1

Concepts of Governance and Management of Information Systems

Learning Objectives
• To understand the concept of Governance, Risk and compliance (GRC) and relationship between governance and management; • To understand the Role of Information Technology (IT), how to align Information Systems (IS) Strategy with business strategy and ensure Business Value from use of IT; • To understand the business impact of IS risks, different types of Information Systems Risks and how IS Risk management is implemented; • To understand the key aspects of IT Compliance and the specific role and responsibilities of top management relating to IT-GRC; • To understand the key concepts of Governance of Enterprise IT (GEIT) and using COBIT as framework of GEIT; and • To understand role of Information Systems Assurance in GEIT.
Task Statements
• To distinguish among key aspects of enterprise governance, corporate governance, GEIT, GRC and IT Management; • To examine the role of IT in formulating IT strategy, aligning IT as per business strategy and identify key processes and practices required for ensuring value creation from IT; • To review IS Risk management strategy based on different types of risks and their impact; • To identify regulatory aspects of IT Compliance and the specific role and responsibilities in IT-GRC implementation; • To use best practices frameworks such as COBIT as framework of GEIT to meet enterprises need for implementing GEIT; and • To provide Information Systems Assurance in GEIT.
Knowledge Statements
• To know Governance, Risk and compliance and relationship between governance and management;

- To know the role of IT, aligning IS Strategy in business strategy and ensuring business value from IT.
- To know IS Risk Management Strategy, business impact of IS risks and different types of IS Risks;
- To know IT Compliance overview – Responsibilities of top management for IT-GRC;
- To know the concepts of GEIT and using GEIT frameworks such as COBIT; and
- To know the role of Information Systems Assurance in GEIT.

1.1 Introduction

The primary objective for the inclusion of the 'Information Systems Control and Audit' paper at the Final Level of the Chartered Accountancy course is to provide conceptual understanding of different aspects of IT risks, security, controls and auditing of IT processes. This paper leverages and builds on the advanced IT Training and enables to understand the enterprise level aspects of governance, risk, compliance, assurance as applicable to enterprises. The topics covered here are closely integrated with Auditing and Assurance Paper. While updating this paper, the primary rationale has been to ensure the coverage of the latest concepts of **Governance, Risk and Compliance (GRC)**, which has been a regulatory requirement not only for listed enterprises but also for all types of enterprises. Further, implementing GRC in an IT environment requires updated knowledge and skills based on the latest developments and the best practices and this is sought to be provided by this paper. Students are advised to read these topics not only from examination point of view but keeping in mind the fact that these topics are highly relevant to their work as articles and in their careers whether they seek to be employed in enterprises or self-employed.

The topics have been organized so as to link all of them topics together from the macro perspective of Governance, risk, compliance and assurance to the micro perspective and implementation level so that a blend of both concepts as well as the practical aspects could be provided. This knowledge will equip CA students with holistic approach to IT assurance rather than function oriented IS controls and audit perspective. This will provide the required competency to meet the challenges of IT environment, which they face in their work area.

Before moving forward, it is important to understand the overall learning objective of the Paper, which is: *"To develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant"*. The detailed learning objectives are given below:

- To understand the key concepts of Governance, Risk and Compliance aspects in enterprises as relevant to IT;
- To identify and review IT risks, security, controls and risk management approach;
- To assess the impact on controls and organizational structure on account of integration of technological applications and resources into operational processes;

- To assess Business Continuity Plans of enterprises for adequacy from perspective of going concern;
- To assess information systems acquisition, development and implementation strategy including review of Systems Development Life Cycle process;
- To understand how to perform auditing including collecting and evaluating evidence in an IT environment; and
- To understand and apply IT best practices and impact of emerging technologies.

It is noteworthy to mention here that understanding of this chapter on "Governance, Risk and Compliance aspects in enterprises as relevant to IT" is very important as it provides the macro concepts and provides a solid platform for understanding of the topics, which are covered in the later chapters.

1.2 Key Concepts of Governance

It is needless to emphasize that enterprises whether they are commercial or non-commercial, exist to deliver value to their stakeholders. Delivering value is achieved by operating within value and risk parameters that are acceptable and advantageous, and by using resources including IT responsibly. In the rapidly changing environment that most enterprises operate in, swift direction setting and agility to change are essential. Senior management is responsible for ensuring that the right structure of decision-making accountabilities are shared among many people in the enterprise and when accountability is shared, governance comes into play.

- **Governance:** The term "**Governance**" is derived from the Greek verb meaning "to steer". Governance refers to "all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language." It relates to "the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions. A governance system typically refers to all the means and mechanisms that will enable multiple stakeholders 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. Governance is a very general concept that can refer to all manner of organizations and can be used in different ways. We shall here understand what is meant by the term- **Enterprise Governance**.
- **Enterprise Governance: Enterprise Governance** can be defined as: 'The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.' Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit. Examples include codes on corporate governance and financial reporting standards.

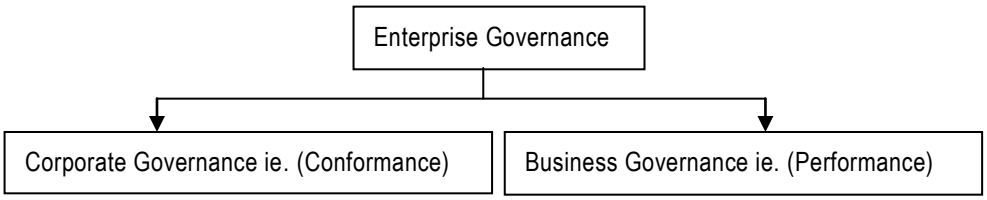

Fig. 1.2.1: Enterprise Governance Framework*

The enterprise governance constitutes the entire accountability framework of an organization as it involves establishing accountability for decision-making. Enterprise Governance has two dimensions as shown in the Fig. 1.2.1:

- Corporate Governance or Conformance, and
- Business Governance or Performance.

These dimensions are discussed as follows:

- **Corporate Governance or Conformance: Corporate Governance** is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.

  Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business to protect shareholders' interest. Corporate Governance drives the corporate information needs to meet business objectives.

  Good corporate governance requires sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of Audit Committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. These are intended to guide companies to achieve their business objectives in a manner such that this those who are entrusted with the resources or power to run the companies to meet stakeholder needs without compromising the shareholders' interest. Legally, the directors of a Company are accountable to the shareholders for their actions in directing and controlling the business, and for the actions of the company's employees, who are in the position of trust to discharge their responsibilities in the best interest of the company. Corporate governance is thus necessary for the purpose of monitoring and measuring their performance.

* http://www.cimaglobal.com/Documents/ImportedDocuments/cid_enterprise_governance__feb08.pdf.pdf

Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. These might include committees composed mainly or wholly of independent non-executive directors, particularly the audit committee or its equivalent in countries where the two tier board system is the norm. Other committees are usually the nominations committee and the remuneration committee. The **Sarbanes Oxley Act of US** and the Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

Good corporate governance is important and it is critical so that any weakness in this area is addressed properly. However, good corporate governance by itself cannot make an organization successful. There is always a risk that inadequate attention is paid to the need for enterprises to create wealth or stakeholder value. Hence, it is important to remember that strategy and performance are also very important. The key message of enterprise governance is that an enterprise must balance the two dimensions of conformance and performance so as to meet stakeholder requirements and ensure long-term success.

- **Business Governance or Performance:** The **Business Governance** is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required.

The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. There is thus an oversight gap in respect of strategy. One of the ways of dealing with this lacuna is to establish a strategy committee of similar status to the other board committees which will report to the board.

1.3 Information Technology and Governance

The usage of IT is rapidly increasing in most of the large enterprises and also to a great extent even in small and medium enterprises and is at the core of most of the key business operations. Further, there is an increasing thrust on corporate governance by regulators

encompassing governance, risk management and controls. The use of IT covering all key aspects of business processes of an enterprise impacts not only 'how information is processed' but also 'how computerized information systems are used for strategic and competitive advantage'. Internal controls are integral part of information systems of an enterprise. Hence, it is important to understand 'how information systems are organized' and 'how controls are integrated'. Thus, as IT is used extensively in enterprises and encompasses all aspects of business, the relevant internal controls get embedded in the IT systems.

1.3.1 Benefits of Governance

Before we proceed further, let us understand the major benefits of governance. These can be summarized as follows:

- Achieving enterprise objectives by ensuring that each element of the mission and strategy are assigned and managed with a clearly understood and transparent decisions rights and accountability framework;
- Defining and encouraging desirable behavior in the use of IT and in the execution of IT outsourcing arrangements;
- Implementing and integrating the desired business processes into the enterprise;
- Providing stability and overcoming the limitations of organizational structure;
- Improving customer, business and internal relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework; and
- Enabling effective and strategically aligned decision making for the IT Principles that define the role of IT, IT Architecture, IT Infrastructure, Application Portfolio and Frameworks, Service Portfolio, Information and Competency Portfolios and IT Investment & Prioritization.

Based on the above, it can be seen that IT is an integral part of the governance. The successful design and deployment of information systems using IT, determines the success of an enterprise. Hence, it is critical to ensure that the required controls are implemented not only from IT perspective but also from management and regulatory perspective. This requires that the controls are implemented from Governance perspective using a holistic approach and has involvement of the senior management as required. Implementing IT Governance as subset of enterprise governance ensures that implementation of IT meets all the stakeholder requirements including regulators and management. Regulatory requirements mandate not only implementation of governance but also its independent evaluation. Hence, auditors are required to evaluate these aspects in their roles as internal or external auditors. As IT proliferates, there is increasing demands for pro-active objective assessments of governance, risk, compliance and controls of information systems.

1.4 Corporate Governance and IT Governance

There is no doubt to say that IT is a key enabler of corporate business strategy. **Chief Executive Officers (CEO), Chief Financial Officers (CFO)** and **Chief Information Officers**

(CIO) agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives. IT has to provide critical inputs to meet the information needs of all the required stakeholders or it can be said that enterprise activities require information from IT activities in order to meet enterprise objectives. Hence, corporate governance drives and sets IT governance.

There are multiple definitions of IT Governance. However, one of the well-known definitions is: "IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs". Hence, the overall objective of IT governance is very much similar to corporate governance but with the focus on IT. Hence, it can be said that there is an inseparable relationship between Corporate Governance and IT Governance or IT Governance is a sub-set of Corporate or Enterprise Governance.

1.5 IT Governance and Governance of Enterprise IT (GEIT)

Let us now specifically understand the key concepts of IT Governance and the distinction between IT Governance and GEIT. Although the terms IT Governance and Governance of Enterprise IT (GEIT) are used inter-changeably, the term GEIT is more macro and broader in its scope of coverage. In this chapter, we shall be using both the terms as relevant and as specifically required as some of the regulatory requirements still refer to the term IT Governance.

1.5.1 IT Governance

The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT. IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT. The active distribution of decision-making rights and accountabilities among different stakeholders in an organization and the rules and procedures for making and monitoring those decisions to determine and achieve desired behaviors and results. It may be noticed that governance and IT governance are similar in their definition and approach except that in case of IT governance the focus is on IT and related areas.

1.5.2 Key practices to determine status of IT Governance

Some of the key practices, which determine the status of IT Governance in the enterprise, are:

- Who makes directing, controlling and executing decisions?
- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

As per regulatory requirements and best practices frameworks of Governance of enterprise IT, it is important for the Board of Directors and senior management to play critical roles in evaluating; directing and monitoring IT Effectiveness of the IT governance structure and processes are directly dependent upon the level of involvement of the board and senior management. Different levels of the framework require different tools, techniques, and standards addressing specific needs of an effective IT governance structure, which consists of the organizational structure, leadership, and processes that ensure IT support of the organization's strategies and objectives.

1.5.3 Benefits of IT Governance

The benefits, which are achieved by implementing/improving governance or management of enterprise, IT would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;
- Improved agility in supporting business needs;
- Better cost performance of IT;
- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;
- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

For every defined benefit, it is critical to ensure that:

- Ownership is defined and agreed;
- It is relevant and links to the business strategy;
- The timing of its realization of benefit is realistic and documented;
- The risks, assumptions and dependencies associated with the realization of the benefits are understood, correct and current;
- An unambiguous measure has been identified; and
- Timely and accurate data for the measure is available or is easy to obtain.

1.5.4 Governance of Enterprise IT (GEIT)

Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective

enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

1.5.5 Benefits of GEIT

These are given as follows:

- It provides a consistent approach integrated and aligned with the enterprise governance approach.
- It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.
- It ensures that IT-related processes are overseen effectively and transparently.
- It confirms compliance with legal and regulatory requirements.
- It ensures that the governance requirements for board members are met.

1.5.6 Key Governance Practices of GEIT

The key governance practices required to implement GEIT in enterprises are highlighted here:

- **Evaluate the Governance System:** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- **Direct the Governance System:** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and
- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

1.6 Corporate Governance, Enterprise Risk Management and Internal Controls

Various prominent frauds committed by some large enterprises across the world including India in the last two decades have awakened regulators to the need of mandating the implementation of corporate governance integrated with Enterprise Risk Management and Internal controls. The concept of Corporate Governance has succeeded in attracting a good deal of public interest because of its importance for the economic health of corporations, protect the interest of stakeholders including investors and the welfare of society, in general. As discussed earlier, Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as, the Board, managers, shareholders and other stakeholders, and spells

out the rules and procedures for making decisions on corporate affairs. Some of the best practices of corporate governance include the following:

- Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors;
- Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;
- Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
- Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. traders);
- Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition; and
- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

1.6.1 Enterprise Risk Management (ERM)

In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise. Hence, the type of controls implemented in information systems in an enterprise would depend on this risk management strategy. The **Sarbanes Oxley Act (SOX)** in the US, which focuses on the implementation and review of internal controls as relating to financial audit, highlights the importance of evaluating the risks, security and controls as related to financial statements. In an IT environment, it is important to understand whether the relevant IT controls are implemented. How controls are implemented would be dependent on the overall risk management strategy and risk appetite of the management. SOX have used **Committee of Sponsoring Organizations (COSO)** as one of the important guidelines for implementing risk management and internal controls.

The Executive Summary of Enterprise Risk Management — Integrated Framework published by COSO of the Treadway Commission highlights the need for management to implement a system of risk management at the enterprise level. Enterprise Risk Management deals with risks and opportunities affecting value creation or preservation, defined as follows: “Enterprise Risk Management is a process, effected by an entity’s board of directors, management and

other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant. IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise

1.6.2 Internal Controls

The **(The US Security and Exchange Commission) SEC's** final rules define "Internal Control over financial reporting" as a "process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's Board of Directors, Management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company;
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements."

Under the final rules, a company's annual report must include "An Internal Control report of management" that contains:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting;
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting; and

- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting."

(a) Responsibility for Implementing Internal Controls: SOX made a major change in internal controls by holding Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) personally and criminally liable for the quality and effectiveness of their organization's internal controls. Part of the process is to attest to the public that an organization's internal controls are effective. Internal controls can be expected to provide only a reasonable assurance, not an absolute assurance, to an entity's management and board. An organization must ensure that its financial statements comply with **Financial Accounting Standards (FAS)** and **International Accounting Standards (IAS)** or local rules via policy enforcement and risk avoidance methodology called "Internal Control." There must be a system of checks and balances of defined processes that lead directly from actions and transactions reporting to an organization's owners, investors, and public hosts.

(b) Internal Controls as per COSO: In a computerised environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if an organization's management sets up a system of internal controls. According to COSO, Internal Control is comprised of five interrelated components:

- **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on. For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.
- **Risk Assessment:** This includes the elements that identify and analyze the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.
- **Information and Communication:** These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to

discharge their responsibilities. These are associated with control activities regarding information and communication systems of the entity that acts as one of the component of internal accounting system. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions. This includes the elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

(c) Clause 49 of the listing agreements issued by SEBI in India is on similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation. Further, it also provides for certification of these aspects by the external auditors.

It may be noted that COSO and COBIT together have been internationally used as best practices framework for complying with SOX. The details of how IT compliance can be best implemented or reviewed by using best frameworks such as COBIT 5 is covered in the further sections.

1.7 Role of IT in Enterprises

In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to decision support systems to online transactions/services. IT has not only automated the business processes but also transformed the way business processes are performed. The way in which business processes are performed/services rendered and how an organization is structured could be transformed through right deployment of IT. It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

The extent of technology deployment also impacts the way internal controls are implemented in an enterprise. Further, extensive organization restructuring or business process re-engineering may be facilitated through IT deployments. Implementing IT has to consider not only implementation of IT controls from conformance perspective but also IT could be a key enabler for providing strategic and competitive advantage. This requires that senior management considers IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services. This makes it imperative to develop an IT strategy, which is aligned with business strategy and ensures value creation and facilitates benefit realization from the IT investments.

1.7.1 Business and IT Strategy

Management Strategy determines at the macro level the path and methodology of rendering services by the enterprise. Strategy outlines the approach of the enterprise and is formulated

by the senior management. Based on the strategy adapted, relevant policies and procedures are formulated. From business strategy perspective, IT is affecting the way in which enterprises are structured, managed and operated. One of the most dramatic developments affecting enterprises is the fusion of IT with business strategy. Enterprises can no longer develop business strategy separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business planning and the incorporation of effective financial and management controls within new systems. Management primarily is focused on harnessing the enterprise resources towards achievement of business objectives. This would involve the managerial processes of planning, organizing, staffing, directing, coordinating, reporting and budgeting.

Every enterprise regardless of its size needs to have an internal control system built into its enterprise structure. Control is defined as "Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieve and undesired events are prevented or detected and corrected". We are aware that auditors could be involved in providing assurance requiring review of Information Systems as implemented from control perspective. However, auditors may also be required to provide consulting before, during or after implementation of information systems strategy. It becomes imperative for the auditor to understand the concepts of the enterprise strategy as relevant. Hence, auditors must have good understanding of management aspects as relevant to deployment of IT and IT strategy. This would include understanding of the IS Strategy, policies, procedures, practices and enterprise structure, segregation of duties, etc.

IT organizations should define their strategies and tactics to support the organization by ensuring that day-to-day IT operations are delivered efficiently and without compromise. Metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of enterprise leaders. Internal audit can determine whether the linkage of IT metrics and objectives aligns with the organization's goals, adequately measure progress being made on approved initiatives, and express an opinion on whether the metrics are relevant and useful. Additionally, auditors can validate that metrics are being measured correctly and represent realistic views of IT operations and governance on a tactical and strategic basis.

1.7.2 IT Steering Committee

Planning is essential for determining and monitoring the direction and achievement of the enterprise goals and objectives. As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the steering committee. Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management. As the members comprise of function heads of departments, they would be responsible for taking decisions relating to their departments as required. The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises. The key functions of the committee would include of the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

1.8 IT Strategy Planning

Planning is basically deciding in advance 'what is to be done', 'who is going to do' and 'when it is going to be done'. There are three levels of managerial activity in an enterprise:

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved. Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among those businesses.
- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and

implementation. Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise. Management should establish processes to capture and report feedback from business process owners and users regarding the quality and usefulness of long and short-range plans. The feedback obtained should be evaluated and considered in future IT planning.

1.8.1 IT Strategic Planning Process

The strategic planning process has to be dynamic in nature and IT management and business process owners should ensure a process is in place to modify the IT long-range plan in a timely and accurate manner to accommodate changes to the enterprise's long-range plan and changes in IT conditions. Management should establish a policy requiring that IT long and short-range plan are developed and maintained. IT management and business process owners should ensure that the IT long-range plan is regularly translated into IT short-range plans. Such short-range plans should ensure that appropriate IT function resources are allocated on a basis consistent with the IT long-range plan. The short-range plans should be reassessed periodically and amended as necessary in response to changing business and IT conditions. The timely performance of feasibility studies should ensure that the execution of the short-range plans is adequately initiated.

1.8.2 Objective of IT Strategy

The primary objective of IT strategy is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives. Alignment of the strategic IT plans with the business objectives is done by clearly communicating the objectives and associated accountabilities so they are understood by all and all the IT strategic options are identified, structured and integrated with the business plans as required.

1.8.3 Classification of Strategic Planning

In the context of Information Systems, **Strategic Planning** refers to the planning undertaken by top management towards meeting long-term objectives of the enterprise.

IT Strategy planning in an enterprise could be broadly classified into the following categories:

- Enterprise Strategic Plan,
- Information Systems Strategic Plan,
- Information Systems Requirements Plan, and
- Information Systems Applications and Facilities Plan.

These aforementioned plans are discussed as follows:

(i) Enterprise Strategic Plan: Business Planning determines the overall plan of the enterprise. The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate. It is the primary plan prepared by top management of the enterprise that guides the long run

development of the enterprise. It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives, a specification of constraints that apply, and a listing of priorities. In an IT environment, it is important to ensure that the IT plan is aligned with the enterprise plan.

(ii) **Information Systems Strategic Plan:** The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment. This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals. Some of the enablers of the IS Strategic plan are:

- Enterprise business strategy,
- Definition of how IT supports the business objectives,
- Inventory of technological solutions and current infrastructure,
- Monitoring the technology markets,
- Timely feasibility studies and reality checks,
- Existing systems assessments,
- Enterprise position on risk, time-to-market, quality, and
- Need for senior management buy-in, support and critical review.

(iii) **Information Systems Requirements Plan:** Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems. This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information. Based on the information architecture requirements of an enterprise, the Information Systems Requirements Plan has to be drawn up so as to meet the information requirements of the enterprise. Some of the key enablers of the information architecture are as follows:

- Automated data repository and dictionary,
- Data syntax rules,
- Data ownership and criticality/security classification,
- An information model representing the business, and
- Enterprise information architectural standards.

The information system requirements plan defines information system architecture for the information systems department. The architecture specifies the major organization functions needed to support planning, control and operations activities and the data classes associated with each function. The business planning will determine the information needs of an enterprise. The information architecture will determine

information needs and flow in an enterprise. Based on the information architecture, the organization structure is determined. This in turn will lead to specific information systems, which include the relevant IT and related processes. For example, depending on the business, information architecture and organization structure, the enterprise will decide whether to acquire or develop the solution and the relevant controls which are required to meet the business requirements.

(iv) **Information Systems Applications and Facilities Plan:** On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan. This plan includes:

- Specific application systems to be developed and an associated time schedule,
- Hardware and Software acquisition/development schedule,
- Facilities required, and
- Organization changes required.

Senior management is responsible for developing and implementing long and short-range plans that enable achievement of the enterprise mission and goals. Senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the enterprise's long- and short-range plans. IT long and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the enterprise. Strategic plan period could vary from 1 year to 3 years. It is important to ensure that the IT strategic plans are aligned with the business strategic plans as IT is ultimately used for achieving business objectives. Strategic planning could be done by the top management or by the steering committee. Strategic planning facilitates in putting organization objectives into time-bound plans and action. Comprehensive planning helps to ensure an effective and efficient enterprise. Strategic planning is time and project oriented, but must also address and help determine priorities to meet business needs.

1.8.4 Key Management Practices for Aligning IT Strategy with Enterprise Strategy

The key management practices, which are required for aligning IT strategy with enterprise strategy, are highlighted here:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.

- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals, extent of stakeholder satisfaction with scope of the planned portfolio of programs and services and the percentage of IT value drivers, which are mapped to business value drivers.

1.8.5 Business Value from Use of IT

Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost. The benefit of implementing this process will ensure that enterprise is able to secure optimal value from IT-enabled initiatives services and assets, cost-efficient delivery of solutions and services, and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.

The key management practices, which need to be implemented for evaluating 'Whether business value is derived from IT', are highlighted as under:

- **Evaluate Value Optimization:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.
- **Direct Value Optimization:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.

- **Monitor Value Optimization:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented. Some of the key metrics, which can be used for such evaluation, are:

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where expected benefits realized;
- Percentage of IT enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

1.9 Risk Management

Enterprise Risk Management and IT Risk Management are key components of an effective IT governance structure of any enterprise. Effective IT governance helps to ensure close linkage to the enterprise risk management activities, including Enterprise Risk Management (ERM) and IT Risk Management. IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite. The risk assessment approach adapted has to consider business impact of IS risk and different types of risks. There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile. This section will provide an overview of related terms like threats, vulnerabilities etc., IS Risks and exposures and risk mitigation strategies, which can be adapted by the organizations.

1.9.1 Information Systems Risks and Risk Management

There are numerous changes in IT and its operating environment that emphasizes the need to better manage IT related risks. Dependency on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. Increasing disclosures of information system disasters and increasing electronic fraud, in turn, drive this. The management of IT related risks is now being understood as a key part of enterprise governance.

Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. This security has to be implemented as per required control system envisaged by the management of the enterprise. Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them. Based on the point of impact of risks, controls are classified as Preventive, Detective and Corrective. Preventive controls prevent risks from actualizing. Detective controls detect the risks as they arise. Corrective controls facilitate correction.

The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

1.9.2 Sources of Risk

The most important step in risk management process is to identify the sources of risk, the areas from where risks can occur. This will give information about the possible threats, vulnerabilities and accordingly appropriate risk mitigation strategy can be adapted. Some of the common sources of risk are as follows:

- Commercial and Legal Relationships,
- Economic Circumstances,
- Human Behavior,
- Natural Events,
- Political Circumstances,
- Technology and Technical Issues,
- Management Activities and Controls, and
- Individual Activities.

Broadly, risk has the following characteristics:

- Loss potential that exists as the result of threat/vulnerability process;
- Uncertainty of loss expressed in terms of probability of such loss; and
- The probability/likelihood that a threat agent mounting a specific attack against a particular system.

1.9.3 Related Terms

Various terminologies relating to risk management are given as follows:

Asset: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:

- They are recognized to be of value to the organization.
- They are not easily replaceable without cost, skill, time, resources or a combination.
- They form a part of the organization's corporate identity, without which, the organization may be threatened.
- Their Data Classification would normally be Proprietary, Highly confidential or even Top Secret.

It is the purpose of Information Security Personnel to identify the threats against the risks and the associated potential damage to, and the safeguarding of Information Assets.

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. Some examples of vulnerabilities are given as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

Missing safeguards often determine the level of vulnerability. Determining vulnerabilities involves a security evaluation of the system including inspection of safeguards, testing, and penetration analysis.

Simply, Vulnerability can be referred as the weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from flaws on the software's design, defects in its implementation, or problems in its operation. Some experts also define 'vulnerability' as opening doors for attackers. Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- 'Allows an attacker to execute commands as another user' or
- 'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
- 'Allows an attacker to pose as another entity' or
- 'Allows an attacker to conduct a denial of service'.

Threat: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.

Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

Exposure: An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

Attack: An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.

Basically, it is a set of actions designed to compromise **CIA (Confidentiality, Integrity or Availability**), or any other desired feature of an information system. Simply, it is the act of trying to defeat Information Systems (IS) safeguards. The type of attack and its degree of success determines the consequence of the attack.

Risk: Formally, risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, and risk analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization. Risk assessment includes the following:

- Identification of threats and vulnerabilities in the system;
- Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
- The identification and analysis of security controls for the information system.

Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap is caused by:

- Widespread use of technology;
- Interconnectivity of systems;

- Elimination of distance, time and space as constraints;
- Unevenness of technological changes;
- Devolution of management and control;
- Attractiveness of conducting unconventional electronic attacks against organizations; and
- External factors such as legislative, legal and regulatory requirements or technological developments.

It means there are new risk areas that could have a significant impact on critical business operations, such as:

- External dangers from hackers, leading to denial of service and virus attacks, extortion and leakage of corporate information;
- Growing potential for misuse and abuse of information system affecting privacy and ethical values; and
- Increasing requirements for availability and robustness.

New technology provides the potential for dramatically enhanced business performance, improved and demonstrated information risk reduction and security measures. Technology can also add real value to the organization by contributing to interactions with the trading partners, closer customer relations, improved competitive advantage and protected reputation.

Counter Measure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure. For example, well known threat 'spoofing the user identity', has two countermeasures:

- Strong authentication protocols to validate users; and
- Passwords should not be stored in configuration files instead some secure mechanism should be used.

Similarly, for other vulnerabilities, different countermeasures may be used.

The relationship and different activities among these aforementioned terms may be understood by the Fig. 1.9.1.

Any risk still remaining after the counter measures are analyzed and implemented is called **Residual Risk**. An organization's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimized, but it can seldom be eliminated. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk can be managed.

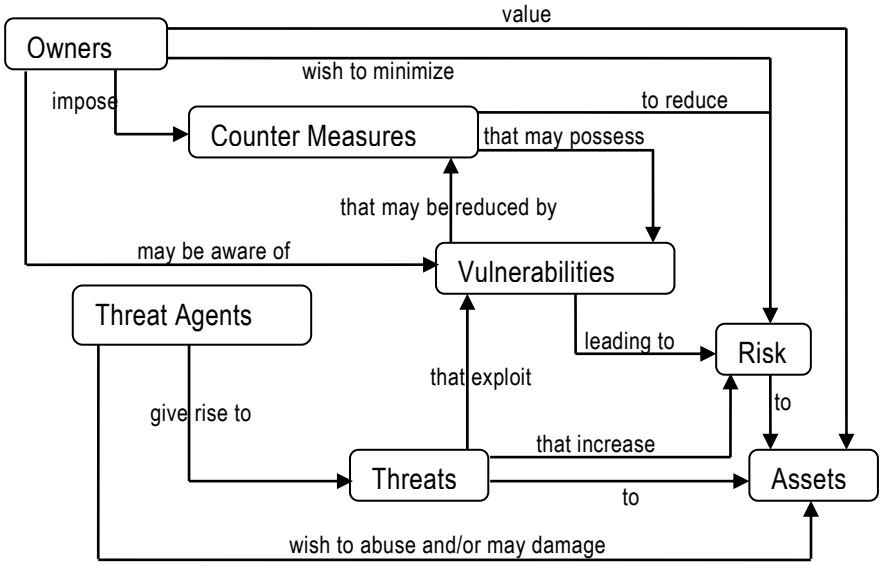

Fig. 1.9.1: Risk and Related Terms*

1.9.4 Risk Management Strategies

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained and illustrated below:

- **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk**. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk**. Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

* Source: http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF p.14

- **Treat/mitigate the risk**. Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back**. Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

1.9.5 Key Governance Practices of Risk Management

The key governance practices for evaluating risk management are given as follows:

- **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;
- **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and
- **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

1.9.6 Key Management Practices of Risk Management

Key Management Practices for implementing Risk Management are given as follows:

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
- **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
- **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

1.9.7 Metrics of Risk Management

Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are as follows:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;

- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

1.10 COBIT 5 Business Framework – Governance and Management of Enterprise IT

We have already discussed that Enterprise Governance is not only a management requirement but is also mandated by law. IT is a key enabler of enterprises and forms the edifice on which the information and information systems are built. Implementing internal controls is not only a management requirement but is now a regulatory requirement too. In an IT environment, embedding the right level of controls within the information systems, which provides information to users securely and safely and as per business requirements, is critical not only for ensuring business success but is also a key requirement for the survival of the enterprise. In implementing internal controls in an IT environment, the legacy approach of considering IT and its contents as boxes to be secured by the IT department is fraught with extreme risk. Both from regulatory as well as enterprise perspective, senior management need to be involved in providing direction on how governance, risk and control are implemented using a holistic perspective based on the need for harnessing the power of information and information technology from a business perspective.

Control Objectives for Information and Related Technology (COBIT) is a set of best practices for Information Technology management developed by **Information Systems Audit & Control Association (ISACA)** and IT Governance Institute in 1996. ISACA develops and maintains the internationally recognized COBIT framework, helping IT professionals and enterprise leaders fulfill their IT Governance responsibilities while delivering value to the business. The latest ISACA's globally accepted framework COBIT 5 is aimed to provide an end-to-end business view of the governance of enterprise IT that reflects the central role of IT in creating value for enterprises.

COBIT 5 is the only business framework for the governance and management of enterprise Information Technology. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. As per COBIT 5, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. This section explains the need for using the approach and latest thinking provided by globally recognized framework COBIT 5 as a benchmark for reviewing and implementing governance and management of enterprise IT. It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help enterprises to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities.

1.10.1 Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues. COBIT 5 is a set of globally accepted principles, practices, analytical

tools and models that can be customized for enterprises of all sizes, industries and geographies. It helps enterprises to create optimal value from their information and technology. COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes, including non-profit and public sector and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT;
- User satisfaction with IT engagement and services;
- Reduced IT related risks and compliance with laws, regulations and contractual requirements;
- Development of more business-focused IT solutions and services; and
- Increased enterprise wide involvement in IT-related activities.

1.10.2 Integrating COBIT 5 with Other Frameworks

COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO). COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as **Information Technology Infrastructure Library (ITIL)**, **The Open Group Architecture Framework (TOGAF)** and ISO 27001. It is also aligned with The GEIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behavior that the governing body (e.g., board) should evaluate, direct and monitor. Thus, COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language. The framework and resulting enablers should be aligned with and in harmony with (amongst others) the:

- Enterprise policies, strategies, governance and business plans, and audit approaches;
- Enterprise risk management framework; and
- Existing enterprise governance organization, structures and processes.

1.10.3 Components in COBIT

- **Framework -** Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;
- **Process Descriptions -** A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

- **Management Guidelines -** Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
- **Maturity Models -** Assess maturity and capability per process and helps to address gaps.

1.10.4 Benefits of COBIT 5

COBIT 5 frameworks can be implemented in all sizes of enterprises.

- A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.
- The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
- Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.
- COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.
- COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.
- The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
- COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

1.10.5 Customizing COBIT 5 as per Requirement

COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, it can be applied to meet needs related to:

- Information security,
- Risk management,
- Governance and management of enterprise IT,
- Assurance activities,
- Legislative and regulatory compliance, and
- Financial processing or CSR reporting.

Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5. Further, the above examples show specific areas based on which best practices can be extracted from COBIT 5.

1.10.6 Five Principles of COBIT 5

COBIT 5 simplifies governance challenges with just five principles. The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and

technology investment and use for the benefit of stakeholders. These principles are shown in Fig. 1.10.1 and are discussed below:

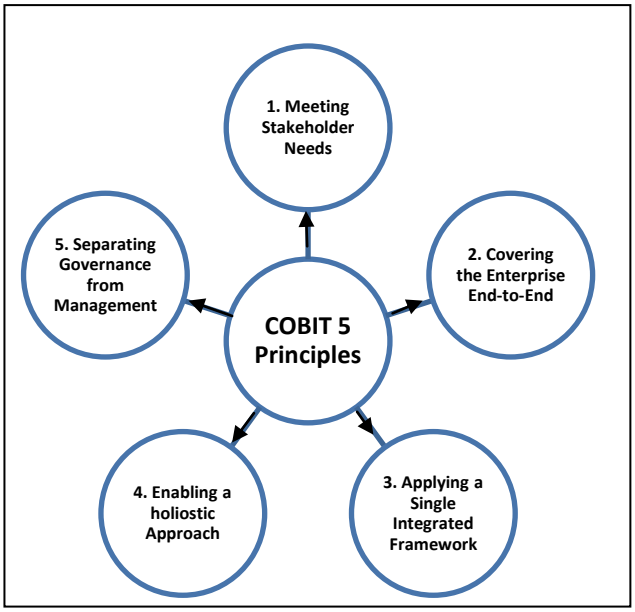

Fig. 1.10.1: Five Principles of COBIT 5

- **Principle 1: Meeting Stakeholder Needs:** Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

  Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organization, risk appetite, etc.), and requires a customized governance and management system. Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

- **Principle 2: Covering the Enterprise End-to-End:** COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by

everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone - internal and external that is relevant to governance and management of enterprise information and related IT. The end–to-end governance approach that is the foundation of COBIT 5 is depicted in Fig. 1.10.2 showing the key components of a governance system.

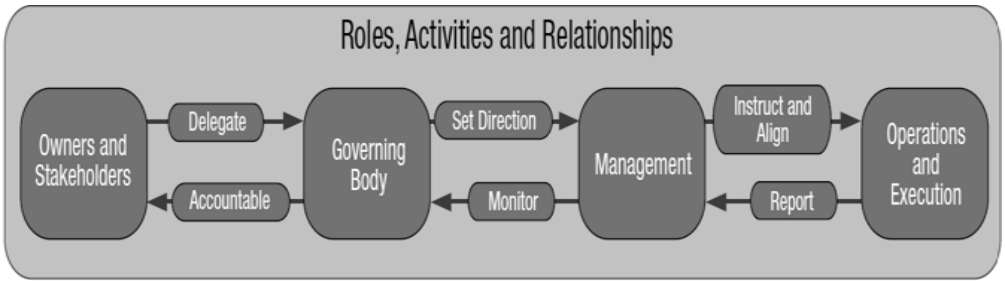

Fig. 1.10.2: Key Components of a Governance System*

- **Principle 3: Applying a Single Integrated Framework:** There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.
- **Principle 4: Enabling a Holistic Approach:** Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.
- **Principle 5: Separating Governance from Management:** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

1.10.7 COBIT 5 Process Reference Model

COBIT 5 includes a Process Reference Model, which defines and describes in detail a number of governance and management processes of enterprise IT into two main process domains- **Governance** and **Management** as shown in Fig. 1.10.3. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation. Incorporating an operational model and a common language for all parts of the enterprise

* Source: www.isaca.org

involved in IT activities is one of the most important and critical steps towards good governance. It also provides a framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers, and integrating best management practices.

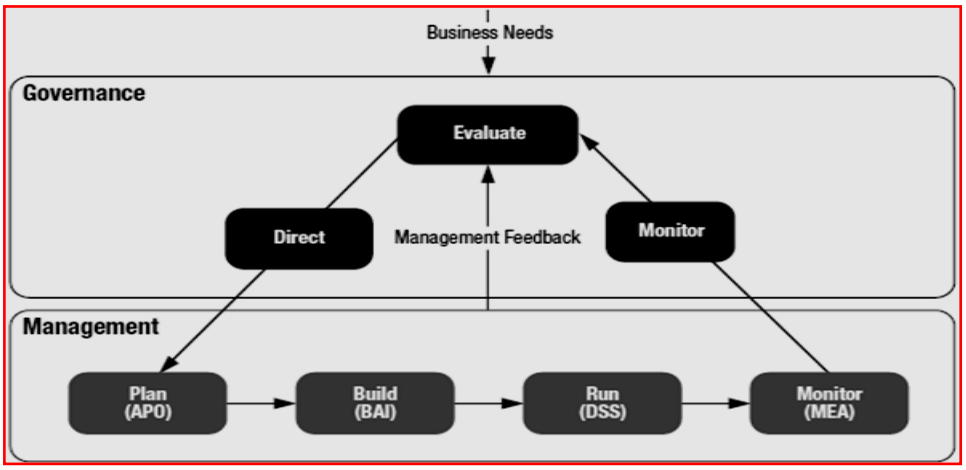

Fig. 1.10.3: Key Areas of Governance and Management*

Governance: It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most of the enterprises, overall governance is the responsibility of the Board of Directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

Management: It contains four domains, in line with the responsibility areas of **Plan, Build, Run and Monitor (PBRM)**, providing the end-to-end coverage of IT in alignment with the direction set by the governance body to achieve the enterprise objectives. In most of the enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

The COBIT 5 process reference model is the successor of the COBIT 4.1 process model, incorporating the both the Risk IT and Val IT frameworks. The complete COBIT 5 enabler model includes a total of 37 governance and management processes as mentioned below:

Governance Processes

- Evaluate, Direct and Monitor Practices (EDM) – 5 processes (EDM01 to EDM05)

Management Processes

- Align, Plan and Organize (APO) - 13 processes (APO01 to APO13)

* Source: www.isaca.org

- Build, Acquire and Implement (BAI) - 10 processes (BAI01 to BAI10)
- Deliver, Service and Support (DSS) - 6 processes (DSS01 to DSS06)
- Monitor, Evaluate and Assess (MEA) - 3 processes (MEA01 to MEA03)

1.10.8 Seven Enablers of COBIT 5

Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers, which are shown in Fig. 1.10.4 and discussed as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

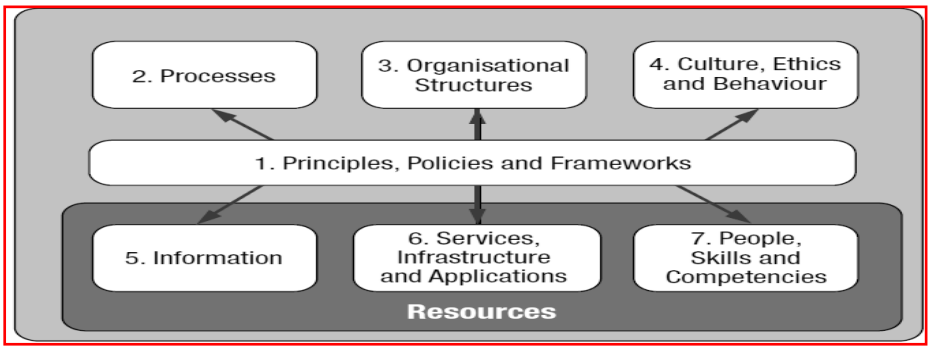

Fig. 1.10.4: Seven Enablers of COBIT 5*

- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

* Source: www.isaca.org

1.10.9 Risk Management in COBIT 5

The COBIT framework provides excellent guidance on risk management strategy and practices from governance and management practice.

The Governance domain contains five governance processes, one of which focuses on stakeholder risk-related objectives: "**EDM03: Ensure risk optimization**". This process ensures that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed. This process provides guidance on how to ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.

COBIT framework has management domain of "Align, Plan and Organize", which contains a risk-related process: "**APO12: Manage risk**". This process requires continually identifying, assessing and reducing IT-related risk within levels of tolerance set by enterprise executive management. The primary purpose of this process is to integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk. All enterprise activities have associated risk exposures resulting from environmental threats that exploit enabler vulnerabilities.

The combination of Governance practices of "EDM03: Ensure risk optimization" (which ensures that the enterprise stakeholders approach to risk is articulated to direct how risks facing the enterprise will be treated) and the management practices of "APO12 Manage risk" (which provides the enterprise risk management (ERM) arrangements that ensure that the stakeholder direction is followed by the enterprise) together ensured that Risk management covers the entire life cycle and covers both governance and management perspective. Further, detailed guidance is available in the form of specific practices and activities that are designed to treat related risk (avoid, educe/mitigate/control, share/transfer/accept). In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process including risk-related roles at each level of management as appropriate. A pictorial representation of various activities relating to risk management is given in Fig. 1.10.5:

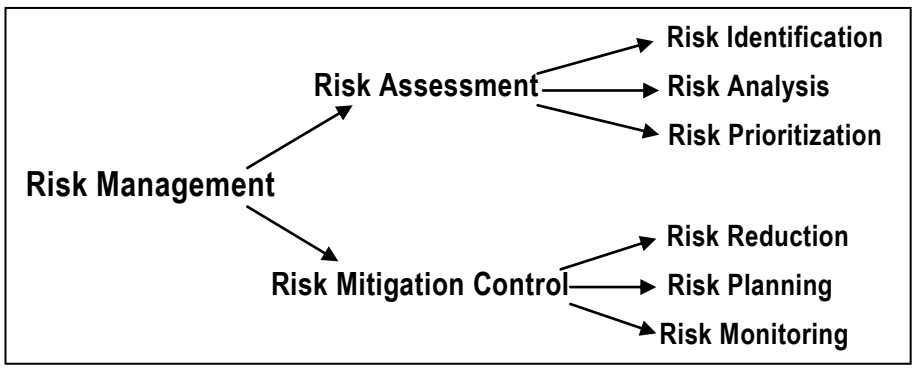

Fig. 1.10.5: Risk Management

1.10.10 Using COBIT 5 Best Practices for GRC

Although a GRC program (project) can be implemented primarily from a compliance perspective, it is advisable to consider business requirements also so as to optimize the investments made in implementing relevant processes, control structures and systems. GRC program implementation requires the following:

- Defining clearly what GRC requirements are applicable;
- Identifying the regulatory and compliance landscape;
- Reviewing the current GRC status;
- Determining the most optimal approach;
- Setting out key parameters on which success will be measured;
- Using a process oriented approach;
- Adapting global best practices as applicable; and
- Using uniform and structured approach which is auditable.

The responsibility of senior management in implementing and monitoring functioning of requisite GRC measures is not only a regulatory requirement but it also makes business sense as effective GRC implementation helps in meeting not only compliance but business requirements as well. Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented. It is advisable that the board should mandate adaption of a GEIT framework such as COBIT 5, as an integral part of enterprise governance development. COBIT 5 frameworks would provide the overall approach and based on this, relevant guidance can be selected from specific standards and good practices for designing specific policies, processes, practices and procedures. This ensures that appropriate governance processes and other enablers are developed and optimized so that GEIT operates effectively as part of normal business practice and becomes a supporting culture as demonstrated by top management. Alignment with COBIT 5 best practices would also result in faster and more efficient external audits since COBIT is widely accepted as a basis for IT audit procedures.

Successful implementation of GRC in enterprise can be measured in general by the assurance provided to the senior management on the adequacy of controls implemented. However, specific success of a GRC program can be measured by using the following goals and metrics:

- The reduction of redundant controls and related time to execute (audit, test and remediate);
- The reduction in control failures in all key areas;
- The reduction of expenditure relating to legal, regulatory and review areas;
- Reduction in overall time required for audit for key business areas;

- Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
- Improvement in timely reporting of regular compliance issues and remediation measures; and
- Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.

1.11 IT Compliance Review

Failures of some large enterprises in the last decade due to lack of adequate level of ERM has compelled regulators to mandate its enforcement thus necessitating compliance with **Governance, Risk and Compliance (GRC)**. Effective implementation of ERM requires consideration of multiple factors such as using a holistic approach, which encompasses enterprise from end-to-end, top down approach, best practices framework, technology deployment, related regulatory requirements and business needs. As IT is a key enabler for most enterprises, it makes good economic sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance.

In the US, Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. In India, Clause 49 of listing agreement issued by **Security and Exchange Board of India (SEBI)** mandates similar implementation of enterprise risk management and internal controls as appropriate for the enterprise. Further, the Information Technology Act, which was passed in 2000 and amended in 2008 provides legal recognition for electronic records and also mandates responsibilities for protecting information. The Act also identifies various types of cyber-crimes and has imposed specific responsibilities on corporate. Hence, it can be rightly said that implementing Governance, Risk, security and controls is not only a management requirement but is mandated by law, too. Hence, it is important for enterprises to be aware of and be well conversant of IT compliances and accordingly, implement processes and practices to manage these compliances both from conformance and performance perspective.

All listed Companies in India have to enter into an agreement with the Stock Exchange and this agreement is called the Listing Agreement. This agreement is more or less defined by SEBI and all Stock Exchanges have similar wordings. Apart from other clauses in the agreement some of the clauses in the listing agreement require additional disclosures from the listed companies and compliance with corporate governance and other requirements. One such clause is Clause 49 of the Listing Agreement that prescribes certain addition disclosure requirements and also corporate governance requirements. This requirement is similar to the requirement of the Sarbanes Oxley Act of the USA and there are similar legislations in Australia, Japan and other countries. In USA, the **Public Company Accounting Oversight Board (PCAOB)** has come out with detailed guidelines on Compliance by Auditors and Companies under the Act. In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members, which focuses primarily on audit requirements.

The Internal control requirements of Clause 49 are similar to SOX requirements. For example: Under section F.i.6, the agreement requires the Directors to cover their internal controls systems and their adequacy in the Management Analysis and Discussion. Under section V (c), the agreement requires the CEO/CFO to accept responsibility for establishing and maintaining internal controls for financial reporting and that they have evaluated the effectiveness of internal control systems of the company pertaining to financial reporting and they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and the steps they have taken or propose to take to rectify these deficiencies. Reporting on Internal control requirements are also mandated by the Indian Companies Act, 1956 for all companies and a separate annexure to the audit report has to be provided by auditors as per **Companies (Auditor's Report) Order, 2003 (CARO)**. Hence, implementing internal controls is mandated by law not only for listed companies but all companies.

1.11.1 Compliance in COBIT 5

The Management domain of "**Monitor, Evaluate and Assess (MEA)**" contains a compliance focused process: "**MEA03 Monitor, Evaluate and Assess Compliance with External Requirements**". This process is designed to evaluate that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. This require that the enterprise has processes in place to obtain assurance and that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance. The primary purpose of this process is to ensure that the enterprise is compliant with all applicable external requirements.

Legal and regulatory compliance is a key part of the effective governance of an enterprise, hence its inclusion in the GRC term and in the COBIT 5 Enterprise Goals and supporting enabler process structure (MEA03). In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with externally imposed legislative or regulatory requirements but also with enterprise governance-determined principles, policies and procedures. In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process, which also include a compliance-related role.

The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities. The Governance activities related to GEIT are covered in the five processes of the Governance domain. The Risk management process and supporting guidance for risk management across the GEIT space meet the compliance need of regulations such as SOX and other similar regulations across the world. In fact, COBIT combined with COSO has been the most widely used framework for implementing IT controls as part of enterprise risk management to meet governance requirements. COBIT has a specific focus on compliance activities within the framework and explains how they fit within the complete enterprise picture. Inclusion of GRC arrangements within the business framework for GEIT helps enterprises to avoid the main issue with GRC arrangements as silos of activity instead provides a comprehensive and holistic approach for ensuring compliance.

1.11.2 Key Management Practices of IT Compliance

COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. The practices are given as follows:

- **Identify External Compliance Requirements:** On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.
- **Optimize Response to External Requirements:** Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider industry standards, codes of good practice, and best practice guidance for adoption and adaptation
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements
- **Obtain Assurance of External Compliance:** Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

1.11.3 Key Metrics for Assessing Compliance Process

Sample metrics for reviewing the process of evaluating and assessing compliance with external laws & regulations and IT compliances with internal policies are given as under:

- **Compliance with External Laws and Regulations:** These metrics are given as follows:
  - Cost of IT non-compliance, including settlements and fines;
  - Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;
  - Number of non-compliance issues relating to contractual agreements with IT service providers; and
  - Coverage of compliance assessments.
- **IT Compliance with Internal Policies:** These metrics are given as follows:
  - Number of incidents related to non compliance to policy;
  - Percentage of stakeholders who understand policies;
  - Percentage of policies supported by effective standards and working practices; and
  - Frequency of policies review and updates.

1.12 Information System Assurance

In the rapidly changing digital world, enterprises are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business

objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations. This dynamic changing environment provides a challenge for Chartered Accountants (as assurance providers) to provide assurance with the required level of confidence. However, with the right type of skills and toolsets, this provides an excellent opportunity for Chartered Accountants to act as consultants, who provide relevant IT enabled services. A key component of this knowledge base is usage of globally accepted good practices and frameworks and developing a holistic approach, which meets the needs of stakeholders.

1.12.1 Using COBIT 5 for Information System Assurance

Auditors will have to understand the business processes of the enterprises and organization structure to be effective. This understanding of the business process has to be coupled with understanding of the enterprise's policies, procedures and practices as implemented. Any enterprise executes its business operations through its staff. These staff needs to have defined job responsibilities, which are provided in the organization structure. The organization structure needs to have internal control structure. IT implementation in the enterprise makes it imperative that the internal control structure is built into the IT as deployed. Further, IT impacts the way business operations could be performed and internal controls are implemented. Hence, it is critical for auditors to understand the organization structure of the enterprise being audited as relevant to the objectives and scope of the assignment.

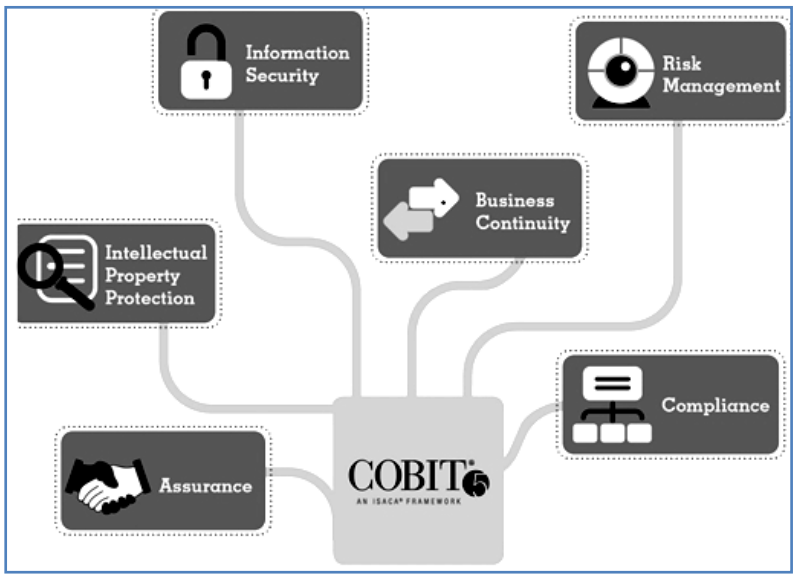

Fig. 1.12.1: Assurance Needs of COBIT 5*

COBIT 5 has been engineered to meet expectations of multiple stakeholders. It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management,

* Source: www.isaca.org

employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc. It is written in a non-technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers; regulators for understanding and addressing IT related issues as relevant to them. Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, regulators and auditors (internal/external) for implementing or evaluating Governance and management practices from an end-to-end perspective. COBIT has been used as an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001 etc. have been integrated into overall enterprise governance. The Fig. 1.12.1 provides sample examples of the different assurance needs, which can be performed by using COBIT 5.

1.12.2 Evaluating IT Governance Structure and Practices by Internal Auditors

IT Governance can be evaluated by both external as well internal auditors. The following guidance is from internal audit perspective as issued by **The Institute of Internal Auditors (IIA)**. It outlines specific areas and critical aspects relating to governance structure and practices, which can be reviewed as part of internal audit. Internal audit activities in evaluating the IT governance structure and practices within an enterprise can evaluate several key components that lead to effective IT governance. These are briefly explained here.

- **Leadership:** The following aspects need to be verified by the auditor:
  - Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.
  - Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.
  - Determine how IT will be measured in helping the organization achieve these goals.
  - Review how roles and responsibilities are assigned within the IT organization and how they are executed.
  - Review the role of senior management and the board in helping establish and maintain strong IT governance.
- **Organizational Structure:** The following aspects need to be assessed by the auditor:
  - Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
  - This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. In addition, how IT mirrors the organization structure in its enterprise architecture should also be included.
- **Processes:** The following aspects need to be checked by the auditor:
  - Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding

processes and underlying systems.

- What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?

- **Risks:** The following aspects need to be reviewed by the auditor:
  - Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.
  - Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.
- **Controls:** The following aspects need to be verified by the auditor:
  - Assess key controls that are defined by IT to manage its activities and the support of the overall organization.
  - Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity.
  - Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.
- **Performance Measurement/Monitoring:** The following aspects need to be verified by the auditor:
  - Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

1.12.3 Sample Areas of GRC for Review by Internal Auditors

IIA provides areas, which can be reviewed by internal auditors as part of review of Governance, Risk and Compliance (GRC) areas. These are given as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
  - Promoting appropriate ethics and values within the organization;
  - Ensuring effective organizational performance management and accountability;
  - Communicating risk and control information to appropriate areas of the organization; and
  - Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that:
    - Organizational objectives support and align with the organization's mission;
    - Significant risks are identified and assessed;
    - Appropriate risk responses are selected that align risks with the organization's risk appetite; and
    - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
- **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.
- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
    - Achievement of the organization's strategic objectives;
    - Reliability and integrity of financial and operational information;
    - Effectiveness and efficiency of operations and programs;
    - Safeguarding of assets; and
    - Compliance with laws, regulations, policies, procedures, and contracts.
- **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
- **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

1.12.4 Sample Areas of Review of Assessing and Managing Risks

This review covers the Controls over the IT process of assessing and managing risks and is expected to provide assurance to the management that the enterprise has identified all the risks relevant to the enterprise/business as relevant to IT Implementation. In addition, it is also expected to provide assurance that it has appropriate risk management strategy to mitigate these risks so as to satisfy the business requirement of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors.

This review broadly considers whether the enterprise is engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks. The specific areas evaluated are:

- Risk management ownership and accountability;
- Different kinds of IT risks (technology, security, continuity, regulatory, etc.);
- Defined and communicated risk tolerance profile;
- Root cause analyses and risk mitigation measures;
- Quantitative and/or qualitative risk measurement;
- Risk assessment methodology; and
- Risk action plan and Timely reassessment.

1.12.5 Evaluating and Assessing the System of Internal Controls

COBIT 5 has specific process: "**MEA 02 Monitor, Evaluate and Assess the System of Internal Control**", which provides guidance on evaluating and assessing internal controls implemented in an enterprise. The objective of such a review is to:

- Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews;
- Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions; and
- Plan, organize and maintain standards for internal control assessment and assurance activities.

Performing this review would provide assurance on the transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risks.

The key management practices for assessing and evaluating the system of internal controls in an enterprise are given as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.

- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

1.13 Summary

The chapter has highlighted the need for implementing the right type of IT controls as IT is all pervasive in enterprises today. For implementing IT controls, it is important to consider not only the regulatory but also the management perspective so as to ensure that both conformance and performance perspectives are covered. The key concepts of governance, enterprise governance, corporate governance, IT governance and Governance of enterprise IT along with the Enterprise Risk Management and internal controls have been explained. This will enable to identify governance practices as implemented in enterprises and confirm their adequacy. This chapter has also provided an overview of the critical role of IT in achieving business objectives.

Risks are all pervasive and could lead to exposures, which could result in loss to enterprise. Hence, it is important to identify sources of risks, types of risks and exposures, the threats and vulnerabilities and the probability of occurrence and impact on the business. This is done through risk management strategy based on which risks are tolerated, terminated, treated, transferred or ignored depending on the cost and benefit analysis. Implementing risk management strategy is not only a management requirement but also a regulatory requirement. Usage of best practice guidance from frameworks such as COBIT enables enterprises to implement a holistic approach covering the complete life cycle of risk encompassing all aspects and ensures accountability is established both from governance and management perspective. Enterprises would be well served if they implement risk management not simply as a compliance issue but rather a new way of enhancing operational effectiveness and efficiency. This chapter has provided guidance and best practices for effective risk management which can be integrated with overall enterprise risk management and Governance.

IT compliance as part of Governance, Risk and Compliance under the umbrella of corporate governance is also discussed. This chapter has outlined the specific provisions pertaining to SOX, which has mandated the implementation of internal controls on management and its certification by external auditors. It has also provided the best practices guidance from COBIT 5, which can be applied for ensuring IT compliance within the enterprise. Clause 49 of listing agreement issued by SEBI of India and related provisions for implementing GRC are also discussed in the chapter.

The chapter has also provided a brief overview of COBIT 5 and highlighted the need for using globally accepted framework such as COBIT 5 for implementing GEIT. Information Technology increasingly impacts how electronic information and related controls are reviewed and accessed for providing compliance, assurance or consulting service for clients. Hence, it is imperative for auditors to update methodologies of how they provide services by using the relevant best practices and tools to ensure quality of services to clients. IT is an area which is a constant state of continuous improvement. Hence, it is vital for auditors to keep on updating knowledge and skills sets and explore innovative ways of delivering services using IT and related best practices.

Information Systems assurance is integral part of enterprise governance and this can be performed by internal as well as external auditors based on the scope and objectives of the review. As part of GEIT or GRC review, regulatory requirements mandate review of specific areas and certification to confirm whether the required Enterprise risk management and internal controls are in place. This chapter has provided a broad overview, sample areas and key management practices using best practices and guidance from COBIT 5 and IIA (The Institute of Internal Auditors) guidance. This could be used by external or internal auditors as per their requirement.