CHAPTER-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". 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.

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.' Examples include codes on corporate governance and financial reporting standards.

3) Corporate Governance: 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. 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.

1.2. Benefits of Governance

1) **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;

2) **Defining and encouraging desirable** behaviour in the use of IT and in the execution of IT outsourcing arrangements;

3) **Implementing** and integrating **the desired business processes** into the enterprise;

4) **Providing stability and overcoming the limitations** of organizational structure;

5) **Improving customer, business** and internal relationships and **satisfaction**, and reducing internal regional conflict by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework; and

6) 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,

1.3. Governance Dimensions

Governance has two dimensions:

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

1) **Conformance or Corporate Governance Dimension:** The conformance dimension of 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.
   Regulatory requirements and standards generally address this dimension with compliance being subject to assurance and/or audit. 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. The Sarbanes Oxley Act of US and the Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

2) **Performance or Business Governance Dimension:** The performance dimension of 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.

1.4. 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, 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. 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.

1.5. Benefits of IT Governance

The benefits, which are achieved by implementing/improving governance or management of enterprise, IT could include:

1) Increased value delivered through enterprise IT;

2) Increased user satisfaction with IT services;

3) Improved agility in supporting business needs;

4) Better cost performance of IT;

5) Improved management and mitigation of IT-related business risk.

6) IT becoming an enabler for change rather than an inhibitor;

7) Improved transparency and understanding of IT's contribution to the business;

8) Improved compliance with relevant laws, regulations and policies; and

9) More optimal utilization of IT resources.

1.6. 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.

1.7. Benefits of GEIT

These are given as follows:

1) It provides a consistent approach integrated and aligned with the enterprise governance approach.

2) It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.

3) It ensures that IT-related processes are overseen effectively and transparently.

4) It confirms compliance with legal and regulatory requirements.

5) It ensures that the governance requirements for board members are met.

1.8. Key Governance Practices of GEIT

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

1) **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;

2) **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

3) **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.

1.9. Corporate Governance, ERM and Internal Controls

Corporate Governance: Same as mentioned earlier

1) Some of the best practices of corporate governance include the following:
   a) Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors;

   b) Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;

   c) Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;

   d) 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) Financial and managerial incentives to act in an appropriate manner offered to senior management, and employees in the form of compensation, promotion and other recognition; and

   f) Appropriate information flows internally and to the public.

2) **Enterprise Risk Management (ERM)**

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

3) **Internal Controls**

The SEC's final rules define "internal control over financial reporting" as a "process designed by, the company's principal executive and principal financial officers, and effected by the company's board of directors 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:

1) Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions of the company;

2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles

3) 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:

1) A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company;

2) 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;

3) 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.

4) 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."

5) **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. 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 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.

6) **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, plus the owners of the 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:** Associated with control activities are information and communication systems. 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

7) 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.

1.10. IT Steering Committee

IT Steering Committee a high-level committee (Appointed by Management) 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. 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 key functions of the committee would include of the following:

1) To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives

2) To establish size and scope of IT function and sets priorities within the scope;

3) To review and approve major IT deployment projects in all their stages;

4) To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;

5) To review the status of IS plans and budgets and overall IT performance;

6) To review and approve standards, policies and procedures;

7) To make decisions on all key aspects of IT deployment and implementation;

8) To facilitate implementation of IT security within enterprise;

9) To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable

10) communication system exists between IT and its users; and

11) To report to the Board of Directors on IT activities on a regular basis.

1.11. IT Strategy Planning

IT strategic plans provide direction to distribution 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.

1.12. 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.

Strategic Planning

Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved. 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.

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,
- Information Systems Applications and Facilities Plan.

1) **Enterprise Strategic Plan:** The enterprise strategic plan provides the overall agreement 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.

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:
   a) Enterprise business strategy,
   b) Definition of how IT supports the business objectives,
   c) Inventory of technological solutions and current infrastructure,

d) Monitoring the technology markets,
e) Timely feasibility studies and reality checks,
f) Existing systems assessments,
g) Enterprise position on risk, time-to-market, quality, and
h) Need for senior management buy-in, support and critical review.

3) **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 IS 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:
a) Automated data repository and dictionary,
b) Data syntax rules,
c) Data ownership and criticality/security classification,
d) An information model representing the business, and
e) Enterprise information architectural standards.

4) **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:
a) Specific application systems to be developed and an associated time schedule,
b) Hardware and Software acquisition/development schedule,
c) Facilities required, and
d) Organization changes required.

1.13. 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:

1) **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).

2) **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.

3) **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.

4) **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.

5) **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.

6) **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.

1.14. 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.

1.15. 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. Some of the common sources of risk are:

1) Commercial and Legal Relationships,
2) Economic Circumstances,
3) Human Behavior,
4) Natural Events,
5) Political Circumstances,
6) Technology and Technical Issues,
7) Management Activities and Controls, and
8) Individual Activities.

Broadly, risk has the following characteristics:

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

Related Terms

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 the assets themselves, they all have one or more of the following characteristics:
   a) They are recognized to be of value to the organization.
   b) They are not easily replaceable without cost, skill, time, resources or a combination.
   c) They form a part of the organization's corporate identity, without which, the organization may be threatened.
   d) Their Data Classification would normally be Proprietary, Highly confidential or even 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, cryptographic system , or other components 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 to exploit the system to adjust their own records.

Normally, vulnerability is a state in a computing system, which must have at least one condition, out of the following:

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

3) **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.

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. 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.

7) **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 followings:
a) Identification of threats and vulnerabilities in the system;
b) 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
c) 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:

a) Widespread use of technology;
b) Interconnectivity of systems;
c) Elimination of distance, time and space as constraints;
d) Unevenness of technological changes;
e) Devolution of management and control;
f) Attractiveness of conducting unconventional electronic attacks against organizations; and
g) External factors such as legislative, legal and regulatory requirements or technological developments.

8) Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as countermeasure. For example, well known threat 'spoofing the user identity', has two countermeasures:
   a) Strong authentication protocols to validate users; and
   b) Passwords should not be stored in configuration files instead some secure mechanism should be used.

9) 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.

1.16. 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 as under below:

1) **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.

2) **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.

3) **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.

4) **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.

5) **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

1.17. Key Governance Practices of Risk Management

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

1) **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

2) **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

3) **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.

1.18. Key Management Practices of Risk Management

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

1) **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

2) **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.

3) **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.

4) **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.

5) **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.

6) **Respond to Risk**: Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

1.19. Compliance in COBIT 5

The Management domain of "Monitor, Evaluate and Assess" 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.

1.20. 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:

1) **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.

2) **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

3) **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements

4) **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.

1.21. COBIT 5 - A GEIT Framework

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; andIncreased enterprise wide involvement in IT-related activities.

1.22. 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 ITIL, 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 behaviour 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.

1.23. 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.

1.24. 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 as follows:

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.

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,

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 make a clear distinction between Governance and Management. These two disciplines encompass different types of activities, require different organizational structures and serves different purposes.

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, discussed as follows:

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 underestimated as a success factor in governance and management activities. Often

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.

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

7) **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.

1.25. Using COBIT 5 Best Practices for GRC

GRC program Implementation requires

- 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.

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:

1) The reduction of redundant controls and related time to execute (audit, test and remediate);
2) The reduction in control failures in all key areas;
3) The reduction of expenditure relating to legal, regulatory and review areas;
4) Reduction in overall time required for audit for key business areas;
5) Improvement through streamlining of processes and reduction in time through automation of control and compliance measures;
6) Improvement in timely reporting of regular compliance issues and remediation measures; and
7) Dashboard of overall compliance status and key issues to senior management on a real- time basis as required.

1.26. Using COBIT 5 for IS Assurance

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, 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 following Fig. 1.12.1 provides sample examples of the different assurance needs, which can be performed by using COBIT 5.

1.27. 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:
   a) Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to relationship to effectively communicate this relationship to IT and organization personnel.

   b) Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.

   c) Determine how IT will be measured in helping the organization achieve these goals.

   d) Review how roles and responsibilities are assigned within the IT organization and how they are executed.

e) 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:
   a) Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.

   b) 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.

3) **Processes:** The following aspects need to be checked by the auditor:
   a) 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.

   b) 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:
   a) Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.

   b) 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:
   a) Assess key controls that are defined by IT to manage its activities and the support of the overall organization.

   b) Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity.

   c) 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:
   a) 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.

1.28. 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 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:
   a) Promoting appropriate ethics and values within the organization;
   b) Ensuring effective organizational performance management and accountability;

c) Communicating risk and control information to appropriate areas of the organization;
d) 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. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

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:
   a) Organizational objectives support and align with the organization's mission;
   b) Significant risks are identified and assessed;
   c) Appropriate risk responses are selected that align risks with the organization's risk appetite;
   d) 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. 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.

7) **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
   a) Achievement of the organization's strategic objectives;
   b) Reliability and integrity of financial and operational information;
   c) Effectiveness and efficiency of operations and programs;
   d) 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. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

1.29. 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:

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

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:

1) Continuously monitor and evaluate the control environment, including self- assessments and independent assurance reviews;
2) Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions; and
3) 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:

1) **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.
2) **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 centres, and network operations centres. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.
3) **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.
4) **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
5) **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
6) **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.
7) **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
8) **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.