Understanding SOX, JSOX, in Light of COSO 2013 Framework and its Compliance Measurement in SAP Environment

Corporate governance is a framework of rules, relationship, systems and procedures or processes within and by which authority is exercised and controlled in Corporations. Sarbanes-Oxley (SOX) and Japan's Financial Instruments and Exchange Law (JSOX) is a compliance tool for achieving corporate governance. Both these compliance tools aim at maintaining an effective & efficient internal control system. COSO (The Committee of Sponsoring Organizations of the Treadway Commission) has released an updated draft of its landmark Internal Control – Integrated Framework in 2013. This is an important development for organisations around the world, in particular for those who have adopted the framework for their SOX compliance programme. The updated COSO framework has a stronger emphasis on the role of information technology in establishing control. This paper examines and evaluates the question, "What are the requirements of SOX and J SOX regarding the Internal controls and how the ERP systems like SAP helps to meet these requirements." To do this, it describes the requirements of SOX and JSOX and their relationship with other control methodologies like COSO and discusses the controls of ERP with a specific reference to SAP system.

CMA Tapas Bhattacharya

(The author is a Consultant. He can be reached at tapasbhattacharya47@yahoo.co.in)

Introduction

The term 'Compliance' has emerged as a buzzword in the last few years. The application and meaning of compliance changes is based on the object area. In accounting and auditing application, ''compliance' refers to SOX or JSOX which talks about strengthening of Internal Controls and quality reporting on Finance.

In Production management, Compliance refers to conformance with product specifications and quality standards, as well as respecting environmental regulations. In Human Resource Management, compliance means adhering to the regulations and requirements related to information privacy, safety measures, health regulations *etc.*

The catalyst for the current focus on compliance in accounting and control is a series of high profile financial frauds and bankruptcies including companies such as ENRON, Worldcom, Tyco, Hollinger International and Satyam *etc.* These sent shock waves through the business world. How could well renowned companies with assets worth billions of Dollars disappear from the face of the earth in a matter of weeks, leaving thousands of employees without jobs and the whole business world reeling from the aftershock? The answer deemed to be lack of internal controls, management fraud & fraudulent financial reporting.

SOX (Sarbanes-Oxley Act)

The Sarbanes–Oxley Act is also known as SOX or Sarbox, an act that came into force in July 2002, is considered as one of the most important changes in United States Securities Laws. Approved by the U.S. House of Representatives and the senate, the SOX brought major modifications to the ruling of corporate administration and financial practice. Passed to appraise all legislative audit requirements, Sarbox offers extra powers and duties to the U.S. Securities and Exchanges Commission (SEC).

In general terms, Sarbanes–Oxley Act's provisions apply to four types of Companies:

1. Domestic US registrants
2. Foreign private issuers, also referred to as 'foreign registrants '
3. Subsidiaries of US registrants (only to the extent that some information applies to the consolidated financial statements) and
4. Potentially, companies planning a US registration in the Future.

In addition, the Act appears to have set a benchmark for companies in Europe and Asia that have interest in enhancing corporate governance, including risk management and internal controls.

Hence, the Act has global implications for corporate governance and the development of internal control systems.

Summary of SOX Major Sections

The summary highlights of the most important Sarbanes-Oxley sections for compliance are listed below.

Section	Title	Description
302	**Corporate Responsibility for Financial Reports**	Certifies that financial statement accuracy and operational activities have been documented and provided to the CEO and CFO for certification.
404	**Management Assessment of Internal Controls**	Operational processes are documented and practiced demonstrating the origins of data within the balance sheet. SOX Section 404 (Sarbanes-Oxley Act Section 404) mandates that all publicly traded companies must establish internal controls and procedures for financial reporting and must document, test and maintain those controls and procedures to ensure their effectiveness.
409	**Real-time Issuer Disclosures**	Public companies must disclose changes in their financial condition or operations in real time to protect investors from delayed reporting of material events.
802	**Criminal Penalties for Altering Documents**	Requires public companies and their public accounting firms to retain records, including electronic records that impact the company's assets or performance. Fines and imprisonment for those who knowingly and willfully violate this section with respect to (1) destruction, alteration, or falsification of records in federal investigations and bankruptcy and (2) destruction of corporate audit records.

COSO Framework and SOX compliance

COSO is a voluntary private sector initiative dedicated to improve organisational performance

& governance through effective internal control, enterprise risk management, and fraud deterrence. Five non-profits are its sponsoring organisations: AAA (American Accounting Association), AICPA (American Institute of Certified Public Accountants), FEI (Financial Executives International), IIA (Institute of Internal Auditors), and IMA (Institute of Management Accountants). The COSO was founded and originated in order to identify factors of fraudulent financial reporting and to establish delineated internal control criteria that entities can follow.

The Internal control framework was published in 1992 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Section 404 of SOX requires management at public companies to select an internal control framework and then assess and report of the design and operative effectiveness of their internal controls annually. The majority of US publicly traded companies have adopted COSO's 1992 framework to do this.

On 14th May, 2013, COSO released an updated version of its internal control-Integrated Framework. But, COSO will continue to make the original Framework available through 15th December, 2014, at which time the 1992 framework will be considered superseded. During this transition period, COSO believes continued use of 1992 framework is acceptable.

The new COSO 2013 framework

The original framework defined internal control as "...a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- *Reliability of financial reporting*
- Compliance with applicable laws and regulations

Following is the updated Framework definition:

> "Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, *reporting*, and compliance."

The updated Framework recognises that the reporting of non-financial data is as important as the reporting of financial data. Non-financial data is used to make key business decisions that affect an organisation's financial condition. For example, consider the manner in which your organisation reports on the number of customer complaints, service calls, sales inquiries and potential prospects. Each of these activities is operational in nature and none directly affect the financial reporting process. But these Operational factors have an impact in your Business either directly or indirectly.

For internal audit departments, consider the extent to which the operational component of your organisation's objectives and the associated risk are prioritised when you formulate your annual audit plan.

Defining Attributes of Effectiveness

In keeping with the adage, "what gets measured gets done," the updated COSO Framework describes 17 principles associated with the five components, which make it easier to evaluate organisational effectiveness.

Following is a summary of the principles by component:

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	1. Specifies relevant objectives 2. Identifies and analyses risk 3. Assesses fraud risk 4. Identifies and analyses significant change
Control Activities	1. Selects and develops control activities 2. Selects and develops general controls over technology 3. Deploys through policies and procedures
Information and Communication	1. Uses relevant information 2. Communicates internally 3. Communicates externally
Monitoring Activities	1. Conducts ongoing and/or separate evaluations 2. Evaluates and communicates deficiencies

What is Not Changing...	What is Changing...
Core definition of internal controls	Changes in business and operating environments considered
Three categories or objectives and five components of internal controls	Operations and reporting objectives expanded
Each of the five components of internal control are required for effective control	Fundamental concepts underlying five components articulated as principles
Important role of judgment in designing, implementing and conducting internal control, and in assessing its effectiveness	Additional approaches and examples relevant to operations, compliance, and non-financial reporting objectives added

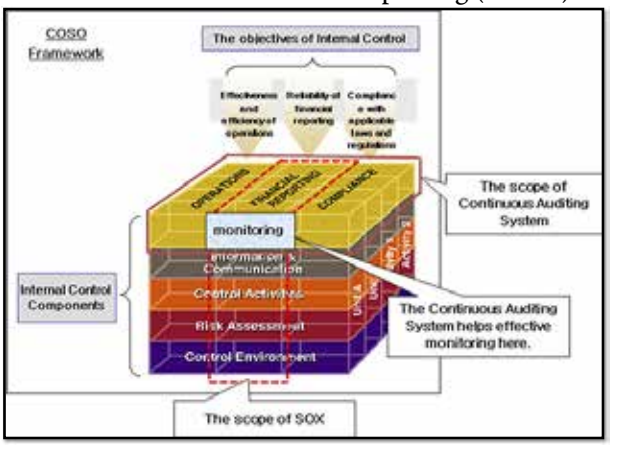
How important are these changes?

The world has sustained a lot of change since 1992 and internal control practices need to keep pace. Competitive pressures, advances in technology and regulatory scrutiny have contributed to increasing expectations for providing relevant information immediately. The Framework's updates came at an opportune time and provide more prescriptive information, making it easier to achieve consistency in our internal control practices and evaluate their effectiveness.

The 2013 Framework has introduced 17 principles, which are new, to enhance users' understanding of the fundamental concepts that were discussed within the original framework.

The 17 principles fit within the five components of internal control that have been retained from the original framework. The 2013 Framework explains that each of the five components and relevant principles need to be "present and functioning" and the five components must operate together in an integrated manner for the system of internal control to be considered effective.While adopting the 2013 Framework, management will need to assess the applicability of the principles within each component of internal control and determine whether or not they have been adequately addressed within the current system of internal control and adequately documented.

The impact of the 2013 Framework on management's assessment of the effectiveness of ICEFR (*i.e.*, to comply with SOX Section 404) will depend on how a company applied and interpreted the concepts in the 1992 Framework. For example, an existing system of internal control may not clearly demonstrate or document that all the relevant principles are present and functioning. COSO developed illustrative Tools for Assessing Effectiveness of a System of Internal Control & Internal Control over external reporting (ICEFR).



Picture 1: Relationship between COSO Framework & SOX Compliances

JSOX

JSOX is the nickname/short form of Japan's Financial Instruments and Exchange Law, which was promulgated in June 2006. Inspired by corporate scandals such as the Kanebo, Livedoor, and Murakami Fund & Seibu Railway episodes, the law has been dubbed as the Japanese version of the Sarbanes-Oxley Act, hence JSOX.

The JSOX compliance requirements are similar to Sarbanes-Oxley Act. Section 302 (management certification) and Section 404 (management evaluation and report on internal controls) of the United States.

The so called JSOX requirements are incorporated in the legislative draft titled as "Financial Instruments and Exchange Laws" passed by DIET (The Japanese parliament). JSOX require the same internal controls over financial reporting as the US Act. This regulation is applicable to all Japanese public companies w.e.f. 1st April, 2008.

In the light of this regulation, the Business Accounting Council of the Japanese Financial services Agency framed & released "Standards and Practice Standards for Management Assessment and Audit Concerning Internal Control Over Financial Reporting". The Practice Standard provides guidance to both companies and auditors on Implementation of JSOX and considers issues faced by Section 404

of US SOX. The Practice standards are consists of 3 (three) Sections:

- Basic Framework of Internal control
- Assessment and report on internal control over Financial reporting
- Audit on Internal control over financial reporting.

This New Internal control framework is similar to the Committee of sponsoring Organisations of the Treadway Commission Report (COSO) report with two (2) additional elements included to take local Japanese conditions into account.

The JSOX internal control framework has four (4) primary control objectives as:

- Effectiveness and Efficiency of Business operations
- Reliability of financial reporting
- Compliance with Applicable Laws
- Safeguarding of Assets

To achieve the said four (4) objectives of Internal Control, management is required to design and effectively operate a process in which Six (6) internal control components are in place.

- Control Environment
- Risk assessment and response
- Control activities
- Information and communication
- Monitoring
- Response to IT

One difference between practice Standards and the COSO framework is that Practice Standards indicate "Safeguarding of Assets" an objective distinct from the other three and it also adds "Response to IT" in the basic five components.

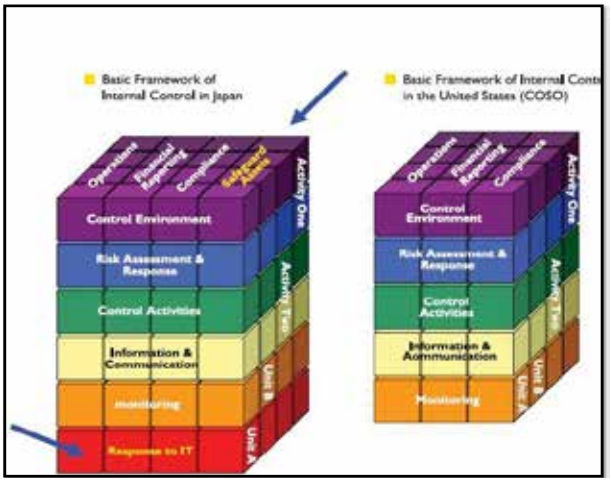


Image Courtesy of Control Solutions International
Picture 2: Relationship between COSO & JSOX compliances

The basic differences between SOX & JSOX

A comparison of JSOX with Section 404 of SO Act illustrates the number of similarities in the two regulations. Both approaches encourage the use of a top-down, risk-based approach to the evaluation of a company's internal controls over financial reporting. However, there are some notable differences, as highlighted in the table below. These differences will affect the compliance approach adopted by individual companies. The recent move by the U.S. regulators towards a more principles-based approach to compliance has narrowed this regulatory gap.

	SOX-Section 404	**JSOX**
Scope	**Audited Financial Statements including Disclosures and Footnotes**	Financial Statements, Footnotes and Unaudited Disclosures Relating to Financial Information
Coverage	**Parent Company and Consolidated Subsidiaries**	Parent Company, Consolidated Subsidiaries and Affiliated Companies (equity method)
Framework & Approach	**An Acceptable Internal Control Framework – Many Companies Use COSO: Top-Down, Risk-Based**	Tailored COSO: Top-Down,Risk-Based
Deficiency Classification	Control Deficiency Significant Deficiency Material Weakness	Control Deficiency Material Weakness
Auditor Opinion	**Opinion on Effectiveness of Internal Control**	Opinion on Management's Assessment Process

Achieving Internal Controls for SOX and JSOX in ERP environment

Both Sox & JSOX are concerned with estabilishing strict internal control of any Business systems. An effective Internal control is foundation of safe & sound organisational financial policy. Controls broadly involves checking, comparing, monitoring and taking action when results do not match. Control system is also cost money. As this cost is a non–product related overhead there is an incitement to minimise it by making control systems as effective and non–disruptive as possible. Today, IT systems plays an increasingly important role in automating controls and thus increasing their effectivenenss and efficiency.

Automation of Controls is about embedding the control in the business process and integrating and supporting the control activity in the ERP system workflow. This means that some controls are transformed from detective to preventive .

IT is of crucial importance in complying with SOX and JSOX both as a part of initial compliance project and is of integral part of the ongoing compliance process

Role of SAP-ERP in SOX, JSOX Compliances

The Sarbanes-Oxley Act, JSOX is geared towards data security and information integrity, and is designed to ensure that financial information is accurate, as well as to ensure the reliability and effectiveness of the system that produces it.

Data integrity is essential to the production of accurate financial reports,which is a the basic control in any ERP systems. These controls are always availble in the SAP which are receiving increasing attention because of corporate SOX/JSOX compliance efforts.

In SAPERP, these controls are divided into three (3) major groups which are known as **Inherent Controls, Configurable Controls, Security and Reporting controls:**

a. Inherent Controls are controls that come delivered with the system and cannot be changed via configuration. Some of these controls are as follows:

- All document-level postings record the time, date, and user who entered the document into SAP.
- The debits and credits for all FI postings must be in balance before the document can be saved.

- All document-level postings are given a unique document number.
- SAP provides online data analysis.
- SAP logs and records the history of program changes.
- SAP logs and records the history of the User profile changes and Role changes.

Generally speaking, system based controls are more reliable and sustainable, because they are not as a susceptible to human error or breakdowns as are people based controls. Because these controls are 'Hard-coded' into an application.

b. Configurable controls are controls which facilates complete, accurate and timely processing and reprting of transactions by Financial reporting applications inaccordance with management's prescribed criteria. These mainly consist of customising settings that prescribe how the system should operate to meet the organisation's needs. Some of these controls are as follows:

- Fiscal Year Settings
- Tolerance Levels
- Edit Checks
- Data entry validations
- Authorisation groups
- Payment Blocking
- User Defined error/warning messages
- Mandatory and/or System populated Fields
- Document blocking *etc.*

These Controls help to ensure that financial and operational information is reliable, operations

are performed efficiently and achieve effective results, assets are properly safeguarded, and that the actions and decisions of the organisation are in compliance with laws, regulations, and contracts. It is important to note that controls are not only used to comply with financial reporting regulations, but provide a balance between process optimisation and risk mitigation. Thus, by implementing controls, companies can increase data reliability and improve reporting and monitoring of information.

c. Security & Reporting Controls:

These controls are critical as they address the risks of Inaccurate and/or unauthorised changes, access to the application, the related database and network and the maintenance of the general IT environment that could impact the integrity of the Data produced by the SAP system.

SAP has several layers of security controls: profiles, roles,transaction codes,authorisation objects, fields and infotypes. From compliance perspective, risks are analysed across each of these layers. The Security controls includes Segregation of Duties (SOD), Sensititive Access (SA) and user provisioning. An SOD risk is present when an employee processes two incompatitble functions, such as 'Creation of Vendors' and "Processing of Invoices". SA risks occur when users have critical privilages such as the manintenance of bank details within a Vendor Master Record. User provisioning involves the granting , changing and removing of employee privilages to a system. All these compliances are the part of SOX 404 ITGC controls.

Generally the said Control consists the followings:

- Network Security
- Access Security
- Remote Function Calls (RFC)
- Web Services
- Password Security
- Central User Management (CUA)
- Change and Transport Management
- Table Maintenance and System Administration
- Patch Management
- Security Audit Log
- Monitoring

Data retention and risk management procedures mandated by the Sarbanes-Oxley Act and regional regulations have all placed unprecedented pressure on IT administrators to coordinate enterprise-wide tracking and organisation of compliance measures. As a result, SAP came out the it's GRC (Governance, Risk & Compliance) package. Which is currently based on business Objects (version 10.0)/ Business Intelligence Tools.

GRC is a management model that promotes the criteria unification, as well as communication and collaboration between different stakeholders in the management and control of the organisation.

The widespread interest in the "C' part of GRC was sparked by the SOX Act, specifically the need for publicly listed US companies to design and implement suitable governance and compliance controls for financial reporting.

Conclusion

SOX, JSOX is here to stay. Not only in US or JAPAN, but also in other parts of the world, companies are following them by enacting similar changes in their Accounting regulations.

It goes without saying that internal controls are not the only primary activity of business. The Challenge is to reach a level of control that achieves the control objectives of the Company, without disrupting the primary objective of the company which is to create value for its stakeholders.

SAP ERP system provides the company with basic internal control functionalities and a framework for control system management. The emergence of wide–reaching legislations such as Sox, JSox *etc.* has spurred an interest in compliance management as a corporate function. Corporations now are hiring compliance managers and looking into how compliance management and processes can be standardised and harmonised across organisational and geographical boundaries. Compliance is seen as something that can even create competitive advantage if it is done more effectively and more efficiently than the competitor. In order to sharpen the organisations competitive edge with a proactive, unified approach to governance, risk, and compliance. SAP AG launched GRC (Governance, Risk & Compliance) solutions which embed financial and operational controls of business processes. The goal of GRC is to help a company efficiently to put the policies and controls in place to address all its compliance obligations while at the same time gathering information which helps proactively to run the business. ■