1

CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

1.2 Key Concepts of Governance

Governance:

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.

Enterprise Governance:

Enterprise Governance can be defined as: 'The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.'

Enterprise governance is an overarching framework into which many tools and techniques and codes of best practice can fit.

Examples include codes on corporate governance and financial reporting standards.

Enterprise Governance has two Dimensions

1. **Corporate Governance or Conformance**
2. **Business Governance or Performance**

1. Corporate Governance or Conformance:

- **Corporate Governance** is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance refers to the structures and processes for the direction and control of companies.
- Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements.
- This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.
- Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business to protect shareholders' interest. Corporate Governance drives the corporate information needs to meet business objectives.

- 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. 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.

Enterprise Governance = Corporate Governance + Business Governance

Write short notes on the following with reference to Governance Dimensions:
(i) Conformance or Corporate Governance Dimension
(ii) Performance or Business Governance Dimension [PM]

1.3 Benefits of Governance

Benefits of Governance can be summarized as below:

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

Describe the major benefits achieved through proper governance in an organization. [PM-ex]

1.4 Corporate Governance and IT Governance

(Not Important)

There is no doubt to say that IT is a key enabler of corporate business strategy. **Chief Executive Officers (CEO), Chief Financial Officers (CFO)** and **Chief Information Officers (CIO)** agree that strategic alignment between IT and business objectives are a critical success factor for the achievement of business objectives. IT has to provide critical inputs to meet the information needs of all the required stakeholders or it can be said t hat enterprise activities require information from IT activities in order to meet enterprise objectives. Hence, corporate governance drives and sets IT governance.

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

1.5 IT Governance and Governance of Enterprise IT (GEIT)

The terms IT Governance and Governance of Enterprise IT (GEIT) are used inter-changeably, the term GEIT is more macro and broader in its scope of coverage.

1.5.1 IT 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.

1.5.2 Key Practices to determine status of IT Governance

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

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

1.5.3 Benefits of IT Governance

- Increased value delivered through enterprise IT;
- Increased user satisfaction with IT services;
- Improved agility in supporting business needs;
- Better cost performance of IT;

- Improved management and mitigation of IT-related business risk;
- IT becoming an enabler for change rather than an inhibitor;
- Improved transparency and understanding of IT's contribution to the business;
- Improved compliance with relevant laws, regulations and policies; and
- More optimal utilization of IT resources.

IT Governance is a Sub set of Corporate Governance

Discuss the key benefits of IT Governance achieved at highest level in an organization. [Nov 16 (6 Marks)]

What is IT Governance? What are the key practices which determine the status of IT governance in the enterprise? [Nov 16 (4 Marks)]

What do you understand by IT Governance? Write any three benefits of IT Governance. [Nov 14 (4 Marks), PM]

'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits. [Nov 15 (4 Marks)]

Explain the key benefits of IT Governance achieved at highest level in organization. [PM]

1.5.4 Governance of Enterprise IT (GEIT)

Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

1.5.5 Benefits of GEIT

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

What are the key benefits of GEIT? [May 17 (4 Marks)]

Write short note on Benefits of GEIT. [May 16 (4 Marks)]

What do you understand by GEIT? Also explain its key benefits. [PM, Nov 14 RTP]

1.5.6 Key Governance Practices of GEIT

The key governance practices of GEIT includes the following 3 steps process.

Evaluate the Governance System

Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;

↓

Direct the Governance System

Inform leadership and obtain their support, buy-in and commitment.
Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels.
Define the information required for informed decision making; and

↓

Monitor the Governance System

Monitor the effectiveness and performance of the enterprise's governance of IT.
Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

In Layman language – **[for better understanding only, don't study]**
IT Governance is very specific
GEIT is very wider & Broader term.
For e.g.
An Organization has 100 Branches.
Suppose if there is IT Governance in one branch then we said that there is IT Governance but we can't say there is GEIT.
Suppose if all the branches i.e. 100 branches have IT Governance then we said that there is Enterprise wise IT Governance i.e. GEIT.
Every Organization will always focus on GEIT.

What are the key governance practices that are required to implement GEIT in an enterprise? [PM-ex]

1.6 Corporate Governance, Enterprise Risk Management and Internal Controls

Some of the best Practices of Corporate Governance including the following:

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

- Appropriate information flows internally and to the public. For ensuring good corporate governance, the importance of overseeing the various aspects of the corporate functioning needs to be properly understood, appreciated and implemented.

1.6.1 Enterprise Risk Management (ERM)

"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.

***Risk Appetite - the amount and type of risk that an organization is willing to take in order to meet their strategic objectives (i.e. the amount of risk, up to which an enterprise can tolerate)**

1.6.2 Internal Controls as per COSO

According to COSO, Internal Control is comprised of five interrelated components:

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

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

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

Write short notes on Internal Controls as per COSO. [NOV 14 (4 Marks), PM]
Answer:

According to COSO, Internal Control is comprised of five interrelated components.

- **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.
- **Risk Assessment:** Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **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.
- **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.
- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

1.7 Role of IT in Enterprises

- 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.
- 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.
- The extent of technology deployment not only impacts the way internal controls are implemented in an enterprise but also provide better and innovative services from strategic perspective.
- An IT strategy aligned with business strategy ensures value creation and facilitates benefit realization from the IT investments.
- Extensive organization restructuring or Business Process Re-Engineering may be facilitated through IT deployment.

What is the role of IT in enterprise? [Nov 15 (3 Marks)]

Write short note on the Role of IT in enterprise. [PM-ex]

1.7.1 Business and IT Strategy: (Not Important)

One of the most dramatic developments affecting enterprises is the fusion or alignment of IT strategy with business strategy. Enterprises can no longer develop business strategy separate from IT strategy and vice versa. Accordingly, there is a need for the integration of sound IT planning with business planning and the incorporation of effective financial and management controls within new systems.

The purpose of business and IT alignment is to optimize the value that IT contributes to the enterprise. An organization can successfully align IT strategy to business strategy when both IT departments and other business departments work tighter and there is:

- A sound and shared understanding of how IT applications, technologies and services will contribute to business objectives – today and in the future.
- A shared focus between IT and business departments for optimum use scarce resources, time and money.
- A credible working relationship between the IT departments and the rest rest of the business departments.

Alignments of business and IT strategies is viewed as key to obtaining value from IT investments, it is necessary not only for success but for survival of business as well.

1.7.2 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.

The key functions of the committee would include of the following:

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

You are appointed as a member of the IT Steering Committee for IT implementation and deployment in a large company. What are the major functions of this committee? [May 17 (6 Marks)]

Explain the key functions of IT Steering Committee in brief. [PM]

1.8 IT Strategy Planning

Planning is basically deciding in advance

'What is to be done'
'Who is going to do' and
'When it is going to be done'

There are three levels of managerial activity in an enterprise.

- **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.
- **Management Control:** Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.
- **Operational Control:** Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aw are 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.

Explain the different levels of managerial activity in an enterprise. [Nov 15 (3 Marks)]

1.8.1 IT Strategy 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.
- 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.

1.8.2 Objective of IT Strategy

The primary Objective of IT strategy is to:

- Provide an understanding of the current IT environment
- Define future IT environment or Future direction
- Provide Initiatives required to migrate to the desired future IT environment by using IT setup and resources that enable reliable & efficient response to strategic objectives.

Alignment of the IT objectives with the business objectives is done by clearly communicating the objectives and associated accountabilities so they are understood by all and all the IT strategic options are identified, structured and integrated with the business plans as required.

1.8.3 Classification of Strategic Planning

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

1. **Enterprise Strategy Plan,**
2. **Information Systems Strategic Plan,**
3. **Information Systems Requirements Plan, and**
4. **Information Systems Application and Facilities Plan.**

1. **Enterprise Strategy Plan:**
   Enterprise strategic plan provides the overall direction 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.
2. **Information Systems Strategic Plan:**
   The IS Strategic Plan has to focus on balancing IT opportunities and IT business requirements. Some of the enablers of the IS Strategic plan are:
   - Enterprise business strategy,
   - Definition of how IT supports the business objectives,
   - Inventory of technological solutions and current infrastructure,
   - Monitoring the technology markets,
   - Timely feasibility studies and reality checks,
   - Existing systems assessments,
   - Enterprise position on risk, time-to-market, quality, and
   - Need for senior management buy-in, support and critical review.

3. **Information Systems Requirements Plan:**
   Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems.
   This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information.
   Based on the information architecture requirements of an enterprise, the Information Systems Requirements Plan has to be drawn up so as to meet the information requirements of the enterprise. Some of the key enablers of the information architecture are as follows:
   - Automated data repository and dictionary,
   - Data syntax rules,
   - Data ownership and criticality/security classification,
   - An information model representing the business, and
   - Enterprise information architectural standards.
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:
   - Specific application systems to be developed and an associated time schedule,
   - Hardware and Software acquisition/development schedule,
   - Facilities required, and
   - Organization changes required.

1.8.4 Key Management Practices for Aligning IT Strategy with Enterprise Strategy

The key management practices, which are required for aligning IT strategy with enterprise Strategy is as follows:

- **Understand enterprise direction:** This considers the current enterprise environment and business processes; enterprise strategy and future objectives and also the external environment of the enterprise.
- **Assess the current environment, capabilities and performance:** This assesses the performance of current internal business and IT capabilities and external IT services, and develops an understanding of the enterprise architecture in relation to IT.
- **Define the target IT capabilities:** This defines the target business and IT capabilities and required IT services on the basis of enterprise environment and requirements; assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices.
- **Conduct a gap analysis:** This identifies the gaps between the current and target environments and considers the alignment of assets with business outcomes to optimize investment.
- **Define the strategic plan and road map:** This creates a strategic plan that defines, in cooperation with relevant stakeholders, how IT - related goals will contribute to the enterprise's strategic goals.

- **Communicate the IT strategy and direction:** This creates awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy.

What are the key management practices which are required for aligning IT strategy of BB with its Enterprise Strategy? [May 16 (5 Marks)]

Discuss the key management practices required for aligning IT Strategy with Enterprise Strategy. [May 15 (6 Marks), PM]

1.8.5 Business Value from use of IT

Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT -enabled investments at an acceptable cost.

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

- **Evaluate Value Optimization:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.
- **Direct Value Optimization:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.
- **Monitor Value Optimization:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

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

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

What are the key management practices to be implemented for evaluating Business Value from the

use of IT? State any three key metrics which can be used for such evaluation.
[Nov 17 (6 Marks)]

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

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

1.9 Risk Management

- Enterprise Risk Management and IT Risk Management are key components of an effective IT governance structure of any enterprise.
- IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite.
- The risk assessment approach adapted has to consider business impact of IS risk and different types of risks.
- There has to be timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile.

1.9.1 Information Systems Risks and Risk Management (Not Important)

Information Systems (IS) is exposed to many direct and indirect risks. These risks primarily have emerged due to frequent technological changes in information technology environment. These frequent technological changes create gaps between protection applied and protection required for information systems because existing controls frequently become weak or invalid due to frequent technological changes. These gaps is applied and required controls result in many IS risks.

Additionally, organizations are becoming increasingly dependent upon information systems. Therefore, it is essential to manage these IS risks appropriately else organization cannot perform business operations efficiently. The information systems risks management is increasingly becoming an important area in organization because it ultimately leads to Enterprise Risk Management.

Risk is likelihood that an organization may be exposed to some threat that may cause harms to organizations. For example, organizations are exposed to risks of fire and theft etc. Thus, fire and theft are risks to organizations and may cause harms to organization's resources and operations.

Risk Management is a systematic process or series of steps taken to manage and control the risks for organization or controls the risks for an IT system. Risk Management includes procedures and steps for identifying, analyzing, evaluating, treating, monitoring, and communicating risks. Risk management is an iterative process, i.e. its steps are not used once only these are used repetitively to continuously manage

the risks with changes in information systems technologies and components. Therefore, risks management process is also known as risk management cycle.
Primarily, risk management cycle involves the following steps:

- Risk Identification
- Analyze the Identified Risks
- Evaluation of Analyzed Risks
- Development of Risk Mitigation Plan or Controls
- Implementation of Risk Mitigation Plan
- Re-assessment or Re-evaluation of Risks.

Generally, IT related risks cannot be completely eliminated but risks can be mitigated by using appropriate security and controls. This security and controls should be implemented as per the controls specifications described by management.

Auditors play very important role in managing information systems related risks. Auditors are required to evaluate whether the available controls and security are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be controls weakness, which has to be reported to management with appropriate recommendations to mitigate them.

Auditors primarily classify controls as:

- Preventive; Prevent risks form occurring (e.g. firewall control)
- Detective; detect the risks and their reasons 9e.g. audit trail control)
- Corrective; helps in correction (e.g. backup and recovery control)

As discussed above, the risks in IT environment are mitigated by using appropriate and adequate IS security. IS security is defined as "procedures and practices to assure that computer facilities are available when required that data is processed correctly and access to data is restricted to authorized users only."

1.9.2 Sources of Risks

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

- Commercial and Legal Relationships,
  For e.g. 'X' is a client to Infosys. He kept his confidential data with Infosys. Infosys is responsible to protect the confidentiality of data of 'X'. If confidentiality is lost, it is a source of risk.
- Economic Circumstances,
  Suppose organization is suffering from loses, organization is not able to implement sufficient controls because of scarcity of funds. Then if controls are not implemented then there is a possibility of risk.
- Human Behavior,
  E.g. Data Theft
- Natural Events,
  For e.g. Fire, earthquake, floods etc.
- Political Circumstances,

- Technology and Technical Issues,
  If Organization technology is Outdated or Organization Technology is not Compatible
- Management Activities and Controls, and
  For e.g. If Management does not implement the controls properly then there is a source of risk
- Individual Activities.

Characteristics of Risk:

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

1.9.3 Related Terms

Asset:

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

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

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.

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 specified access restrictions for that data' or
- 'Allows an attacker to pose as another entity' or
- 'Allows an attacker to conduct a denial of service'.

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

called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm.

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.

Vulnerability Vs Threat Vs Exposure. [for better understanding only, don't study]
If there is no Vulnerability (i.e. Weakness) then there is no Threat. If there is no Threat then there is no Exposure.
For e.g.
Mr. X does not lock Office gate at night – Vulnerability (i.e. Weakness)
Because of doors are not locking Unauthorized people are entered the Organization – Threat
These Unauthorized people stolen Organizations Laptop & Data – Exposure

Organizations doesn't have Fire Extinguishers – Vulnerability
Fire occurred in the Organization - Threat
Because of fire occurred Organization suffered a loss of 50 Lacs – Exposure

Counter Measure:

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

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

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

Residual Risk:

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

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.

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.

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 and **[CIA means "Confidentiality, Integrity & Availability]**
- The identification and analysis of security controls for the information system.

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

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

Write short note on Vulnerability. [May 15 (4 Marks)]

Write short note on the following:
Risk, Threat, Exposure, Attack, Vulnerability, Likelihood of threat, Countermeasure, Residual Risk. [PM]

1.9.4 Risk Management Strategies

Risk Management Strategies are as below:

- **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Turn back**. Where the probability or impact of the risk is very low, then management may decide to ignore the risk.
- **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.
- **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.
- **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.

Write short note on Risk Management Strategies. [May 16 (4 Marks)]

Briefly explain various risk management strategies [PM]

1.9.5 Key Governance Practices of Risk Management

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

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

1.9.6 Key Management Practices of Risk Management

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

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

The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective. [May 15 (6 Marks), PM]

Describe key management practices for implementing risk management [PM]

1.9.7 Metrics of Risk Management

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

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

Write short note on Metrics of Risk Management. [Nov 15 (4 Marks)]

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

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

COBIT 5 incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

1.10.1 Need for Enterprises to Use COBIT 5

- Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues.
- COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies. It helps enterprises to create optimal value from their information and technology.
- COBIT 5 provides the tools necessary to understand, utilize, implement and direct important IT related activities.
- COBIT 5 is intended for enterprises of all types and sizes, including non - profit and public sector and is designed to deliver business benefits to enterprises, including:
  - ✓ Increased value creation from use of IT;
  - ✓ User satisfaction with IT engagement and services;
  - ✓ Reduced IT related risks and compliance with laws, regulations and contractual requirements;
  - ✓ Development of more business-focused IT solutions and services; and
  - ✓ Increased enterprise wide involvement in IT-related activities.

1.10.2 Integrating COBIT 5 with Other Frameworks

COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as **Information Technology Infrastructure Library (ITIL)**, **The Open Group Architecture Framework (TOGAF)** and ISO 27001. It is also aligned with The GEIT standard ISO/IEC 38500:2008, which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behavior. 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.

Write short note on Integrating COBIT 5 with other frameworks. [PM-ex]

1.10.3 Components in COBIT

- **Framework -** Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;
- **Process Descriptions -** A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- **Management Guidelines -** Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.
- **Maturity Models -** Assess maturity and capability per process and helps to address gaps.

Write short note on Components of COBIT 5. [Nov 16 (4 Marks), PM-ex]

1.10.4 Benefits of COBIT 5

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

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

Write short note on Benefits of COBIT 5. [PM-ex]

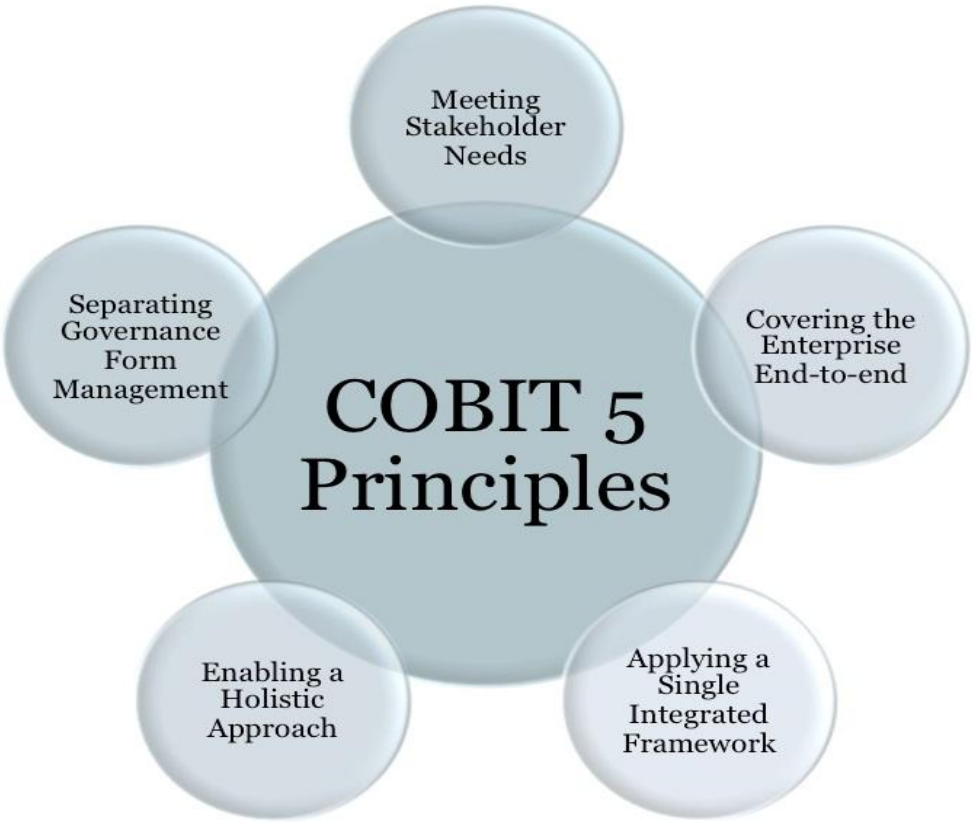
1.10.5 Customizing COBIT 5 as per Requirement

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

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

1.10.6 Five Principles of COBIT 5

The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective Governance and Management framework that optimizes information and technology investment and use for the benefit of stakeholders.



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. COBIT 5 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 allowing the enterprise to use COBIT 5 as the overarching governance and management framework integrator.

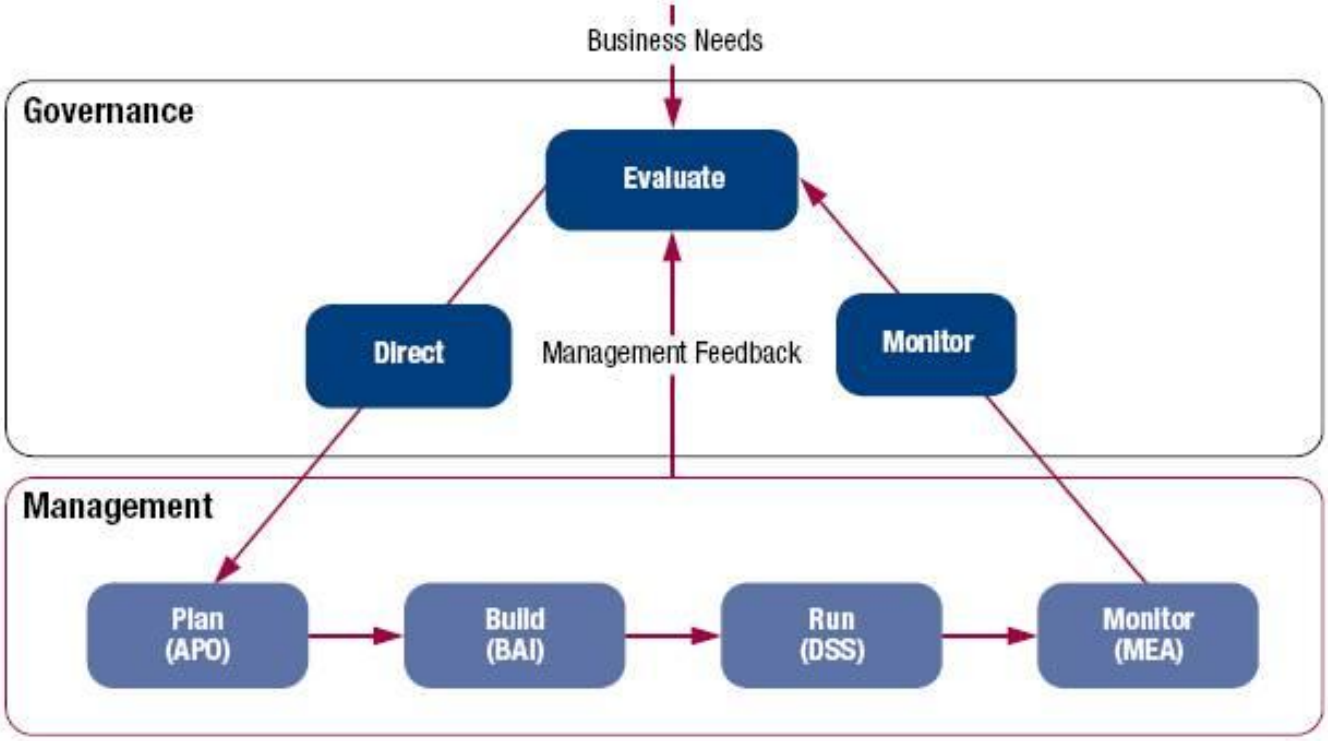
Principle 4: Enabling a Holistic Approach - COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT that require a holistic approach, taking into account several interacting components.

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.

Write short note on Principles of COBIT 5 **[May 15 (4 Marks), PM]**

1.10.7 COBIT 5 Process Reference Model **(Not Important)**

COBIT 5 includes a Process Reference Model, which describes number of processes for **Governance** and **Management** as shown in below diagram**.** It provides a common reference model of processes understandable by both the Information Technology Management and Business Management. However, COBIT describes that each enterprise should define its own process set by considering its own requirements. And, setting a common language for IT and business is key step to achieve good governance. This Process Reference Model also provides framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers and integrating with best management practices.



Governance: It ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved and monitoring performance & compliance against agreed-on direction and objectives. Overall governance is the responsibility of Board of Directors, but some responsibility may be delegated to special organization structures at an appropriate level.

Management: It contains 4 domains – **(1) Plan, (2) Build, (3) Run & (4) Monitor [PBRM],** providing the end-to-end coverage of IT in alignment with the direction set by governance body to achieve organization objectives.

COBIT 5 model includes a total of 37 governance and management processes as mentioned below:

Governance Processes:
Evaluate, Direct and Monitor Practices (EDM) – 5 processes (EDM01 to EDM05)

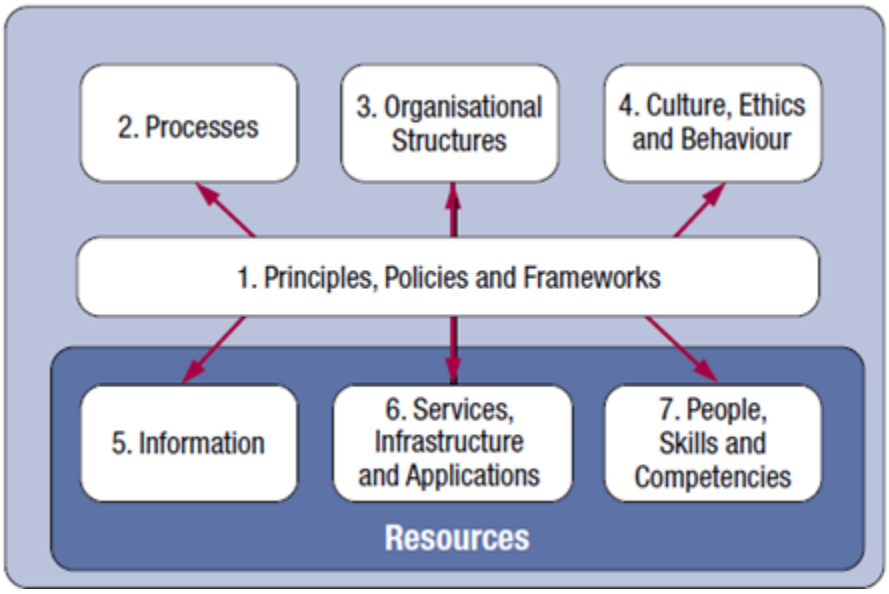
Management Processes:

- Align, Plan and Organize (APO) – 13 processes (APO01 to AP013)
- Build, Acquire and Implement (BAI) – 10 processes (BAI01 to BAI10)
- Deliver, Service and Support (DSS) – 6 processes (DSS01 to DSS06)
- Monitor, Evaluate and Assess (MEA) – 3 processes (MEA01 to MEA03)

1.10.8 Seven Enablers of COBIT 5

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

What are the enablers described by COBIT 5 Framework? [Nov 16 (5 Marks)]

Discuss various categories of enablers under COBIT 5 [PM]

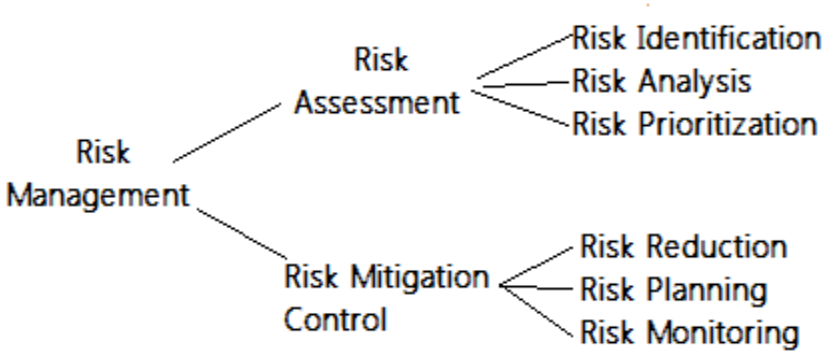
1.10.9 Risk Management in COBIT 5 (Not Important)

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

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

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

The combination of Governance practices of "EDM03: Ensure risk optimization" and the management practices of "APO12 Manage risk" together ensured that Risk management covers the entire life cycle and covers both governance and management perspective. Further, detailed guidance is available in the form of specific practices and activities that are designed to treat related risk (avoid, educe/mitigate/control, share/transfer/accept). In addition to activities, COBIT 5 suggests accountabilities, and responsibilities for enterprise roles and governance/management structures (RACI charts) for each process including risk -related roles at each level of management as appropriate. A pictorial representation of various activities relating to risk management is given in below diagram.



Risk Management Practices

1.10.10 Using COBIT 5 Best Practices for GRC

Successful GRC Implementation requires the following:

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

Success of a GRC program can be measured by using the following goals and metrics:

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

1.11 IT Compliance Review

(Not Important)

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

In the US, Sarbanes Oxley Act has been passed to protect investors by improving the accuracy and reliability of corporate disclosures as part of compliance with corporate governance and risk management or as a part of overall GRC Framework.

As discussed above, in India, Clause 49 of listing agreement issued by SEBI mandates similar implementation of enterprise risk management and Internal Controls as appropriate for the enterprise. Further, the Information Technology Act, which was passed in 2000 and amended in 2008 provides legal

recognition for electronic records and also mandates responsibilities for protecting information. The Act also identifies various types of cyber – crimes and has imposed specific responsibilities on corporate.

1.11.1 Compliance in COBIT 5

The Management domain "Monitor, Evaluate and Assess" (MEA) contain a compliance focused process: "MEA03 Monitor, Evaluate and Assess Compliance with External Requirements". 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 and hence its inclusion the COBIT 5. In addition to MEA03, all enterprise activities include control activities that are designed to ensure compliance not only with regulatory requirements but also with enterprise governance-determined principles, policies and procedures.

This management domain process of COBIT 5 describes procedures to evaluate IT processes and IT supported business functions for compliance requirements. It also provides guidelines for organization in terms of having procedures and practices in place to meet compliance requirements and integrating IT compliance with overall enterprise compliance

1.11.2 Key Management Practices of IT Compliance

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

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

Briefly describe the key management practices provided by COBIT for ensuring IT compliances. [Nov 15 (4 Marks)]

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

1.11.3 Key Metrics for Assessing Compliance Process

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

1. **Compliance with External Laws and Regulations:** These metrics are given as follows:
   - Cost of IT non-compliance, including settlements and fines;

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

2. **IT Compliance with Internal Policies:** These metrics are given as follows:
   - Number of incidents related to non compliance to policy;
   - Percentage of stakeholders who understand policies;
   - Percentage of policies supported by effective standards and working practices; and
   - Frequency of policies review and updates.

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]

1.12 Information System Assurance

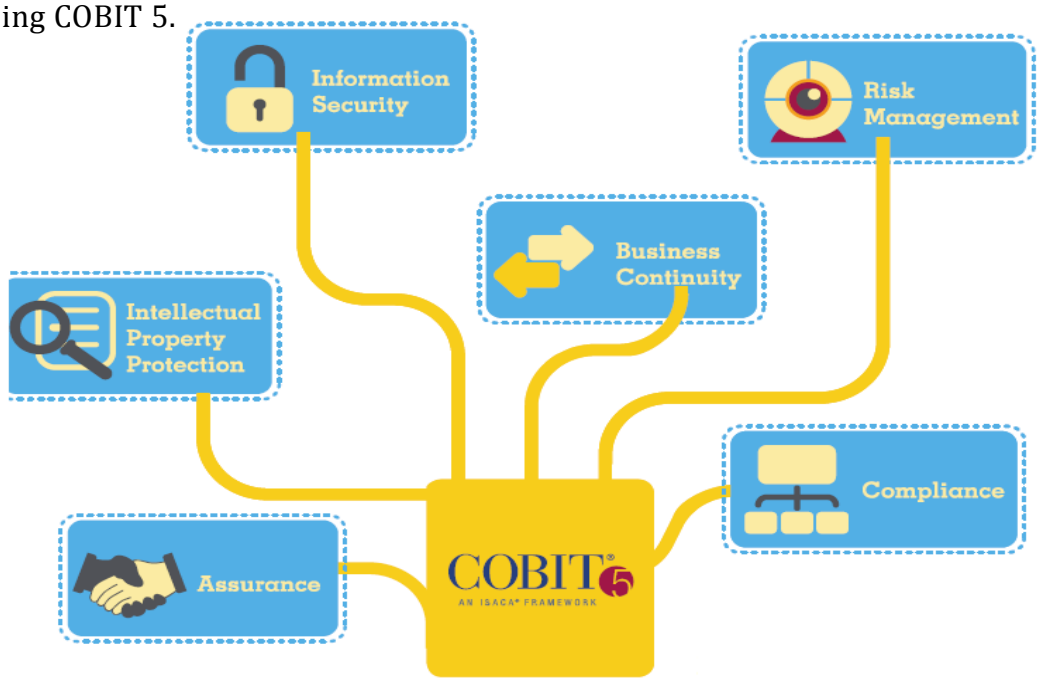
In the rapidly changing digital world, enterprises are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations.

There is a challenge for Chartered Accountants (as assurance providers) to provide IS assurance with the required level of confidence. However, with the right type of skills and toolsets, this provides an excellent opportunity for Chartered Accountants to act as IS assurance consultants. Auditor should have knowledge of globally accepted good practices and frameworks and develop a holistic approach, which meets the needs of stakeholders.

1.12.1 Using COBIT 5 for Information System 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 Figure provides sample examples of the different assurance needs, which can be performed by using COBIT 5.



Assurance Needs of COBIT 5

1.12.2 Evaluating IT Governance Structures and Practices by Internal Auditors

IT Governance can be evaluated by both external as well internal auditors. **The Institute of Internal Auditors (IIA)** issues the guidance that outlines specific areas and critical aspects relating to governance structure and practices, which can be reviewed as part of internal audit. These are briefly explained here.

1. **Leadership:** The following aspects need to be verified by the auditor:

- Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.
- Assess the involvement of IT leadership in the development and on -going execution of the organization's strategic goals.
- Determine how IT will be measured in helping the organization achieve these goals.
- Review how roles and responsibilities are assigned within the IT organization and how they are executed.
- Review the role of senior management and the board in helping establish and maintain strong IT governance.

2. **Organizational Structure:** The following aspects need to be assessed by the auditor:

- Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.
- This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed

via formal evaluation and prioritization. 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 and whether they provide the necessary assurance regarding processes and underlying systems.
- What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?

4. **Risks:** The following aspects need to be reviewed by the auditor:

- Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment.
- Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.

5. **Controls:** The following aspects need to be verified by the auditor:

- Assess key controls that are defined by IT to manage its activities and the support of the overall organization.
- Ownership, documentation, and reporting of self -validation aspects should be reviewed by the internal audit activity.
- Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.

6. **Performance Measurement/Monitoring:** The following aspects need to be verified by the auditor:

- Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

Write short note on Evaluating IT Governance Structure and Practices by Internal Auditor.[PM-ex]

1.12.3 Sample Areas of GRC for Review by Internal Auditor

Major areas, which should be reviewed by internal auditors as a part of the review of Governance, Risk and Compliance, are given as follows:

1. **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
2. **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
   - Promoting appropriate ethics and values within the organization;
   - Ensuring effective organizational performance management and accountability;
   - Communicating risk and control information to appropriate areas of the organization; and
   - Coordinating the activities of and communicating information among the board, external and internal auditors, and management.
3. **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation and effectiveness of the organization's ethics related objectives, programs and activities. 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 support and align with the organization's mission;
   - Significant risks are identified and assessed;
   - Appropriate risk responses are selected that align risks with the organization's risk appetite; and
   - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
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:
   - achievement of the organization's strategic objectives;
   - reliability and integrity of financial and operational information;
   - effectiveness and efficiency of operations and programs;
   - safeguarding of assets; and
   - compliance with laws, regulations, policies, procedures, and contracts.
8. **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
9. **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

Based on the Institute of Internal Auditors (IIA) guidance, briefly explain any six samples areal which can be reviewed by Internal Auditors as part of the review of GRC.
[Nov 16 (6 Marks)]

Discuss the Areas, which should be reviewed by Internal Auditors as a part of the review of Governance, Risk and Compliance. [PM]

1.12.4 Sample Areas of Review of Assessing and Management Risks

Primarily, in this controls for assessing and managing risks for IT processes are reviewed. This review provides assurance to management that risks related to IT implementation and use are identified and

controlled. In addition, this involves reviewing whether organization is taking cost-effective measures to mitigate risks.

The following areas can be reviewed for assessing and managing risks:

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

Write short note on Sample Areas of review for assessing and managing risks. [PM-ex]

1.12.5 Evaluating and Assessing the System of Internal Controls

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 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 include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers.
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.

COBIT 5 has a specific process "MEA02 Monitor, Evaluate and Assess the system of Internal Control." Discuss in brief any 6 key practices for assessing and evaluating the system of Internal Control in an enterprise based on this process. [May 17 (6 Marks)]

You are appointed by a leading enterprise to assess 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? [Nov 14 (6 Marks), PM]

Discuss the key management practices for assessing and evaluating the system of Internal Controls in an enterprise in detail. [PM]

Last 7 attempts RTP Questions:

NOV 14

What is Governance of Enterprise IT (GEIT)? Explain its key benefits in brief.
Discuss key management practices for implementing risk management.
Discuss the areas, which should be reviewed by Internal Auditors as a part of the review of Governance, Risk and Compliance (GRC).
Discuss the key management practices for assessing and evaluating the system of Internal Controls in an enterprise in detail.

MAY 15

What are the key management practices, which are required for aligning IT Strategy with enterprise Strategy?
Discuss the key governance practices for evaluating risk management.
Discuss COBIT and its Components in brief.
Discuss major benefits of Governance.

NOV 15

"The success of the process of ensuring business value from the use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and how transparency of IT costs, benefits and risks is implemented." Explain some of the key metrics which can be used for such evaluation.
Discuss the seven enablers of COBIT 5.
Write short note on Internal Controls as per Committee of Sponsoring Organizations of the Treadway Commission (COSO).

MAY 16

Discuss different levels of managerial activity that are carried out in an enterprise.
Discuss key benefits of COBIT 5 framework.
As an internal auditor, what shall be your perspective while evaluating IT Governance of an enterprise?

NOV 16

What is Governance of Enterprise IT (GEIT)? Explain its key benefits in brief.
Discuss the key governance practices for evaluating risk management
Discuss the seven enablers of COBIT 5 Framework.
As an IT consultant, elaborate on the major benefits of Governance to the Management of an enterprise.

MAY 17

Discuss Risk Management Strategies in detail.

What do you understand by "Information Systems Risks"? Discuss broadly the characteristics of risk.

Discuss the components of Internal Controls as per COSO (Committee of Sponsoring Organizations).

Explain the term "Corporate Governance".

NOV 17

What are the three levels of managerial activity in an enterprise during IT Strategy Planning.

Discuss the key Governance practices for evaluating Risk Management.

What are the benefits of COBIT5?

Discuss various key management practices for assessing and evaluating the system of internal controls in an enterprise.

SUMMERY OF EXAMINATION WEIGHTAGE

ATTEMPT	MARKS
N-17	16
M-17	16
N-16	15
M-16	13
N-15	18
M-15	14
N-14	14