

## SOX Compliance Requires an Effective Security Program



*Prepared for*  
**The IT Security Community and our Customers**

*Prepared by*

Lunarline, Inc.  
1875 I ST, NW, Suite 500  
Washington, DC 20006  
[www.lunarline.com](http://www.lunarline.com)

**20 February 2007**

**By Matt Metheny, PMP, CISSP, CAP, CISA**

## **Abstract**

This paper discusses the impact an effective security program has on Sarbanes-Oxley (SOX) compliance. SOX requires an organization's leadership to ensure the accuracy of their financials reporting, and actively measure implemented controls required to mitigate potential anomalies that could lead to errors in the financial statements. The characteristics of a good information security program will provide the governance, and security management foundation for the rigorous demand placed on organizations when creating a framework to meet SOX compliance. Over the past several years, organizations have become more efficient in meeting many of the critical compliance requirements, and have begun to turn to IT to automate the manual activities, and alert senior management when a compliance issue arises. As a result of SOX compliance, the incorporation of industry standards and processes are enabling organizations to become more mature and efficient.

## Table of Contents

Abstract .....	2
Introduction to SOX.....	4
History Sarbanes-Oxley also known as SOX .....	4
SOX 101.....	4
SOX, IT Governance and Information Security Management .....	5
Components of a Good Information Security Program .....	6
How SOX Compliance is Achieved through Good Information Security Management ....	9
Information Security Roadmap.....	9
Linking Business and IT Layers with SOX Requirements .....	9
Selecting Internal Controls .....	10
The Current Trends in SOX Compliance.....	11
The Cost of Compliance .....	11
Steps to Compliance .....	11
Conclusion .....	13
References.....	14
Appendix A: Security Lifecycle .....	15

## Introduction to SOX

### History Sarbanes-Oxley also known as SOX

The Sarbanes-Oxley Act of 2002 (SOX) was signed into law in July 30, 2002. The SOX legislation was born out of years of corporate scandal and was seen as a overarching guideline to ensure corporations were being run correctly. Although the law passed was titled Sarbanes-Oxley Act of 2002, the origins of this legislation were actually a merger from two different bills submitted to the House and Senate for approval. One of the bills was named the Corporate Auditing Accountability, Responsibility and Transparency Act (CAARTA)<sup>1</sup> and the other was known as the Public Company Accounting Reform and Investor Protection Act<sup>2</sup>.

The SOX legislation was the result of the corporate scandals of the late 1990's to 2001. One such company, Enron, was the centerpiece for one of the most noteworthy and recognizable faces of modern corporate accounting practice failures. Enron's scandal started with the approval of a market-to-market accounting practice by Securities and Exchange Commission (SEC) and followed by deliberate debt hiding schemes that were designed to prevent disclosure of losses to the SEC and the public through corporate quarterly filings. The limitations in internal controls and the oversight by senior management was a major reason for the fall of Enron. The false reporting of accounting anomalies given by many major corporations eventually hurt the public's confidence in the Governments ability to properly monitor publicly traded companies.

### SOX 101

In this section, we will discuss the basics of SOX, including the major provisions that were mandate to be apart of the new corporate governance processes. SOX compliance primarily affects both large and small publicly traded companies, but the constructs of SOX (accuracy of financial reporting and management of IT-related internal controls) should be integrated into all businesses to ensure overall good corporate governance. As part of the compliance mandate, the legislation contains provisions that ensure the accuracy of disclosed financial reports, auditing and certification of internal controls by outside auditors, reporting requirements for financial changes, and the retention of financial and auditing documents.

Let's begin our discussion into the intricacies of SOX by discussing the provisions that make up the legislation as the basis for further understanding how security plays a significant role in helping the organization meet the requirements of SOX. According to the Sarbanes-Oxley Act of 2002, the major provisions that apply to publicly

---

<sup>1</sup> "HR 3763" (U.S. House of Representatives, 2002)

<sup>2</sup> "The Public Company Accounting Reform and Investor Protection Act was signed into law on July 30, 2002, and has been referred to as "the most far-reaching reforms of American business practices since the time of Franklin Delanore Roosevelt." The law is now known as the "Sarbanes-Oxley Act," name for the principal sponsors of the legislation" (United States Senate, 2004).

traded companies (large and small) that file reports with the SEC, foreign private issuers, and companies with only registered debt securities are as follows:

- § Section 101-109: Creation of the Public Company Accounting Oversight Board (PCAOB)
- § Section 201-209: Assurance of Auditor Independence
- § Section 301-308: Enforcement of Corporate Responsibility
- § Section 401-409: Enhanced Financial Disclosures
- § Section 901-906: Enhanced Criminal Penalties

These provisions are high-level requirements that mandate the establishment of corporate oversight and governance. The discipline outlined in the SOX legislation should be an inherent part of every organization regardless of the status (e.g., public or private). The requirement of SOX helps organizations improve on the processes that report on financial information through good corporate governance. The activities required by SOX should be consistently applied uniformly across the organization, therefore delivering a basic groundwork for measuring the overall effectiveness of financial reporting internal controls through regular auditing. This effectiveness can be historically captured, and provide a benchmark for organizations to gauge their performance against competitors. The organization can also show how they guarantee accurate reporting of financial through these quality metrics, therefore demonstrating the linkage between the effectiveness of the organization's financial reporting process and their IT infrastructure.

## **SOX, IT Governance and Information Security Management**

There are essential elements within SOX that directly relate to IT governance and information security management. The SOX legislation specifically directs organizations to develop a corporate governance structure that ties the business processes to IT components, and requires routine quarterly tests of these IT controls. As part of the compliance process, the "SOX auditor must examine many IT activities, such as controls on financial applications, data retention, and security. IT managers must establish procedures to deal with the business implications of IT activities and implement the same control found in non-IT areas of business" (Waschke, 2005).

SOX compliance, as noted in section 404, requires a company and its auditor's to attest and report on the effectiveness of the internal controls. As part of the auditing of internal controls, the IT controls of financial systems must be assessed to ensure they are adequate and operating effectively. This controls effectiveness will be evaluated against the documented processes and design specifications for the assurance of financial accuracy. The documented controls should specifically address how the controls were implemented and its function within the financial information system, or related processes.

There are many standards that relate to IT governance (e.g., ITIL, COBIT) and information security management (e.g., ISO 17799, ISO 27001). The selected standards

that are applied within an organization must be implemented in accordance with the overall processes contained within the controls framework such as that released by the Committee of Sponsoring Organizations (COSO)<sup>3</sup>. As part of the organization's SOX compliance, the corporate management must document the control framework that will be incorporated to ensure internal control management. After selection, the control framework must be consistently applied across the organization, and used for all control assessment activities.

## **Components of a Good Information Security Program**

The establishment of a good information security program is an important part of meeting SOX requirements. Insufficient security programs are characterized as immature and ineffective in detecting internal control (management, operational, and technical) deficiencies. Organizations that do not establish and maintain adequate internal controls will have a costly road to meeting SOX compliance. Inadequate internal controls prevent the organization from measuring their effectiveness and the improving processes associated with ensuring the accuracy of financial reporting, critical to complying with SOX.

There are several important components of a good information security program that help ensure SOX legislative requirements can be achieved, with decreasing reoccurring costs and overall efficiency in the operational effectiveness. The following components are of particular importance for an effective organization-wide security program:

- § Risk analysis to identify threats and vulnerabilities to critical information assets
- § Involvement of senior management (e.g., CEO, CIO, CFO)
- § Senior security official responsibility and authority
- § Development and dissemination of security policies
- § Regular security awareness training and education programs
- § Regular security assessment and audits
- § Business continuity and contingency planning
- § Incident response and reporting capability

In this section we will discuss each of these components in detail to fully understand how they contribute to a good security program.

### **Risk Analysis to Identify Threats and Vulnerabilities to Critical Information Assets**

As part of an ongoing security lifecycle (see [Appendix A](#)), the organization must first understand what the current and most likely threats and vulnerabilities are within the operational environment. Threat and vulnerability identification enables the organization

---

<sup>3</sup> "COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the casual factors that can lead to fraudulent financial reporting and developed recommendations for public companies, and their independent auditors, for the SEC and other regulators, and for educational institutions" (COSO, 2006).

to efficiently plan and implement countermeasures to reduce or eliminate the residual (or overall) risk to critical information assets. The more extensive the risk analysis, the more effective the security controls will be to ensure the organization can respond to an event. There are many different types of threats that must be analyzed as part of a risk analysis. Some environmental threats do not require human interaction but instead are resident based on the locale of the organization, such as hurricanes or floods. Other types of threats are conditional influenced by external circumstances that are not predictable such as riots or political movements.

### **Involvement of Senior Management (e.g., CEO, CIO, CFO)**

The recognition of the importance provided by the implementation of information security industry standards and “best practices” is critical for the overall effectiveness of the security program. The involvement of senior management in all phases of the security lifecycle (see [Appendix A](#)) - from initiation, through continuous regular security assessments – is fundamental for the security program to be beneficial. The leadership of the organization needs to become a supporter that encourages all members of the organization from business unit managers to individual employees to take security seriously, and understand how their role(s) fits into the “big picture”.

### **Senior Security Official Responsibility and Authority**

The organization should identify a senior security official that has the responsibility and authority to enforce security policies developed and disseminated by the organization. Having a security authority in the organization is essential for the organizations to properly comply with government mandates, which if not met could limit the organization’s ability to conduct business (e.g., insurance or publicly traded company). These organizations are regularly scrutinized to ensure they meet specific standards, and it requires a security practitioner to manage the activities and developed processes to regular monitor new and existing compliance requirements.

### **Development and Dissemination of Security Policies**

A security policy is a tool used by management to address the expectations for security that are translated into specific measurable and testable goals and objectives (Rhodes-Ousley, 2004, p 47). The support of senior management should be delivered through written policies that state how security controls should be implemented, enforced, who is responsible for ensuring compliance, and how the policy will be communicated to the intended recipients addressed in the policy.

### **Security Awareness Training and Education Programs**

The organizational commitment to security requires an understanding of the key security issues, and an investment in training programs that institutionalize organizational security awareness and education. Security awareness and education has been a part of the training required by the IT staff to protect information and prevent access to

information systems, but individuals at all levels and across all segments of the organization need to understand what security threats exist, and how to approach them (Payne, 2003, para. 2).

External threats to the organization are continuously updating their skill, which requires the organization to consistently deliver current and up-to-date information through an established security education program. This gives the individual employees the knowledge needed to combat threats and prevent attacks from both inside and outside the organization.

### **Regular Security Assessment and Audits**

Security assessments and auditing of internal controls are an important part of evaluating the effectiveness of control implementation. Security assessments test and evaluate the overall effectiveness of the controls in the organization's environment, and provide feedback to senior management on how well the security program is performing. The security of the organization is assessed against management, operational, and technical controls that measure the overall security posture of the organization, and create an actionable plan for gaps discovered through regular assessments.

### **Business Continuity and Contingency Planning**

After the organization has identified the mission-critical functions, the organization needs to understand which systems support those functions. This identification can be made through a business impact analysis (BIA)<sup>4</sup> which seeks to properly prioritize and plan the appropriation of funds to those critical IT components needed to maintain ongoing business operations. The four main components of business continuity planning are: plan initiation of the BIA, perform the BIA, develop recovery strategies, and exercise the disaster recovery and business continuity plans (Chapple, 684, p. 685).

### **Incident Response and Reporting Capability (IRC)**

Establishment of operational incident response and reporting capability is essential for an organization to effectively respond to an event or incident that could adversely affect the confidentiality, integrity or availability of the organization. IRC is a formal, documented process for responding and reporting security incidents that includes the violation security policies and standards, and other security related events that could lead to a loss of data, misrepresentation of data, and disruption of information system operations and data availability (Grance, Kent, & Kim, 2004, p. 16).

---

<sup>4</sup> Business impact analysis (BIA) provides a company with a monetary value associated with the impact of an unexpected event (Chapple, 2005, p. 683).

## **How SOX Compliance is Achieved through Good Information Security Management**

### **Information Security Roadmap**

The application of information security principles is critical as component of the organization's SOX compliance strategy. The importance of information security as part of the mandatory regulatory requirements raises the visibility of security to key leadership within the organization such as the board of directors and the CEO. To ensure compliance, leadership must ensure security is an integral part of the organization's culture and core business processes.

Meeting SOX requirements can become a complicated task for some organizations with an immature security program, however if the organization has already instituted a well-defined security program, the organization will exceed many of the requirements for SOX compliance. SOX requires the internal controls to be assessed quarterly by the organization and a third-party auditor. As part of a good information security management program the organization will implement an assessment process that requires the organization to review security controls on an ongoing basis.

Prior to implementing a security program, all organizations should assess their current security through a gap analysis. A gap analysis involves reviewing existing controls, and identifying which controls are acceptable based on the organization's environment. The output of the gap analysis is an understanding of the deficiencies or weaknesses that are needed to effectively address through security controls requirements included in a corporate governance framework (e.g., COSO) used to by the organization to meet SOX compliance.

Through a regular assessment process, the maturity of the organization's security program will be evaluated to ensure controls established to meet the financial management criteria of section 404 of the SOX and changes in the organization's environment do not affect the implemented controls overall effectiveness. The metrics captured through security a program assessment will allow the organization to make changes to their SOX compliance process.

### **Linking Business and IT Layers with SOX Requirements**

The organization's information technology components play an essential part of the design and implementation of the internal controls framework that helps the organization meet SOX compliance. Depending on the IT governance used, information security management practices and standards (e.g., ISO 17799, ISO 27001) should be incorporated throughout the business processes that drive the company.

Beyond the selection and implementation of information security management standards, the framework used for internal control management must be fully documented and applied consistently across the organization. Documentation plays a

critical role in conducting audits and measuring the effectiveness of controls that lead to identifying areas of improvement.

The SOX compliance goals and requirements must be included in the business processes and should be a part of the organization's IT governance. Three business and IT functions produce interdependent controls that should be considered as part of the scope of SOX control definition.

- § Business Processes
- § IT Financial Applications
- § Organizational IT Infrastructure

These layers cut across the business and IT functions within the organization and are the building blocks for ensuring the reliability of the financial reports generated by the organization. Prior to selecting internal controls to support the organization's requirements for SOX, there needs to be an educational phase that links the relationship between the business and IT processes. The organization needs to define the various control levels to produce a fully documented linkage between each level and the SOX objectives.

### **Selecting Internal Controls**

Once the organization has defined the relationship between the business and IT functions and the requirements for SOX compliance, the organization can focus on identifying and selecting internal controls. The internal controls selection process should be management-driven and will be established to meet specific SOX objectives or goals. The internal controls selected based on that flow of the organization's financial transactions from initiation to reporting. There are several categories of internal controls that are usually adopted to meet the SOX compliance which include:

- § Information Classification
- § Access Controls (Information and Information Systems)
- § Information System Documentation
- § Computer, Media and Documentation Disposal
- § Data Retention
- § Security Assessment and Audits
- § Data Encryption
- § Data Integrity
- § Backup and Recovery
- § System Monitoring
- § Authentication and Authorization

## The Current Trends in SOX Compliance

### The Cost of Compliance

Over the past several years, SOX compliance has been seen as a relatively expensive undertaking by large and small companies. This trend in the high cost of meeting SOX compliance can be associated with both external and internal cost drivers. The cost drivers include legal fees and third-party auditing, the initial establishment of a corporate governance structure, productivity loss due to time spent on meeting the requirements of section 404, and senior level-management compensations for the increased time and skills needed for compliance activities.

At current, there is an expected overall cost increase in 2006 mainly due to the IT investment companies will be making in automated technologies used to refine existing business and IT controls for continuous monitoring. "Spending on Sarbanes-Oxley (SOX) technology continues to rise, according to the latest research from AMR Research, Inc. in Boston. This year technology purchases are expected to account for 32% [28% higher than 2005 and 21% higher than 2004] of \$6 billion in total SOX spending" (Tucci, L, 2006, para. 1). The cost associated with other compliance cost drivers such as internal labor and external consultants will see a slight decrease from the previous years, demonstrating organizations are beginning to see SOX compliance as an instituted operational activity rather than a compliance initiative.

### Steps to Compliance

There are many methodologies that have been developed to help organizations with a framework for SOX compliance, but all have a basic foundation that involves 5 key steps that guide the organization through the SOX compliance process.

- § Define scope of SOX compliance
- § Evaluate and assessment process
- § Budget, plan, and implement remediation action plan
- § Audit and test internal controls
- § Automate and monitor

In this section we will discuss each of these steps to meeting SOX compliance in detail. The compliance strategy chosen by the organization should include an established, well-documented process for defining the scope of the SOX compliance effort. Throughout each step beginning with evaluating and assessing the process (including making adjustments as needed to mature the organization's compliance process) through ongoing compliance monitored activities senior management should have a true visibility into state of the compliance effort, usually through a dashboard that reports overall compliance and internal control effectiveness.

## **Define Scope of SOX Compliance**

The first step in SOX compliance involves defining the regulatory objectives and requirements, including the framework and standards such as COBIT or ISO 17799 that will be applied within the organization. Once the organization has a clear understanding of the controls necessary to ensure compliance, the scope should be evaluated to ensure only SOX related systems are considered part of compliance initiative. This ensures that the SOX compliance project focuses only on critical systems that relate to the integrity and accuracy of financial reporting, rather than the entire enterprise.

## **Evaluate and Assessment Process**

After the organization defines the scope of the SOX compliance effort, the organization needs to evaluate and develop an assessment process that seeks to identify associated risks to the financial reporting processes and currently existing controls that may not operate effectively or appropriately. During the initial stages of the assessment process, the organization will document the deficiencies to the assessment procedures and reporting process, and document action items. As the organization documents that improvements to the assessment process, they will also evaluate and analyze the results of the assessment of the organizations internal controls to understand what reasonable actions can be taken to remediate the deficiencies.

## **Budget, Plan, and Implement Remediation Action Plan**

The next step of the SOX compliance process has three major objectives (budgeting, planning and implementation of a remediation plan) that help guide the organization to improve the assessment process, and remediate deficiencies encountered during the organization's assessment of the internal controls. For those organizations that are going through the compliance process for the first time, there will be a great deal of time and budget associated with implementing the compliance strategy, and remediation activities on deficiencies found. This may require the organization to phase in the control deficiencies over a period of time, with intermittent testing of controls integrated into the information systems.

## **Audit and Test Internal Controls**

As part of the organization's compliance strategy, there is a requirement that an outside audit firm conducts testing of the internal controls, and assesses their effectiveness in preventing and detecting material errors in the financial statement assertions. As part of the assessment process, the organization will verify the results of the organization's internal auditor's testing of the evaluated controls. Also, the outside auditors will document noted ineffective controls or deficiencies and recommend actionable items that will need to be prioritized, budgeted and planned for future remediation activities.

### **Automate and Monitor**

The organization needs to ensure compliance monitoring is a part of their ongoing compliance activities. This gives the senior management and the board of directors who are responsible for taking action on deficiencies a facility to engage when a problem occurs. Most organizations have moved towards automation so that internal controls are tested regularly, and there is less cost associated with the manual testing efforts. Automation also provides assurance against human error since they can be modeled to the specific organization's environment, and scheduled to deliver real-time feedback through a dashboard reporting system.

### **Conclusion**

Sarbanes-Oxley (SOX) compliance initiatives enforce "best practices" and provide assurance in the reliability and accuracy of financial reporting. The scrutiny and strictness of the legislation limits companies from presenting false financial statements, effectively increases public trust, and addresses the issues regarding corporate governance and accountability. IT governance and information security management have become the new "hot topic" in the board rooms, which helps create sustainability and ensures oversight through involvement of a Company Accounting Oversight Board (PCAOB) that is held accountable for the compliance activities. As a result of SOX compliance, the incorporation of industry standards and processes enables any organization to become more mature and efficient.

## References

- COSO. (2006). Retrieved October 2, 2006 from <https://www.coso.org>
- Grance, T., Kent, K., & Kim, B. (2004). Computer Security Incident Handling Guide. National Institute of Standards and Technology (NIST): Maryland.
- Payne, Shirley (2003). Educause Quarterly.  
<http://www.educause.edu/ir/library/pdf/eqm0347.pdf#search=%22security%20education%20and%20awareness%20security%20program%22>
- Rhodes-Ousley. (2004). Network Security: The Completed Reference. New York: McGraw-Hill/Osborne.
- Tucci, L. (2006). Spending on Sarbanes-Oxley Software Climbs. Retrieved October 10, 2006 from  
[http://searchcio.techtarget.com/originalContent/0,289142,sid\\_gci1164826,00.html](http://searchcio.techtarget.com/originalContent/0,289142,sid_gci1164826,00.html)
- United States Senate. (2004). Biography of United States Senator Paul S. Sarbanes Democrat from Maryland. Retrieved September 20, 2006 from  
[http://www.senate.gov/~sarbanes/pages/biography\\_2004.html](http://www.senate.gov/~sarbanes/pages/biography_2004.html)
- U.S. House of Representatives (2002). 107<sup>th</sup> Congress 2d Session. Retrieved September 20, 2006 from [financialservices.house.gov/media/pdf/hr3763ai.pdf](http://financialservices.house.gov/media/pdf/hr3763ai.pdf).
- Walt, C. V. (2002). Security Focus. Assessing Internet Security Risk, Part One: What is Risk Assessment? Retrieved October 2, 2006 from  
<http://www.securityfocus.com/infocus/1591>.
- Waschke, M. (2005). Sarbanes-Oxley Compliance Journal: Service for SOX. Retrieved October 1, 2006 from <http://www.s-ox.com/feature/detail.cfm?articleID=914>

## Appendix A: Security Lifecycle

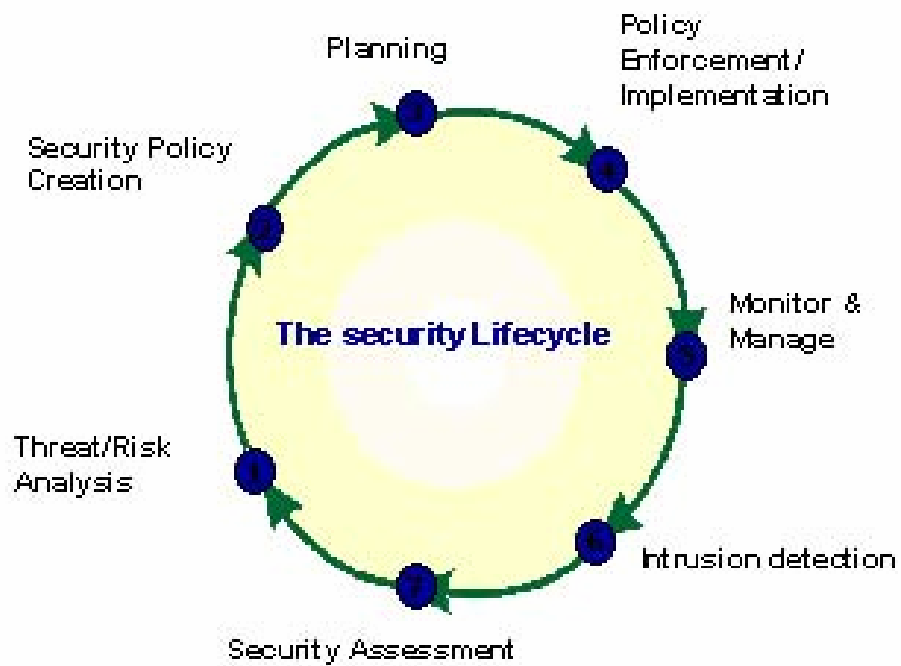


Figure 1: Security Lifecycle (Walt, 2002)