SARBANES OXLEY REVIEW AND IMPLEMENTATION IN MODERN ORGANISATIONS UNDER COSO FRAMEWORK

Tanvir Orakzai, PhD
AUTHOR INFO

Author Name: Tanvir Orakzai

Qualification: PhD, MSIT, MA

Organisation: Eureka Solutions Singapore

Email: tanvir_orakzai@yahoo.com
# Table of Contents

Abstract........................................................................................................................................... 4  
Introduction ....................................................................................................................................... 5  
Sarbanes-Oxley Explained ................................................................................................................... 6  
  Section 302 Key Points ..................................................................................................................... 6  
  Section 404 Key Points ..................................................................................................................... 6  
SOXS Implementation Guidelines ......................................................................................................... 7  
  Suggested Action Plan (18 months) .................................................................................................... 7  
COSO Framework for Internal Control and SOX Compliance ............................................................. 8  
Conclusion.......................................................................................................................................... 10  
Reference .......................................................................................................................................... 11
Abstract

Information security experts today confront cluster of government regulations that can influence the way they do their occupation. Some of these examples include Sarbanes Oxley, Gramm-Leach-Bliley Act, the Health Insurance Portability and Responsibility Act (HIPAA) etc that and California Senate Bill affect the data security prerequisites for an organization. A lot of these Acts are vague and ambiguous simply tells what should be done rather than how it should be done. This article examines the Sarbanes Oxley Act focusing on the control Section of 302 and 404 and how COSO framework can be utilized for information security compliance in modern organisation.

Keyword: Sarbanes Oxley, COSO, Information Security Compliance, SOX Control, SOX implementation Guidelines,
Introduction

Data security experts today confront a mind boggling cluster of government regulations that can influence the way they do their work. For example, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Responsibility Act (HIPAA) and California Senate Bill 1386 can generously affect the data security prerequisites for an organization and create complexities that a number of organisation find them too complex and vague to implement. The information security experts are required to be familiar with, comprehend, and guarantee that their organization is in consistence with these laws (Holt, 2007).

While organizations are speculatively recognized to be the consequence of their shareholders’ wishes, really they are more slanted to be the eventual outcome of the endeavours, yearnings and longing of their senior executives, basically in light of the way that these people are the ones with the data and energy to guide the method for the organization, and doubtlessly with the capability and judgement to accomplish their corporate targets. This is, to be totally straightforward, their work, to make the organization productive and valuable that is not often the case (Holt, 2007).

The shareholders wouldn't fuss their ventures paying unlimited recompenses and prizes to their executives such as CEOs, CEFOS or COOS in the hope of stability and security of business. However titanic pay rates don't outfit much spurring energy for executives to strain themselves to profit an occupation. It is vain hope and reasoning that top monetary instalments will motivate CEOs to support shareholder regard- such view is partial true. The US Government and other Western Governments saw the breakdown of these associations with Top Executives misleading authority as a threat to shareholder in the securities trades. It was clear that despite requesting a description from the executives in court, some tightening of the rules was paramount to thwart practically identical events from happening again. It was under these circumstances that Senator Paul Sarbanes and Congressman Mike Oxley with the occupation of making some serious new laws that aims to balance and decrease the probability of corporate shames like Enron, Worldcom from happening again (Don, 2008).

The expressed motivation behind the Sarbanes Oxley law is "to ensure speculators by enhancing the precision and dependability of corporate exposures made in accordance with the security laws, and for other purposes." The impact of the law is clearing, long haul changes in the way openly exchanged organizations oversee evaluators, money related reporting, official obligation and inner controls. While various laws and regulations legislating the behaviour of open organizations as of
recently exist, SOX is viewed as the most generous bit of tool to circumvent the authority of the Top Executives. The making of SOX emulated a standout amongst the most turbulent periods in US corporate history. The exact open breakdown of corporate monsters like Enron and Worldcom harmed the basic confidence in US partnerships. It additionally prompted the downfall of one of the country’s biggest open bookkeeping firms. Overall Sarbanes Oxley (SOXs) is intended to restore speculator’s trust and comprehension of open company money related reporting (Holt, 2007).

Sarbanes-Oxley Explained
According to Aanad, (2007) and Arjun (2009)- the Sarbanes-Oxley Act is organized into eleven 'titles'. The normally acknowledged title are 302, 401, 404, 404 409, 802 and 906 but this paper would focus only on section 302, 404.

Section 302 Key Points
Intermittent statutory budgetary reports are to incorporate affirmations that:

- The marking officers have explored the report
- The report does not hold any material untrue proclamations or material oversight or be acknowledged deluding
- The fiscal proclamations and related data reasonably show the monetary condition and the outcomes in all material regards
- The marking officers are answerable for inner controls

The section 302 clearly states that the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) should affirm that monetary reports are correct and complete. They should likewise evaluate and investigate the adequacy of inward controls around monetary reporting. This section unmistakably puts obligation regarding faultless fiscal reporting on the most elevated amount of corporate administration. Presidents and CFOs now confront the potential for criminal misrepresentation liability.

Section 404 Key Points
According to Graham (2007) Section 404; an organization must evaluate the adequacy of its inward controls and report this evaluation every twelve-months to the SEC. The evaluation must likewise be audited and judged by an outside examining firm. The effect of segment 404 is generous in a sense that a lot of assets are required for consistence. An exhaustive audit of all inward controls identified
with budgetary reporting is an overwhelming errand. Likewise with area 302, the wording of segment 404 is expansive and does not furnish particular direction as to which controls must be surveyed.

While the theme of information security is not particularly talked about; the actuality is that monetary reporting frameworks are vigorously dependant on effective controls. Any survey of inward controls might not be complete without tending to controls around data security. An unreliable framework might not be viewed as a wellspring of dependable fiscal data due to the likelihood of unapproved transactions or control of numbers. Section 302 and 404 in a roundabout way drive the examination of information security controls for SOX consistence.

**SOXS Implementation Guidelines**

Normally in every organisation the audit team would conduct assessment and present it to the management for further action. In short the internal auditor and the management have to work together to understand Sarbanes Oxley’s requirements and work towards the implementation in clear timeline. The vital issue will be reviewing the requirement of section 404 along with 302 to addresses the control issues prior to going live (Chorafa, 2009).

**Suggested Action Plan (18 months)**

The suggested project timeline is 18 months, however it depends on organisation efforts, how sooner or later, and it can deliver.

- Project initiation (3 months)
- Documentation evaluation (6 months)
- Remediation of gaps (5 months)
- Dr Run/Test Phase (3 months)
- Go Live

The following conditions are vital for SOX Implementations:-

- Management clearly comprehends the importance of effective control and accepts the responsibility
- Management understands the effectiveness of internal control
- Control Objective and relative control (COBIT) is clearly documented
Those companies; who wish to put SOX in place, the crucial issue is to put 100% control in place rather than fulfilling the job for the sake of compliance or doing from the comfort zone. The purpose of control is not to opine on the financial statement that is part of financial audit but to put effective InfoSec controls in place, where risk of fraud is minimised.

Complying with SOXs doesn’t mean companies are living in vacuum with no policy and procedures for internal control. Most companies have information security control procedures in place; however they may lack compressive security framework that’s the main purpose of SOXs. In order to comply with SOXS, companies would require a clear and formal plan to address the regulations and normally the COSO is considered more suitable framework (Marchetti, 2007).

**COSO Framework for Internal Control and SOX Compliance**

Section 404 requires that management should evaluate a suitable control framework, where COSO is recognised an acceptable framework and can work as benchmark for Section 404 reporting. Under COSO framework, the internal controls are affected by board of directors, management and other senior officials who gives the judicious assurance to achieve the internal control objective:

Chorafas (2009) has mentioned that COSO has five components of control as following:-

- Control Environment
- Risk Assessment
- Control Activities
- Information and communication
- Monitoring
Anon (2014) and Switze (2007) have mentioned that the most effective way to meet the legal requirements of SOXs will be the size, nature and complexity of the organisation including the quality of business process and internal control system. An ideal way would be to conduct maturity analysis that would make it easier to evaluate, how existing control meets the requirements and what gap is present in the current control and how can it be aligned to COSO control framework. For eg companies with multiple business segments and geographical units will determine the financial importance and how an error can lead to financial risk. A few additional risks include major system update, management turnover, acquisition or volatile business environment etc. Often the individual units independently may not pose any risk; however when grouped with other units, the outcome may be a misstatement that needs to be prevented. In such scenario, the ideal way would be to have enterprise wide control in addition to individual controls. This will create a double layer of control and a comprehensive outlook that will create little space for error or mistakes with effective security and control in place.

---

**Figure 1.0: COSO Control Framework**

| Control Environment | • Change Organisation Mindset  
|                     | • Instill integrity value in individuals |
| Risk Assessment     | • Analyse the inherent risk in the organisation and mitigate it through control activities |
| Control Activities  | • Design policies and procedures  
|                     | • Segregation of role and responsibilities |
| Information & Communicaiton | • Capture all relevant information  
|                     | • Communicate info to management for action |
| Monitoring          | • Assess control activities  
|                     | • Management and Supervisor activities  
|                     | • Internal audit |
Conclusion

The Sarbanes-Oxley Act has radically stretched senior organization's mindfulness to information security. This can fundamentally grow workload and push on IT work power, yet it can furthermore give the backing for advantages of information security issues that may have a while back been given a simpler need. SOXS has constrained open organizations to clean up their enactment regarding the matter of budgetary reporting that appears to have increased certainty in the market. On the other hand some privately owned businesses have voluntarily stuck to this same pattern to changing degrees, in light of the fact that they see that the SOX standards can enhance their operations through better administration and expanded effectiveness, and position them in a superior way in the market.
Reference

Available at: www.soa.org/library/journals/actuarial-practice-forum/.../apf0701_5.pdf
[Accessed 10 March 2014].


