1

CONCEPT OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEM

Chapter Overview

This chapter introduces the concepts relating to IT Governance, Risk Management and best practices like CoBIT

Major Topics / Sub-head

I. Key Concepts in Governance

i. Governance:

The term Governance is derived from the Greek verb- meaning "to steer". A Governance system typically refers to all the means and mechanisms that will enable multiple stakeholders (people who are interested or impacted by the Company- i.e shareholders, employees, management, public, government etc) in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance in order to satisfy specific enterprise objectives.

ii. Enterprise Governance:

It can be defined as a set of responsibilities and practices exercised by the Board and executive management with the objective of:

a. Providing strategic direction

b. Ensuring objectives are achieved

c. Ascertaining risks are managed appropriately

d. Verifying that organisations resources are used responsibly.

iii. Corporate Governance:

A system by which a Company or Enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance.

It includes the following:

a. Structures and processes for the direction and control of companies

b. Concerns relationship amongst management (CEO, CFO, CTO etc.), Board of Directors, the controlling shareholders and other stakeholders

c. Contributes to sustainable economic development by enhancing company performance.

Some of the factors which contribute to good corporate governance includes a system of good internal controls, elimination of conflict of interests, establishing audit committee, establishing a risk management process, due compliance with laws and regulations.

Such practices ensure organisations meet the stake holders needs without comprising their interest- the Directors being accountable to shareholders for discharge of their duties in fiduciary capacity. (Trust/good faith)

iv. IT Governance:

It is defined as "System by which IT activities in a Company are directed and controlled to achieve the business objectives with a view to meeting the stake holders needs"

IT Governance will entail a system wherein the Directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

IT Governance is derived from Corporate Governance- it is a sub-set focusing on IT.

II. Benefits of Governance

i. Achieving enterprise objectives - by managing mission and strategy- implementing transparency in decision making process.

ii. Ensuring IT is put to proper use- ensuring they are used responsibly.

iii. Integrating business processes within the enterprise

iv. Defining a stable organisational structure.

v. Implementing a holistic governance framework- where customers, business processes and IT services are integrated.

vi. Aligning IT Decisions in line with business decisions

III. Two Dimensions to Governance

The concept of good governance by itself would not make the organisation successful- it needs to be integrated with need for the enterprise to create wealth to stakeholders.

Hence there is a need to balance the two aspects- conformance and performance.

i. Conformance or Corporate Governance Dimension:

This focusses on regulatory requirements. It covers aspects like role of Chairman, CEO, Composition and function of the BoD, Committees of the Board- ex: Audit Committee, Control Assurance and Risk Management etc.

This aspect is generally driven by regulatory requirements and may be subject to assurance or audit process. There are established oversight mechanisms for the BoD- like committees mainly of non-executive directors- like audit committee which ensure corporate governance processes are effective.

ii. Performance or Business Governance:

This dimension focusses on strategy and value creation with the objective of helping the Board take strategic decisions, understanding the risk appetite and its key performance drivers. It is pro-active, business oriented and takes a futuristic/forward looking view.

Unless corporate governance, performance governance is not amenable to an oversight mechanism or to any standards – varies from company to company. Overall strategy is the responsibility of the Board. It may help to create a committee like a strategy committee to fill the oversight gap.

IV. IT Governance and related concepts

i. Key practices to determine the status of IT Governance

Some of the key practices which determine the status or extent of implementation of IT Governance in an enterprise are:

i. Who is responsible for directing, controlling and executing decisions ?

ii. How are those decisions made ?

iii. What is the information required to make those decisions ?

iv. What decision making mechanisms are required ?

v. How does the management handle exceptions ?

vi. Is there a monitoring process for governance results ? Are there process improvements being undertaken ?

ii. Benefits of IT Governance

i. Increased value to business- delivered through IT initiatives

ii. Increased user satisfaction amongst users of IT (i.e all departments)

iii. IT becomes agile and flexible to support the needs of the business units- alignment of IT with business.

iv. Better utilization of IT Costs and investments

v. Improved management of IT and management of IT Related Risks

vi. IT driven compliance with corporate policies, applicable legislations and laws

vii. Optimal utilization of IT resources

viii. Ensures IT related processes are **overseen effectively and transparently**

ix. **Confirms compliance with legal** and regulatory requirements

iii. How to achieve Benefits of IT Governance ?

i. Ownership is defined and agreed

ii. It is relevant and the links to business strategy

iii. Realistic time frames set for benefit realization

iv. Risks and assumptions associated with benefit realization are factored

v. Key performance measurements (KPI) are identified

vi. Data about the KPI is available in timely manner and duly collected.

V. Corporate Governance, Enterprise Risk Management (ERM) and Internal Controls

Corporate Governance

It is defined as a system by which business corporations are directed and controlled. It spells out the distribution of rights and responsibilities amongst different participants in the corporation- like the BoD, shareholders and other stake holders. It spells out rules and procedures for making decisions on corporate affairs.

Some of the **best practices relating to Corporate Governance** include the following:

i. Clear assignment of responsibilities and decision making authority

ii. Establishing a mechanism for interaction and co-operation amongst BoD, Senior Management and Auditors.

iii. Implementing strong internal controls , risk management functions

iv. Special monitoring of risks arising due to conflict of interest

v. Financial and managerial incentives to act in an appropriate manner

vi. Appropriate information flows internally and to the public

Enterprise Risk Management (ERM)

According to the Committee of Sponsoring Organisation (COSO) framework, ERM is defined as a process effected by the Board, management across the enterprise to :

a. Apply strategy setting relating to Risk

b. Manage risk within the risk appetite (i.e how much risk the management is willing to take)

c. To provide reasonable assurance regarding achievement of entity objectives

Controls in an organisation are to be holistic and comprehensive. They should consider the overall business objectives, processes, organisational structure, technology deployed and risk appetite.

An overall risk management strategy is to be adopted and implemented across the organisation. Such a strategy should consider implementation of information and associated risks while formulating IT Security Policy and controls.

Internal Controls

Internal Controls are defined as policies, procedures, practices and enterprise structures that are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected or corrected.

According to Securities Exchange Commission (SEC) of the US, Internal Controls on Financial Reporting (ICFR) are to provide a reasonable assurance on the reliability of financial reporting. It includes the following:

i. Maintenance of records that is in reasonable detail accurate and fairly reflective of transactions

ii. Reasonable assurance that transactions are recorded as necessary to help preparation of financial statements

iii. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition or use of Company's Assets

As per COSO, internal controls are comprised of 5 interrelated components:

i. **Control environment:** Each business process needs to be categorized based on its criticality and suitable control environment needs to be developed.

ii. **Risk Assessment:** Control environment must include assessment of risks associated with each business process.

iii. **Control Activities:** Controls to be developed to manage , mitigate and reduce the risk associated with each business process

iv. **Information and Communication:** These systems enable an organisation to capture and exchange the information needed to run its business processes

v. **Monitoring:** Continuous monitoring of control environment is required to ensure it is adapted to changing circumstances.

Clause 49 of SEBI's listing agreement also seeks implementation of risk management and internal controls and holds the senior management responsible for such implementation.

VI.IT Strategy, IT Steering Committee

Strategic planning is the process by which top management determines overall organisational purposes and objectives and how they are achieved. It is process of deciding on objectives of the enterprise, on resources required to achieve these objectives. It takes a holistic view of current IT environment, the future direction and initiatives required to migrate to desired future environment.

It outlines the approach of the enterprise and is formulated by the senior management. Based on the strategy relevant policies and procedures are formulated.