Articles/View Points 4

Sarbanes & Oxley Act and COSO Guidelines: An Integrated Framework for Risk Management

Arvind Shendye
Senior Consultant,
Protiviti, Kuwait

Prof. Utkarsh Jain
Assistant Professor, SIBM, Pune
E-mail: utkarshjain@sibm.edu

Prof. Kaustubh Medhekar
Associate Professor, SIBM, Pune
E-mail: kaustubh_medhekar@sibm.edu

Introduction

The major scandals in the US during the early 2000s lead to the emergence of the Sarbanes & Oxley Act (SOX), which tries improve corporate governance practices. It applies to all companies, whose shares are listed on the stock exchanges under the jurisdiction of the U.S. Securities and Exchange Commission (SEC). The goal of the SOX is to ensure the accuracy and reliability of published financial information, and therefore the main part of the said Act deals with the proper administrative routines, procedures and control Activities.

The purpose of the Act is to review the legislative audit requirements and to protect investors by ensuring the accuracy and adequacy of corporate disclosures. The Act covers issues such as establishing a public company accounting oversight board, auditor independence, and corporate responsibility and enhanced financial disclosures. It also significantly tightens accountability standards for directors,corporate executives ,auditors, securities analysts and legal counsel.

The simplest way to comply with the Sarbanes& Oxley (SOX) Act is to incorporate the Committee of Sponsoring Organizations (COSO) integrated Risk Management Framework. According to the Sarbanes& Oxley Act it is not mandatory for an entity to follow COSO Framework; however it is the easiest, effective and efficient way to comply the requirements of the Act. As the COSO Integrated Risk Management Framework is recommendatory, an organization may design its own risk management Framework to

protect the organization from any kind of financial risk.
COSO, a nonprofit commission established in 1992 formalized the concept of internal control and proposed a Framework for evaluating its effectiveness. The Framework effectively integrates various types of risk that pose as threats to an organization. COSO developed a Risk management integrated Framework which covers all the aspects to protect an organization from any threat. The COSO Framework views internal controls as consisting of the following aspects:

I) First Aspect:

1) **Control Environment-** This aspect covers integrity and the ethical values of an organization, including its code of conduct, involving top management and Board of Directors. It seeks to set an internal environment which gives a robust ethical standard in order to conduct the business with integrity and transparency.
2) **Risk Assessment-** Risk management is a management process of identifying potential risks that could result in misstated financial statements and developing actions to address those risks. It also covers identification of the risk appetite in accordance with the nature of the business, geographical location, stakeholders' requirement etc. Risks should be assessed on an inherent and a residual basis. The three major aspects of the risk which require emphasis here are Identification, Measurement and Prioritization of the risk. Management needs to design processes to identify potential risks arising business transactions develop mechanisms to address those risks. The process needs to set the magnitude of risk commensurate with factors such as the nature of the business, geographical location, and stakeholder's expectations.
3) **Control Activities-** These Activities are usually thought of as "The Internal Controls." They include segregation of duties, account reconciliations and information processing controls that are designed to safeguard the assets and enable an organization to timely prepare reliable financial statements. An organization must have the basic documents, policies and procedures as a part of the risk management system which should cover areas like segregation of duties, Specifications on authority, Delegation of authority/responsibility etc.
4) **Information And Communication-** Internal and external reporting process include an assessment of the technological environment. All relevant information should be identified, captured and communicated in a specified format and within an acceptable time frame to enable employees to execute their responsibilities.
5) **Monitoring-** Assessing the quality of an organization's internal control over a long period of time and taking actions, when required, to ensure that potential risks for the organization are continuously monitored.

II) Second Aspect

1) **Operations-** This aspect deals with effective mechanisms to deploy appropriate

resources to achieve intended objectives.

2) **Financial Reporting-** This aspect focuses on how transparent the financial reports are and the extent to which one can rely on information given in the financial statements.
3) **Compliance-** The particular aspects emphasizes on the compliance with the applicable legislations and regulatory Framework

III) Third Aspect

1) **Units And Activities-** This aspect requires the entities following the COSO Framework to apply the risk management Framework to various subunits and business Activities on an individual level, rather than the entire business unit as a whole. The risk assessment and monitoring is required to be done at subunit level of business.
2) **Risk Assessment Approach-** Two separate approaches have been developed for risk assessment under the COSO Framework; which are "Bottom Up" & "Top Down" Approach.
3) **Bottom Up Approach-** Bottom Up is considered as a traditional approach to risk assessment. The Primary emphasis is given on the controls and rather than identification and assessment of risk which are inherent in the business processes. Appropriate controls are integrated within the business processes to identify and mitigate the risk.
4) **Top Down Approach-** Top Down Approach first tries to ascertain potential risk in the processes and sub-processes. Once the potential risks have been identified, then the emphasis is placed on structuring a control system to mitigate the potential risk. Top Down Approach is considered a better approach to risk assessment and mitigation as it requires to focus on the risks first and then on the design of the controls for risk mitigation. Top Down approach is accepted by SEC (Security Exchange Commission of US) and approved by PCAOB (Public Company Accounting Oversight Board). Also according to Auditing Standard 5 issued by PCAOB (An Audit of Internal Control over Financial Reporting that is integrated with an Audit of Financial Statements) this approach is accepted and approved. According to Section 404 of the Sarbanes & Oxley Act 2002; assessment of the internal controls should be performed using top down risk assessment approach. Thus the Top Down Approach has been explicitly accepted by Auditing standards and various other statutory guidelines as a more superior method for risk identification and mitigation.

The other major concept that requires some discussion here is Enterprise Risk Management (ERM) to completely comprehend the COSO Framework. The concept of ERM was introduced by COSO in the late nineties. According to the Trade way commission definition of ERM, "Enterprise Risk Management is a process, effected by entity's board of directors, management and other personal, applied in strategy setting and across the enterprise, designed to identify potential events that may affect

the entity, and manage the risk to be within its risk appetite, to provide reasonable assurance regarding the achievements of entity's objective."

Accordingly the COSO report on Enterprises Risk Management encapsulates,

1) **Aligning risk appetite and strategy**- Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanism to manage related risk.
2) **Enhancing risk response decision-**Enterprises Risk Management provides the rigor to identify and select among alternative risk responses: risk avoidance, reduction, sharing and acceptance.
3) **Reducing operational surprises and losses-** Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
4) **Identifying multiple and cross enterprise risk-** Every enterprise faces a myriad of risk affecting different parts of the organization, and enterprise risk management facilitates effective risk response to the interrelated impacts, and integrated responses to multiple risks.
5) **Seizing opportunities-** By considering a full range of potential events management is positioned to identify and proactively realize opportunities.
6) **Improving deployment of capital-** Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

In the last few years, COSO Framework has gained acceptance for Sarbanes & Oxley Act compliance. Since a number of companies to whom Sarbanes & Oxley Act is applicable operate in India, all the big four consulting firms have set up separate consulting domains to enable companies to comply with Sarbanes & Oxley Act by implementing and adopting COSO Framework of risk management. With the ever increasing complexity of business structures, it will be exciting to see how and where the COSO Framework leads us.

References

1. www.COSO.org