ISO 17799 standard, the Code of Practice for Information Security Management, "provides specific security objectives, risks, and controls relevant to application security."[16] Also, books and other research on the security of specific ERP systems may be useful when assessing the IT security control environment at the process-level.

Summary

The Sarbanes-Oxley Act of 2002 requires impacted organizations to analyze the design and operating effectiveness of the controls in place at both the entity and process levels that act to ensure the accuracy of financial reporting data. Although its ingredients will vary by organization, the presence of a strong IT security control structure is crucial to Sarbanes compliance. Without it, management will have to either disclose a significant deficiency in the corporate internal control structure or expose the organization's executive officers to personal liability in the case that they certify inaccurate financial statements. While the legislation may not have been specifically written to address IT security controls, as compliance efforts progress, the impact of the Sarbanes-Oxley Act on IT security will be substantial.

[15] Tuteja, p.1.
[16] Greene, p.2.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

Barrett, Jeff & and Stanek, Steve. "Technology Critical to Sarbanes-Oxley Efforts". URL: http://www.protiviti.com/knowledge/current_feature/091203.html (23 Sept 2003).

Bolles, Gary A. "Sarbanes-Oxley: Comply with Me". CIO Insight. 8 August 2003. URL: http://www.cioinsight.com/article2/0,3959,1217378,00.asp (23 Sept 2003).

Cole, Eric, et al. SANS Security Essentials with CISSP CBK Version 2.1. SANS Press, 2003. 289-825.

Greene, Fredric. "Compliance with Sarbanes-Oxley and SAS 94: The Critical Role of Application Security in Internal Control". URL: http://www.nysscpa.org/committees/emergingtech/sarbanes_act.htm (23 Sept 2003).

Hoffman, Thomas. "Sidebar: Guidelines Meld IT Governance, Sarbanes-Oxley Compliance". ComputerWorld. 14 July 2003. URL:http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,82991,00.html (23 Sept 2003).

Information Systems Audit and Control Association (ISACA). 2003 CISA Review Manual. Rolling Meadows: ISACA, 2003. 196-387.

Information Systems Audit and Control Association (ISACA). COBIT Control Objectives 3rd Edition. Rolling Meadows: ISACA, 2000. 96-103.

Information Systems Audit and Control Association (ISACA). "COBIT Mapping". URL: http://www.isaca.org/Content/ContentGroups/Research1/Projects/ISACF_Research_Current_Projects.htm#cobit (23 Sept 2003).

Internet Security Systems. "Security Best Practices for Sarbanes-Oxley Act Compliance". URL: http://documents.iss.net/marketsolutions/ISSSarbanesOxleyBrochure.pdf (23 Sept 2003).

Power, Richard. "2003 Global Security Survey". URL: http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf (29 Sept 2003).

Protiviti Inc. Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements. Second Edition (2003): 10-102.

Regan, Keith. "The Non-Security Security Law". Information Security Magazine. May 2003. URL: http://infosecuritymag.techtarget.com/2003/may/oxley.shtml (23 Sept 2003).

Roberts, Paul. "Blaster, blackout combination boon for some". IDG News Service. 18 Aug 2003. URL: http://security.itworld.com/4356/030818blasterboon/ page_1.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Tuteja, Akhilesh. “Enterprise Resource Planning: Can it be risky? – Part 2”. 15 June 2000. URL: http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=83 (24 Sep 2003).

Williams, Brett. “Sarbanes-Oxley – Another Driver for Business Continuity Management”. URL: http://www.disaster-resource.com/articles/03p_029.shtml (23 Sept 2003).

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

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

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**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**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 Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**