IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 140-142
www.iosrjournals.org

Sox Compliance: Eleven Essential Controls for Sme

Utkarshni Sharma'
Assistant professor Ankita Gupta" Computer Science Engineering (IS) 'PEC University, Chandigarh

Abstract: *Sarbanes-Oxley (SOX) act, was enacted in 2002, in the wake of large accounting scandals ENRON and WORLDCOM .Especially for SMEs (small to mid-sized enterprises) that can benefit from implementing the control objectives, for governance, compliance and improved security. SOX compliance did not gave detailed requirements for IT compliance, therefore many auditors adopted COBIT and COBIT guidelines to comply with SOX. This research discusses the latest sox developments in the SME, key findings from ISACA study and COBIT control objectives to satisfy internal IT controls .This compliance escalates and maps out internal it controls that protect information assets.*
Keywords*: SOX, COBIT, ISACA, IT controls.*

I. Introduction

This act was launched as corporate and auditing accountability act of 2002, by Mike Oxley on 14th Feb 2002.This was passed in the house on 24th April 2002, and by U.S congress to protect shareholders and public from accounting errors and Janus-faced practices in the enterprise, andto improve accuracy of corporate disclosures. This act was enacted after major accounting scandals of ENRON and WORLDCOM.SOX covers responsibilities of public corporation's board of directors, adds penalties for certain misconduct and defines how public corporations can comply with this law.Led to the benefit of firms and investors by acquires top down approach of risk assessment. Evaluates company and entity levels controls which corresponds to the components of the COSO framework. Scales the assessment based on the size and complexity of the company. This act had a limitation of not providing detailed requirements for IT compliance, therefore COBIT and its guidelines were being adopted by auditors to comply with SOX. COBIT bridges gap between control requirements, technical issues and business risks and gives top controls as recommended in the ISACA study with rank, control objective and what to implement.

II. Sox And Cobit

SARBANES-OXLEY ACT:-

Sarbanes –Oxley act was enacted in 2002 in the wake of large accounting scandals Enron and WorldCom. Especially for small to mid-sized enterprises that can benefit from implementing the control objectives, for governance, compliance and improved security. Two sections of SOX are noteworthy for its implementation: sec 302 and sec 404, which states corporate responsibility for financial reports and Management assessment of internal controls respectively.

Sarbanes Oxley act has eleven titles:

- Title 1: Public Company Accounting Oversight Board (PCAOB).
- 2. Title 2: Auditor Independence.
- 3. Title 3: Corporate responsibility.
- 4. Title 4: Enhanced financial disclosures.
- 5. Title 5: Analyst conflicts of interest.
- 6. Title 6: Commission resources and authority.
- 7. Title 7: Studies and reports.
- 8. Title 8: Corporate and criminal fraud accountability.
- 9. Title 9: White collar crime penalty enhancements.
- 10. Title 10: Corporate tax returns.
- 11. Title 11: Corporate fraud and accountability.

Frailty of Sarbanes Oxley act:

- Sins SOX was enacted there were repeated concerns about increasing cost to comply with its requirements.
- A workload estimation of five hundred additional man hours was required to comply with SOX.
- During last 5 years surveys were made that measured that ratio of audit fees to assets increased between 2000 and 2002.

- Also there were no rules for control requirements, technical issues and business risks and on IT management governance.

ISACA FOR THE SALVAGE:

SME have very limited IT resources and staff for risk controlling and many don't know how to prioritize them. Compromised controls too have proportionally greater impact on SME as well, while larger enterprises tend to imbibe financial losses whereas on the other hand SME may face obdurate loss of customer or even bankruptcy.

ISACA (The Information Systems Audit and Control Association) sets standards for auditing and grants certification to auditors, conducted a study in 2006 to ordain top IT controls, that SME should have
For security of information assets. And to do so COBIT controls were adopted by a panel of experts, and were asked to choose important ones to achieve unison.

COBIT:

Control objectives for information and related technology framework by ISACA for IT management and IT governance, to bridge the gap between control requirements, technical issues and business risks. Obit was first released in 1996, the current version COBIT 5 that came in June 2013, included information security and assurance. COBIT has thirty controls for management, governance and security, out of which, top eleven controls were chosen and prioritized by ISACA.

Table 1.1 List of Controls

RANK	CONTROL OBJECTIVE	WHAT TO IMPLEMENT
1.	Network security	Updated firewall, secure wireless transmission.
2.	Virus protection	Updated anti-virus, anti-spyware applications.
3.	Backups	Regular and tested backup procedures.
4.	File access privilege controls	Role-based access control, least privilege.
5.	It as a part of strategic plans	Technologies that support business goals.
6.	It continuity and recovery plans.	Basic disaster recovery plan (DRP) procedures.
7.	Id and authorization procedures.	Complex passwords, password change policies.
8.	Management support/buy in.	Leadership from CEO for IT control projects.
9.	Risk evaluation program.	Basic risk assessment and/or self-audits.
10.	Employee it security training.	Training for email, web and password use.
11.	Data input controls.	Field formats, periodic data range testing.

III. Improvement And Optimization:

Controls can come in policies, technologies that restricted access to sensitive data or even a process within an application.IT controls must be documented in order to meet the audit requirements and should at least contain following IT controls:

-information security.

Policies, procedures, standards, risk assessments, authentication controls, user-level controls, logging,monitoring,configurations and physical security.

-change management and development.

Development standards and procedures, requests, approval, maintenance, testing, quality assurance, software development lifecycle documentation.

-operations.

Batch jobs, backups

Comparitive Analysis

Table 1.2 Comparative Study

PARAMETERS	**ONLY SOX (SARBANES OXLEY ACT)**	**SOX WITH COMBINATION OF COBIT FRAMEWORK**
COST	Increasing cost for compliance.	Reduction in cost of compliance.
MAN HOURS	Workload estimation of additional 500 man hours	Minimized human error.
POLICIES/ RULES	No rules for control requirements, technical issues and IT management governance.	Provided detailed requirement for IT compliance.
COMLEXITY	More professionals, more confusion.	Reduced complexity.

IV. Bottom Line

SME can benefit from implementing control objectives for governance, compliance and improved security. In obtaining Sarbanes Oxley compliance, most widely accepted standard is COBIT, which will be the path of least resistance to Sarbanes Oxley compliance. Sarbanes Oxley act with COBIT has strengthened control environment, improved documentation, increased audit committee involvement, reduced complexity and minimized human error. Sox has led to increased effectiveness and efficiency of operations, duplicate and superfluous controls can now be easily identified , reduced cost of compliance and external audit can more readily rely on internal audit.

References

[1]. Sarbanes Oxley requirement: http://www.sarbanes-oxley-101.com/.
[2]. IT Control Objectives for Sarbanes-Oxley Using COBIT 5, 3rd Edition.
[3]. The costs and benefits of Sarbanes Oxley act: www.forbes.com/sites/.../03/.../the-costs-and-benefits-of-sarbanes-oxley.
[4]. Corporate Ethics and Sarbanes-Oxley:corporate.findlaw.com › Corporate Counsel › Law Library
[5]. COBIT 5: A Business Framework for the Governance: www.isaca.org/cobit/pages/default.asp.
[6]. COBIT 5 (Control Objectives for Information and related Technology) https://managementmania.com/en/cobit-control-objectives-for-information-and-related-technology.
[7]. COBIT 5 framework for the governance of enterprise IT: www.itgovernance.co.uk/cobit.aspx.
[8]. eleven essential controls: www.infotech.com/research/sox-compliance-eleven-essential-controls-for-the-sme.
[9]. Essential controls: www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=2106.
[10]. Guide to the Sarbanes-Oxley Act: IT Risks and Controls: www.protiviti.in/en-US/.../Guide-to-SOX-IT-Risks-Controls-Protiviti.pdf.
[11]. SAS 70 Type II Audits – Interlinks https://www.intralinks.com/sites/default/files/file_attach/wp-sas70ii.pdf.
[12]. Midrange & Mainframe systems for Security Policies https://www.sans.org/.../midrange-mainframe-systems-security-policies-**c**.
[13]. The Impact of the Sarbanes-Oxley Act on American Businesses http://smallbusiness.chron.com/impact-sarbanes-oxley-act-american-businesses-1547.html
[14]. Benefits of SOX: https://hbr.org/2006/04/the-unexpected-benefits-of-sarbanes-oxley.
[15]. The Impact Of Sarbanes Oxley On Companies, Investors: www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=1141.
[16]. Beyond Sarbanes-Oxley - Journal of Accountancywww.journalofaccountancy.com/issues/2006/.../beyondsarbanesoxley.html.