1. Concepts of Governance and Management of Information Systems

1.1 Key Concepts of Governance

1) 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."
- A governance system refers to all the means and mechanism 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.

2) 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.
- The enterprise governance constitutes the entire accountability framework of an organization as it involves establishing accountability for decision-making.
- Enterprise Governance has two dimensions:
  - Corporate Governance or Conformance, and
  - Business Governance or Performance.

i). Corporate Governance or Conformance –

- Corporate Governance is defined as the system by which a company is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance.
- Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders.
- This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of board of directors, Board committees, Controls assurance and Risk management.
- Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital.
- 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.
- Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit.

- Good corporate governance is important and it is critical so that any weakness in this area is addressed properly. Good corporate governance by itself cannot make an company successful.

ii). Business Governance or Performance –

- The Business Governance is pro-active in its approach. It is business oriented.
- 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 that can be applied intelligently for different types of enterprises as required.
- 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.

1.2 Benefits of Governance

- The major benefits of governance are summarized as follows:
  - ✦ Achieving enterprise objectives by ensuring that each element of the mission and strategy are assigned and managed with a clear 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.

1.3 Corporate Governance and IT Governance

- 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.
- **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, 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.

1.4 IT Governance and Governance of Enterprise IT (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.

1.4.1 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.

1.4.2 Key practices to determine status of IT Governance

- 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.
- **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?

1.4.3 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.

1.4.4 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.

1.4.5 Benefits of GEIT

- These are given as follows:
  - ✦ It provide 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.

1.4.6 Key Governance Practices of GEIT

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

i). Evaluate the Governance System –

- ✦ Continually identify and engage with the enterprises stakeholders, document an understanding of requirements and make judgment on current & future design of governance of enterprise IT;

ii). 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.

iii). 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.

1.5 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.

1.5.1 Corporate Governance

- 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.
- Corporate Governance has been defined as the system by which business corporations are directed and controlled.
- **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 & managerial incentives to act in an appropriate manner offered to senior management, business line management and employee in the form of compensation 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.

1.5.2 Enterprise Risk Management (ERM)

- 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 deal with risks & opportunities affecting value creation or preservation.
- 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 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.

1.5.3 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.
- It 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 are being made only in accordance with authorizations of management and directors of the company;
  - ✦ Provide reasonable assurance regarding 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; 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.
- **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.
  - ✦ 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.

- **Internal Controls as per COSO –**
  - ✦ According to COSO, Internal Control is comprised of five interrelated components:

    i). Control Environment –

    - For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process.

    ii). Risk Assessment –

    - Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

    iii). Control Activities –

    - 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.

    iv). Information and Communication –

    - These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

    v). Monitoring –

    - The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

- **Clause 49 of the listing agreements issued by SEBI –**
  - ✦ 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.

1.6 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.

1.6.1 IT 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 IT deployment is in tune with the business goals and objectives, known as IT Steering Committee.
- 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.
- 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 ROI, 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.

1.7 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:

i). Strategic Planning –

- ✦ 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.

ii). 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 enterprise's objectives.

iii). Operational Control –

- ✦ Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

1.7.1 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.

1.7.2 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.

1.7.3 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:

  i). Enterprise Strategic Plan,

  ii). Information Systems Strategic Plan,

  iii). Information Systems Requirements Plan, and

  iv). Information Systems Applications and Facilities Plan.

  These aforementioned plans are discussed as follows:

1) Enterprise Strategic Plan

- ✦ 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 attainment of these objectives, a statement of strategies for achieving objectives, a specification of constraints and a listing of priorities.
- ✦ In an IT environment, it is important to ensure that the IT plan is aligned with the enterprise plan.

2) 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.

3) Information Systems Requirements Plan

- ✦ The information system requirements plan defines information system architecture for the information systems department.
- ✦ 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 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.

4) Information Systems Applications and Facilities Plan

- ✦ On the basis of the information system 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.

1.7.4 Key Management Practices for Aligning IT Strategy with Enterprise Strategy

- Key management practices required for aligning IT strategy with enterprise strategy are as follows –

i). 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.

ii). 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.

iii). 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 proposal.

iv). Conduct a gap analysis –

- ✦ Identify the gaps between the current & target environments and consider alignment of assets with business outcomes to optimize investment and utilization of internal & external asset base.

v). Define the strategic plan and road map –

- ✦ Create a strategic plan that defines, in cooperation 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.

vi). 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.

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

i). 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.

ii). Direct Value Optimization –

- ✦ Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.

iii). 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.

- **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 how transparency of IT costs, benefits and risk is implemented. Some of the key metrics, 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.

1.8 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.

1.8.1 Information Systems Risks and Risk Management

- 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.
- 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.
- 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".

1.8.2 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.

- **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 particular system.

1.8.3 Related Terms

Various terminologies relating to risk management are given as follows:

1) 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 asset themselves, they all have one or more of 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 Top Secret.

2) Vulnerability

- ✦ Vulnerability is the weakness in the system safeguards that exposes the system to threats.
- ✦ It may be a weakness in information system/s, security system or other components that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.
- ✦ 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.
- ✦ Normally, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

i). Allows an attacker to execute commands as another user or

ii). Allows an attacker to access data that is contrary to specified access restriction for that data or

iii). Allows an attacker to pose as another entity or

iv). Allows an attacker to conduct a denial of service

3) Threat

- ✦ Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification 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.
- ✦ 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.

4) 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.

5) 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.

6) 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.

7) Risk

- Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset.
- 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 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 factor such as legislative, legal & regulatory requirement or technological development

- ✦ **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 &ethical value;
  - Increasing requirements for availability and robustness.

8) 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:

i). Strong authentication protocols to validate users; and

ii). Passwords should not be stored in configuration files instead some secure mechanism should be used.

9) Residual Risk

- ✦ Any risk still remaining after the counter measures are analyzed and implemented is called Residual Risk. Even when safeguards are applied, there is probably going to be some residual risk.
- ✦ An organization's management of risk should consider these two areas: acceptance of residual risk and selection of safeguards.
- ✦ 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, the risk can be managed.

1.8.4 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 use expensive control processes.
- Risk management strategy is explained and illustrated below:

i). 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.

ii). Terminate/Eliminate the risk.

- ✦ It is possible for a risk to be associated with 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.

iii). Transfer/Share the risk.

- ✦ Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management.
- ✦ Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

iv). 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.

v). Turn back.

- ✦ Where the probability of the risk is very low, then management may decide to ignore the risk.

1.8.5 Key Governance Practices of Risk Management

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

i). 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;

ii). 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

iii). 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.

1.8.6 Key Management Practices of Risk Management

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

i). Collect Data

- ✦ Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

ii). Analyze Risk

- ✦ Develop useful information to support risk decisions that take into account the business relevance of risk factors.

iii). 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.

iv). 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.

v). Define a Risk Management Action Portfolio

- ✦ Manage opportunities and reduce risk to an acceptable level as a portfolio.

vi). Respond to Risk

- ✦ Respond in timely manner with effective measure to limit magnitude of loss from IT related event.

1.8.7 Metrics of Risk Management

- Enterprises have to monitor the processes & practice 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.

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

- 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.
- 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 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.

1.9.1 Need for Enterprises to Use COBIT 5

- COBIT 5 provides good practices in governance & management to address the 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 nonprofit 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.

1.9.2 Integrating COBIT 5 with Other Frameworks

- 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 & resulting enabler should be aligned with and in harmony with (amongst other) the:
  - ✦ Enterprise policies, strategies, governance and business plans, and audit approaches;
  - ✦ Enterprise risk management framework; and
  - ✦ Existing enterprise governance organization, structures and processes.

1.9.3 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 & illustrate interrelationship with other processes.
- **Maturity Models –**
  - ✦ Assess maturity and capability per process and helps to address gaps.

1.9.4 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.

1.9.5 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.
- Enterprises can select required guidance and best practices from specific publications and processes of COBIT 5.
- 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.

1.9.6 Five Principles of COBIT 5

- 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 discussed below –

1) 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.

2) 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 '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.

3) **Principle 3: Applying a Single Integrated Framework:**
   - ✦ 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.
4) **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 defined as anything that can help to achieve the objectives of the enterprise.
5) **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.

1.9.7 Seven Enablers of COBIT 5

- Enablers are factors that, individually and collectively, influence whether something will work – in this case, governance and management of the enterprise IT.
- Enablers are driven by the goals cascade, i.e., higher level IT related goals define 'what the different enablers should achieve'.
- The COBIT 5 framework describes seven categories of enablers :

1) Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.

2) 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.

3) Organizational structures are the key decision-making entities in an enterprise.

4) Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.

5) Information is pervasive throughout any organization and includes all information produced and used by enterprise. Information is required for keeping the organization running & well governed, but at the operational level, information is very often the key product of the enterprise itself.

6) Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.

7) Skills and competencies are linked to people and are required for successful completion of all activities for making correct decisions and taking corrective actions.

1.9.8 Using COBIT 5 Best Practices for GRC

- A GRC program (project) can be implemented primarily from a compliance perspective.
- 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.
- Using best practices frameworks such as COBIT 5 can help in discharging this responsibility by ensuring that all aspects of GRC are implemented.
- 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.
- **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 realtime basis as required.

1.10 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.
- 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.
- The Information Technology Act, 2000 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.
- Reporting on Internal control requirements are 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.

1.10.1 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.
- 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.
- The COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities.
- 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.

1.10.2 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:

i). Identify External Compliance Requirements

- ✦ On a continuous basis, identify and monitor for changes in local and international laws, regulations and other external requirement that must be complied with from an IT perspective.

ii). 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.

iii). Confirm External Compliance

- ✦ Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.

iv). 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.

1.10.3 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:

1) 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;
- ✦ Coverage of compliance assessments.

2) 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.

1.11 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.

1.11.1 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.
- These are briefly explained here.

1) 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.

2) **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.

3) **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?

4) **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.

5) **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.

6) **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 important part in internal outputs in IT operation & development.

1.11.2 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:

1) **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.

2) 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.

3) Evaluate Enterprise Ethics

- The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.

4) Risk Management –

- The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

5) 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;
  - 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.

6) Risk Management Process

- The internal audit activity may gather the information to support this assessment during multiple engagements. Risk management processes are monitored through on-going management activities, separate evaluations, or both.

7) 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.

8) 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.

9) 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.

1.11.3 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.
- This review broadly considers whether 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.

1.11.4 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 selfassessments 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.

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

a) Monitor Internal Controls

- ✦ Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.

b) 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.
- ✦ This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.

c) 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.

d) Identify and Report Control Deficiencies

- ✦ Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.

e) Ensure that assurance providers are independent and qualified

- ✦ The entities performing assurance should demonstrate an appropriate attitude & appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.

f) Plan Assurance Initiatives

- ✦ Plan assurance initiatives based on enterprise objectives & conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints and sufficient knowledge of the enterprise.

g) Scope assurance initiatives

- ✦ Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.

h) Execute assurance initiatives

- ✦ Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement.