CHAPTER 1

Concepts of Governance and Management of Information Systems

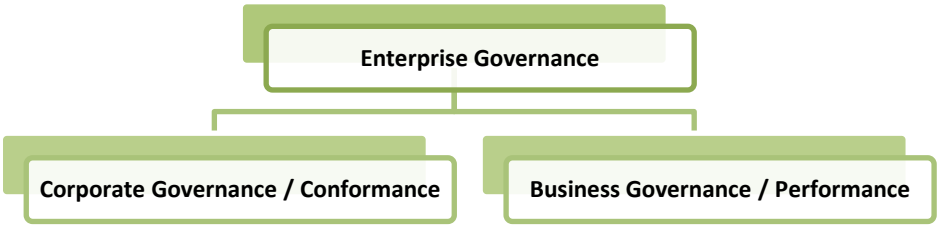
1. Governance

- 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

- the set of responsibilities and practices
- exercised by the BOD and executive management
- with the goal of
- providing strategic direction,
- ensuring that objectives are achieved,
- ascertaining that risks are managed, and
- organization's resources are used responsibly.

3. Enterprise Governance has **two dimensions** as shown below: **[Short Notes – PM]**



These dimensions are discussed as follows:

- **Corporate Governance or Conformance:**

  - the system by which a company or enterprise
  - is directed and controlled
  - to achieve the objective of
  - increasing shareholder value
  - by enhancing economic performance.

Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.

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

The Sarbanes Oxley Act of US and the Clause 49 listing requirements of SEBI are **examples** of providing for such compliances from conformance perspective.

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

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

4. Benefits of Governance [PM-Ex, RTP-M15]

→ These can be summarized as follows:

1) Improving customer, business and internal relationships and satisfaction, and reducing internal strife by integrating the customers, business units, and external IT providers into a holistic IT governance framework;
2) Enabling effective and strategically aligned decision making for the IT Principles that define the role of IT
3) Defining and encouraging desirable behavior in the use of IT;
4) Implementing and integrating the desired business processes into the enterprise;
5) Achieving objectives of enterprise by ensuring that each element of the mission are assigned with transparent decisions rights and accountability framework;
6) Providing stability and overcoming the limitations of organizational structure;

5. IT Governance and Governance of Enterprise IT (GEIT)

▪ IT Governance [N-14, N-15]

→ The objective of IT Governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT.

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.

a) Key practices to determine status of IT Governance

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

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

b) Benefits of IT Governance [PM, N-14, N-15]

→ The benefits would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

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

▪ Governance of Enterprise IT (GEIT) [PM, RTP-N14]

→ 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 frame 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.

a) Benefits of GEIT [PM, RTP-N14, M-16]

→ These are given as follows:

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

b) Key Governance Practices of GEIT [PM – Ex]

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

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

6. Best Practices of Corporate Governance

→ Some of the best practices of corporate governance include the following:

1) Clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the board of directors;
2) Establishment of a mechanism for the interaction and cooperation among the board of directors, senior management and the auditors;
3) Implementing strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;

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

5) Appropriate information flows internally and to the public as well.

6) 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);

7. Enterprise Risk Management (ERM)

- ✓ Framework published by COSO.
- ✓ Highlights the need for management to implement a system of risk management at the enterprise level.

→ Enterprise Risk Management defined as follows:

- ERM is a process,
- effected by an entity's BOD, 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 is a sub - set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

8. Internal Controls as per COSO: [N-14, RTP-N15]

→ According to COSO, Internal Control is comprised of **FIVE INTERRELATED COMPONENTS**:

1) **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.

2) **Risk Assessment**: Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

3) **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.

4) **Information and Communication**: These are associated with control activities. These enable an organization to capture and exchange the information needed for its business processes.

5) **Monitoring**: The internal control process must be continuously monitored with modifications made as required by changing conditions.

9. Role of IT in Enterprises [PM-Ex, N-15]

1) Today 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.

2) IT has not only automated the business processes but also transformed the way business processes are performed. IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

3) The extent of technology deployment also impacts the way internal controls are implemented in an enterprise.

4) Extensive organization restructuring or business process re-engineering may be facilitated through IT deployments.

5) IT strategy aligned with business strategy and ensures value creation and facilitates benefit realization from the IT investments.

10. IT Steering Committee

→ The senior management may appoint a high -level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

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

➢ Key functions of the committee [PM]

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 communication system exists between IT and its users; and
10) To report to the Board of Directors on IT activities on a regular basis.

11. There are three levels of managerial activity in an enterprise [N-15, RTP-M16]

- ✓ **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. It is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.

- ✓ **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.

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

> ***Q.*** *Discuss different levels of managerial activity that are carried out in an enterprise.*
> ***[RTP-M16]***

12. Key Management Practices Required for Aligning IT Strategy with Enterprise Strategy [PM, RTP-M15, M-15]

→ 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.

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.

3) **Define the target IT capabilities:** This should be based on the understanding of the enterprise environment; the assessment of the current business process and consideration of best practices and emerging technologies.

4) **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets with business outcomes to optimize investment in and utilization of the internal and external resources.

5) **Define the strategic plan and road map:** Create a strategic plan that defines co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. IT should define the initiatives that will be required to close the gaps and achievement of goals and 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 through communication to stakeholders and users throughout the enterprise.

13. Discuss key management practices, which are needed to be implemented for evaluating 'whether business value is derived from IT' in an organization. [PM-Ex]

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

1) 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.

2) Direct Value Optimization: Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.

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

14. Business Value from Use of IT [PM, RTP-N15]

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

1) Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;

2) Percentage of IT services where expected benefits realized;

3) Percentage of IT enabled investments where claimed benefits met or exceeded;

4) Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;

5) Percentage of IT services with clearly defined and approved operational costs and expected benefits; and

6) Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

Q. *"The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented." Explain some of the key metrics, which can be used for such evaluation.* ***[PM, RTP-N15]***

RELATED TERMS [Short Notes – PM, RTP, Exam]

→ Various terminologies relating to risk management are given as follows:

➢ **Asset**

- Asset can be defined as
- something of value to the organization;

E.g. - information in electronic or physical form, software systems, employees.

Irrespective the nature of the assets themselves, they all have one or more of the following characteristics:

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.

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

➢ **Vulnerability**

- Vulnerability is the
- weakness in the system safeguards
- that exposes the system to threats.

It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. Some examples of vulnerabilities are given as follows:

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

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

In other words, vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

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

➢ Threat

- Any entity, circumstance, or event
- with the potential to harm the software system or component
- through its unauthorized access, destruction, modification,
- and/or denial of service
- is called a Threat.

A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.

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

➢ Exposure

- the extent of loss
- the enterprise has to face
- when a risk materializes.

It is not just the immediate impact, but the real harm that occurs in the long run.

For example - loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.

➢ Likelihood

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

➢ Attack

→ An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.
Basically, it is a set of actions designed to compromise CIA (Confidentiality, Integrity or Availability), or any other desired feature of an information system.

➢ Risk

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

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

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

1) Widespread use of technology;
2) Interconnectivity of systems;
3) Elimination of distance, time and space as constraints;
4) Unevenness of technological changes;
5) Devolution of management and control;
6) Attractiveness of conducting unconventional electronic attacks against organizations; and
7) External factors such as legislative, legal and regulatory requirements or technological developments.

➢ Counter Measure

- An action, device, procedure, technique or other measure
- that reduces the vulnerability
- of a component or system.

For example, well known threat 'spoofing the user identity', has two countermeasures:

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

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

➢ Residual Risk

→ Any risk still remaining after the counter measures are analyzed and implemented is called **Residual Risk**. Management 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.

15. Risk Management Strategies [PM, RTP-N14(CL), M-16]

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

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.

16. Key Governance Practices for Evaluating Risk Management [RTP-M15]

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

- **Evaluate Risk Management:** Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed.

- **Direct Risk Management:** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite; and

- **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

17. Key Management Practices for Implementing Risk Management [PM, RTP-N14]

→ 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.

> ***Q.*** *The management of IT related risks is a key part of enterprise governance. Name the key management practices to achieve this objective.* ***[M-15]***

18. Short Notes – Metrics of Risk Management [N-15]

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

1) Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;

2) Number of significant IT related incidents that were not identified in risk assessment;

3) Percentage of enterprise risk assessments including IT related risks; and

4) Frequency of updating the risk profile based on status of assessment of risks.

19. COBIT 5 Business Framework – Governance and Management of Enterprise IT

a) What do you understand by COBIT? [RTP-M15]

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

b) Need for Enterprises to Use COBIT 5

→ Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues. COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies. It helps enterprises to create optimal value from their information and technology. COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes 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.

c) 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 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 behavior. Thus, COBIT 5 acts as the single overarching framework, which serves as a integrated source of guidance for other framework which should be aligned with the:

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

d) Components in COBIT [RTP-M15]

1. **Framework -** Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;

2. **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.

3. **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

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

e) Benefits of COBIT 5 [RTP-M16]

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

1) A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.

2) 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.

3) 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.

4) COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.

5) COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.

6) 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.

7) COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

f) Five Principles of COBIT 5 [PM, M-15]

→ 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 discussed below:

- **Principle 1: Meeting Stakeholder Needs:** COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. 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 and considers all IT related governance and management enablers to be enterprise-wide and end- to-end.

- **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.

- **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.

- **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.

g) Seven Enablers of COBIT 5 [PM, M-14, RTP-N15]

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

1) Principles, Policies and Frameworks are the vehicle to translate the desired behavior 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 Behavior of individuals and of the enterprise is 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 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 and services.

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.

h) Key Management Practices (provided by COBIT) of IT Compliance [PM-Ex, N-15]

→ 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.

Q. *'COBIT 5 provides various management practices for ensuring compliance with external compliances as relevant to the enterprise'. Explain these practices in brief.* ***[PM-Ex]***

i) Key Metrics for Assessing Compliance Process

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

Compliance with External Laws and Regulations: These metrics are given as follows:

- Cost of IT non-compliance, including settlements and fines;
- Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;
- Number of non-compliance issues relating to contractual agreements with IT service providers; and
- Coverage of compliance assessments.

IT Compliance with Internal Policies: These metrics are given as follows:

- Number of incidents related to non compliance to policy; o Percentage of stakeholders who understand policies;
- Percentage of policies supported by effective standards and working practices; and o Frequency of policies review and updates.

Q. *Discuss some of the sample metrics for reviewing the process of evaluating and assessing compliance with external laws & regulations and IT compliances with internal policies.[PM-Ex]*

j) Evaluating IT Governance Structure and Practices by Internal Auditors [PM-Ex, RTP-M16]

→ Internal audit activities in evaluating the IT governance structure and practices within an enterprise can evaluate several key components that lead to effective IT governance. These are briefly explained here:

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.

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 to appropriate authorities. 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:

- Evaluate IT process activities and the controls in place to mitigate risks to the organization.
- 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.
- Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels.

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 an important part in the internal outputs in IT operations and developments.

Q. *As an internal auditor, what shall be your perspective while evaluating IT Governance of an enterprise.* ***[RTP-M16]***

k) Sample Areas of GRC for Review by Internal Auditors [PM]

→ 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 and
- Communicating risk and control information to appropriate authorities.

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:

- Organizational objectives are in line 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;

6) **Risk Management Process:** The internal audit activity may gather the information during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

7) **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.

8) **Address Adequacy of Risk Management Process:** Internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

Q. *Discuss the areas, which should be reviewed by internal auditors as a part of the review of Governance, Risk and Compliance.* ***[PM, RTP-N14]***

I) Evaluating and Assessing the System of Internal Controls [PM]

→ 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 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, independent assessments etc. All this provides 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 and are competent with adequate 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 recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

Q. *Explain the key management practices for assessing and evaluating the system of internal controls in an enterprise in detail.* ***[PM, RTP-N14]***

Q. *You are appointed by leading enterprise to access and to evaluate its system of IT internal controls. What are the key management practices to be followed to carry out the assignment complying with COBIT-5?* ***[N-14]***