APPLICATION OF TECHNOLOGY IN IMPLEMENTATION OF SARBANES OXLEY ACT 2002

Akshaya Kothale[*]

Abstract:

SOX Compliance applies to any company governed by the Securities and Exchange Commission (SEC) which includes all publicly traded companies; including all divisions, and their wholly owned subsidiaries, must comply with Sarbanes-Oxley. In addition Sarbanes-Oxley also applies to any non-US public multinational company engaging in business in the US. . The act is a tool for the implementation of the greater responsibilities that was lacking in some of the companies that was convicted of fraud. The act means that companies shall try to focus on strong ethic codes, honesty in business, integrity and transparency. . The act is a tool for the implementation of the greater responsibilities that was lacking in some of the companies that was convicted of fraud. The act means that companies shall try to focus on strong ethic codes, honesty in business, integrity and transparency. IT systems play a critical role in ensuring the accuracy of a company's financial reports. As a result, validation of IT controls is a key part of Sarbanes-Oxley compliance initiative. The report hence summarizes that implementing SOX aspects along with IT controls is a daunting task but the checklist and the tools mentioned here could prove to be an aid for organizations and also with a lesser deploying cost to their benefit.

Keywords: SOX, SEC, IT, ethic codes, frauds

[*] Academician

Introduction:

The Sarbanes-Oxley Act (SOX) came into force in July 2002 in the wake of major corporate and accounting scandals. SOX introduced major changes to the regulation of corporate governance and financial practice.

The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. The first part of the Act establishes a new quasi-public agency, the Public Company Accounting Oversight Board, which is charged with overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. The Act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.

SOX Compliance applies to any company governed by the Securities and Exchange Commission (SEC) which includes all publicly traded companies; including all divisions, and their wholly owned subsidiaries, must comply with Sarbanes-Oxley. In addition Sarbanes-Oxley also applies to any non-US public multinational company engaging in business in the US.

The report aims at establishing a link between the IT control aspects of an organization and the implementation of Sarbanes-Oxley Act of 2002. The report is endorsed with the help of a generalized IT control checklist. Furthermore, the report introduces a OpenSource Tool named "ITSOX Toolkit" and also explains a very succinct description of tools and softwares which are an integral part of the ITSOX toolkit.

The report hence summarizes that implementing SOX aspects along with IT controls is a daunting task but the checklist and the tools mentioned here could prove to be an aid for organizations and also with a lesser deploying cost to their benefit.

Background:

The corporate scandals in 2001 and 2002 came to change the way internal and external auditors, board of directors and senior corporate management needed to work. Companies such as Enron and WorldCom were accused of filing inaccurate financial statements, using off balance sheet accounting to hide certain debt that was not viewed positive from management and accountants.

In order to restore the broken trust that had been damaged after the Enron, WorldCom and Healthcare scandals, President Bush signed in a new act in the legislation system in July 2002, and the Sarbanes- Oxley Act was enacted. The act is a tool for the implementation of the greater responsibilities that was lacking in some of the companies that was convicted of fraud. The act means that companies shall try to focus on strong ethic codes, honesty in business, integrity and transparency.

There are 11 titles that describe specific of the Sarbanes Oxley Act. They are:

Titles	*Heading of the title*
Title I	Public Company Accounting Oversight Board (PCAOB)
Title II	Auditor Independence
Title III	Corporate Responsibility
Title IV	Enhanced Financial Disclosures
Title V	Analyst Conflicts of Interest
Title VI	Commission Resources and Authority
Title VII	Studies and Reports
Title VIII	Corporate and Criminal Fraud Accountability
Title IX	White Collar Crime Penalty Enhancement
Title X	Corporate Tax Returns
Title XI	Corporate Fraud Accountability

SOX – Title 3

TITLE III – CORPORATE RESPONSIBILITY

1) Sec. 301. Public company audit committees.

2) Sec.302.Corporate responsibility for financial reports.

3) Sec. 303. Improper influence on conduct of audits.

4) Sec. 304. Forfeiture of certain bonuses and profits.

5) Sec. 305. Officer and director bars and penalties.

6) Sec. 306. Insider trades during pension fund blackout periods.

7) Sec. 307. Rules of professional responsibility for attorneys.

8) Sec. 308. Fair funds for investors

Titles	*Heading of the title*
Title I	Public Company Accounting Oversight Board (PCAOB)
Title II	Auditor Independence
Title III	Corporate Responsibility

Title IV	Enhanced Financial Disclosures
Title V	Analyst Conflicts of Interest
Title VI	Commission Resources and Authority
Title VII	Studies and Reports
Title VIII	Corporate and Criminal Fraud Accountability
Title IX	White Collar Crime Penalty Enhancement
Title X	Corporate Tax Returns
Title XI	Corporate Fraud Accountability

SOX – Title 4

TITLE IV – ENHANCED FINANCIAL DISCLOSURES

1) TITLE IV – Enhanced financial disclosures

2) Sec. 401. Disclosures in periodic reports.

3) Sec. 402. Enhanced conflict of interest provisions.

4) Sec. 403. Disclosures of transactions involving management and principal stock-holders.

5) Sec. 404. Management assessment of internal controls.

6) Sec. 405. Exemption.

7) Sec. 406. Code of ethics for senior financial officers.

8) Sec. 407. Disclosure of audit committee financial expert.

9) Sec. 408. Enhanced review of periodic disclosures by issuers.

10) Sec. 409. Real time issuer disclosures.

Roles of IT in SOX

IT systems play a critical role in ensuring the accuracy of a company's financial reports. As a result, validation of IT controls is a key part of Sarbanes-Oxley compliance initiative. However, in Year 1 most companies pursued IT control validation in a reactive manner. As a result, the cost of compliance was very high.

Controls over the IT environment

Most Business Processes are either partially or wholly enabled by IT

Achieving control objectives is often dependant on IT based controls

Many controls depend on data generated by IT systems

IT controls need to be considered at 2 levels:

Controls over the IT environment (General Controls)

Controls over individual applications (Application Controls)

SOX Impact on IT Departments

- IT services are now a vital part of the financial reporting process applications and services support creation, storage, processing, and reporting of financial transactions
- SOX compliance also must include controls for the use of technology in data handling, processing, and reporting
- General computing controls are critical
- Ensuring data integrity and secure operations of financial reporting
- IT departments now must formally address the design, documentation, implementation, testing, monitoring, and maintaining of IT internal controls.
- CEOs and CFOs look to the information services department to ensure that the general and specific internal controls for all applications, data, networking, contracts, licenses, telecommunications, and physical environment are documented and effective

Overall risk and control considerations are assessed at the departmental level of information services and then at the entity level.

Specific IT Controls Required for Sarbanes-Oxley Compliance

- ▪ **IT security**
- Security administration
- Monitoring and enforcement of security policies
- Policies communicated to all users
- Who has access to the application and data? Who authorizes access? How often is access level reviewed? What is the authorization process? What happens when an authorized person leaves or changes jobs? Is data security enforced at the element level? Are passwords enforced and changed regularly?
- Need to know basis
- Access to financial and "protected personal" data likewise must be limited to those individuals who have an authorized business reason for access.

- **<u>Change control</u>**
- Applies to applications, productivity tools, and operating system software
- To ensure accuracy, completeness, and integrity of financial reporting, companies must have a documented, effective change-control process that includes changes to financial

applications, all interface applications, operating systems that control the desktop and host server, productivity tools used to create summary analysis, database management systems, and networks.

- change process must provide the following:
- Points for management review
  - Authorization
  - Migration of changed components
  - Change scheduling
  - Management reporting
  - Communication of changes to the user community
  - Who can initiate a change? Who authorizes changes? Who can make changes? What testing should be done prior to making a change to production components? Who does the testing and validates the changes? How is testing documented? What process is used to promote development components into production?
- **Data management**
  - encompasses both logical and physical data management as well as identification and protection of critical data, especially data related to financial processing and reporting.
  - Data Transfer between Systems
  - whether downloads are consistent, timely, and complete with validation routines. Errors found in the extract, transform, and download process should be segregated, reported, and cleared within a reasonable time frame to ensure accurate financial reporting
  - Database Structures
  - Compatibility of database management systems
  - Different structures leads to integrity of summation, interpretation, and analysis can be jeopardized.
- Data-Element Consistency
  - metadata files and data dictionaries should be used to ensure consistent interpretation of key data elements
  - Physical Control of Data
  - crucial to the integrity of financial reporting
  - Data Backup

- Timing and frequency of the backup process should be determined by the business need for short-term recovery of data in problem situations

- **IT operations**
  - Ineffective IT control environments are a significant indication that material weaknesses in internal control over financial reporting exist
  - Extend well beyond the obvious management of hardware and the data center
  - Example: acquiring an IT environment,
  - controls over the definition, acquisition, installation, configuration, integration, and maintenance of the IT infrastructure

The 12 attributes on which the Checklist is based is:

1. Information Availability
2. Reliability of IT Systems
3. Communications
4. IT Strategic Planning
5. IT Processes, Organizations and Relationships
6. Manage IT Resources
7. Educate and Train Users
8. Assess and Manage IT Risk.
9. Manage Quality
10. Monitor and Evaluate Performance
11. Monitor and Evaluate Internal Control
12. Change Management.

Conclusion:

SOX forces companies to take control of business processes or face stiff penalties. Developing and documenting business processes and internal financial controls is a complex task that requires the interaction of CEO, CFO and CIO to develop a consistent system optimized to specific needs. While there is no single magic bullet for SOX compliance, a strong and secure IT foundation will speed compliance activities, enable higher levels of process control and support both internal and external audits.

While building IT control is only a part of developing and documenting overall financial controls, IT tools can help provide added value to overall business processes.

Implementing IT control processes that can support overall business objectives not only requires that CEOs, CFOs and CIOs work together to plan, evaluate, refine and optimize core technology systems, but also determine how those systems are used throughout the organization.

Limitations:

1) Noncompliance to Sarbanes-Oxley regulations is harsher.
2) The act is only applicable for the companies having large capital and doing business in the USA.
3) The complexity of SOX has led to greater confusion system auditors.
4) The awareness of SOX is very low or virtually zilch.

References:

1)http://www.metricstream.com/insights/sox_it_controls.htm

2)http://www.insidesarbanesoxley.com/2004/09/it-control-objectives-for-sarbanes.asp

3)http://www.bmc.com/products/documents/42/37/54237/54237.pdf.

4)www.meritsolutions.com/products/Delivering_IT_Controls_for_Sarbanes_Oxley_Compliance.pdf

5)www.amper.com/services/amper-risk-SOX-IT-controls.asp

6)http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=12383

7)www.gantthead.com/project-plans/IT-Controls-for-SOX-Implementation.html

8)www.deloitte.com/dtt/cda/doc/content/Final%20IT%20Control%20Objectives(2).pdf

9)pcidss.wordpress.com/category/sox/

10) www.wikipedia.org/en/