SOX perspective of internal control & COSO, COBIT Control frameworks.

Applies to:

Business Experts.

Summary

An effective internal control is foundation of safe and sound organizational financial policy indeed it’s now the law (Section 404 of SOX).This article describes the COSO,COBIT Control framework and IT requirement of Section 404.It also briefs about the importance of IT in internal control.

Author: Charukesh R Gaikwad

Company: HCL Technologies Ltd.

Created on: 13 July 2007

Author Bio

Charukesh R Gaikwad is working as a GRC specialist at HCL Technologies Ltd.

Table of Contents

Internal Control:

An effective internal control is foundation of safe and sound organizational financial policy. Internal control means different things to different people. Internal control is a broadly defined process, carried out by people, designed to provide reasonable assurance regarding the achievement of the following three objectives that all businesses should strive towards attaining.

They are as follows:

- Economy and efficiency of operations, including achievement of performance goals and safeguarding of assets against loss.
- Reliable financial and operational data and reports.
- Compliance with laws and regulations.

SOX perspective:

Internal control is now the law. The Sarbanes-Oxley Act of 2002 was created to restore investor confidence in the public markets. Section 404 of the Act requires management to establish and maintain internal control and requires the independent auditors to evaluate the same.

Various overlapping but not identical definitions of internal control exists in different places; For the purpose of Section 404 Compliance, of Sarbanes-Oxley Act, internal control over financial reporting means the process that ensures reliability of financial reporting.

From a SOX perspective, controls must be established to ensure no changes to software have an unexpected impact on the integrity of financial data. Controls must ensure that all financial data is properly secured once software is deployed.

The Management is expected to base its evaluation of internal control over financial reporting on a recognized control framework. No particular framework is specified but the COSO framework is explicitly mentioned as being acceptable and meeting SEC criterion.

COSO: The Committee of Sponsoring Organization

The Committee of Sponsoring Organization of the Treadwell Commission (COSO) defined Internal Controls in a broad fashion that can be described as a process or set of processes designed to address operating efficiencies and effectiveness and reliability of financial reporting and compliance with laws and regulations

Key Concepts

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is effected by people. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

The overall goal of COSO is to keep company profitable, achieving its mission and minimizing surprises. To achieve this goal, Control objectives fall into three categories:

- Operational: Promote efficiency of operations and reduce risk of assets loss
- Financial: Help ensure the reliability of financial statements
- Compliance: Help ensure compliance with applicable laws and regulations

COSO Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process

1. Control Environment:
    - Foundation for all other components of control
    - Integrity, ethical values, competence, authority, responsibility
2. Risk Assessment:
    - Identifying and analyzing relevant risks.
3. Control Activities:
    - Policies that ensure management directives are carried out
    - Approval and authorizations, verifications, evaluations, safeguarding assets security and segregation of duties
4. Information and Communication Systems:
    - Relevant information identified, captured and communicated timely
    - Access to internal and externally generated information
    - Information flow allows for management action
5. Monitoring:
    - Assess control system performance over time
    - Ongoing and separate evaluations
    - Management and supervisory activities

These five components provide the framework for effective internal control over financial reporting and in similar fashion provide a framework more generally for disclosure controls and procedure. They provide the context for evaluating internal control over financial reporting.

For each of the five components, COSO provides several attributes. For each attribute COSO provides point of focus; For each point of focus, more granular criterion may be developed to support the assessment

Section 404 IT Controls Requirements

1. Security
    - Application and platform based
    - Focused on applications that may impact financials and supporting infrastructure
    - Requires secure operating systems, database, network, firewalls and infrastructure
    - Auditors will look for excessive access; lack of segregation of duties; inadequate approval of access; they will be testing key processes to determine that they are effective
2. Change Control

- Need to ensure that procedures are in place to control and ensure proper approval of changes to production
- Technical controls must tightly limit and control developer access to production

3. Disaster Recovery
    - Focus will be on basic backup and recoverability of financial data
4. IT Governance
    - Focus will be on determining of there are clear policies, procedures, and communications within IT
    - Is there clear segregation of duties?
5. Development And Implementation Activities
    - Proper controls need to be built in before a new system or system changes go in the production environment
    - Auditors may evaluate new financial systems; data conversion and testing are critical

The Importance of IT in Internal Control over Financial Reporting:

According to Public Company Accounting and Oversight Board (PCAOB) "The nature and characteristics of a company's use of information technology in its information system affect the company's internal control over financial reporting"

For most organizations, IT is critical to the financial reporting process. Financial and routine business applications are commonly used to initiate, authorize, record, process and report transactions

Relevant IT controls include:
Application controls - those that are embedded in financial and business applications .
General computer controls – underlying infrastructure components that support the applications

Application Control:

- Controls embedded within software programs to prevent or detect unauthorized transactions.
- Controls that ensure the completeness, accuracy and validity of processing transactions.

Examples of application controls:

- Balancing control activity within the system
- Check digits
- Predefined data listings
- Data reasonableness tests
- Logic tests, range limits, etc.

General control

- Administration - planning and controlling IT activities
- Logical Security Controls - access control
- Accounting Systems Development - application system development life cycle
- Accounting Systems Change Management - change control and authorization
- Packaged Software Evaluation - maintenance of software packages
- System Software - development and maintenance of infrastructure support software
- Data Center/Network Operations - backup, recovery and contingency planning, job scheduling, performance and monitoring

COBIT: Control Objectives for Information and related Technology

The internal control framework (COSO) recommended for Sarbanes Oxley compliance by the SEC, addresses the topic of IT controls, but does not dictate requirements for control objectives and activities. As such the Industry sentiment is that COSO does not address the specific concerns of IT with sufficient fidelity.

To address the IT gaps, the IT Governance Institute (ITGI) developed the Control Objectives for Information and related Technology (COBIT) COBIT plugs into the over-arching COSO framework and is recognized as an industry standard for addressing SOX IT concerns. About 15% of COBIT is related to software engineering. It includes over three hundred specific 'control objectives' and includes a framework and audit guides for over 30 information technology processes. Overall, COBIT is organized into six components, Executive Summary, Management Guidelines, Framework; Control Objectives, Implementation Toolset, Audit Guidelines

Pros

- Complete IT control framework available
- Gaining acceptance as standard approach
- Supported by leading bodies ISACA / ITGI
- Backed by excellent academic research

Cons

- Complexity – 34 processes, 318 control objectives
- Guidelines only – no specific control information
- No supporting process flows, procedures etc

ITIL and ISO 17799

Apart from COSO and COBIT the other two bodies of knowledge ITIL and ISO 17799 are excellent sources of practice information. They can be used to leverage process improvements.

ITIL (the IT Infrastructure Library), is an authoritative source of descriptive IT best practices, notably in operations and service management

ISO 17799 (the International Organization for Standardization's code of practice for information security management) is an excellent standard for IT security.

Integration of COSO, COBIT, and ITIL provides a sustainable model for compliance and a tightly controlled infrastructure.

Related Content

- Internal Control-Integrated framework Executive Summary
- Internal Control over financial reporting
- Section 404 IT Control Requirements
- COBIT forums and Information

Disclaimer and Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.