Chapter 1. *Concepts of Governance and Management of Information Systems*

1. Key Concepts of Governance: Major terms used in governance are explained as follows:

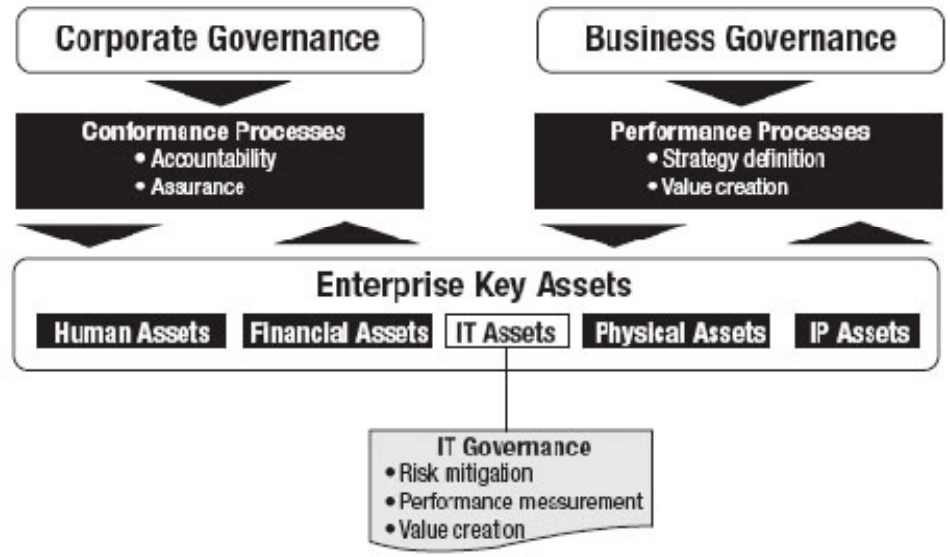
· **Governance:** A Governance system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives.

· **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.

· **Corporate Governance**: Corporate governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders.

- major Benefits of Governance [ADI PIER]
  - Achieving enterprise objectives
  - Defining and encouraging desirable behaviour in the use and execution of IT
  - Implementing and integrating the desired business processes
  - Providing stability and overcoming the limitations of organizational structure;
  - Improving customer, business and internal relationships and satisfaction,
  - Effective and strategically aligned decision making,
  - reducing internal disputes.

2. Governance Dimensions: Governance has two dimensions:



· **Conformance or Corporate Governance:**	· **Performance or Business Governance:**
The conformance dimension of governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.	The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. 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.

3. IT Governance: The objective of IT governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT. IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT activities to ensure effectiveness, accountability and compliance of IT.

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?

Question: *Explain the key benefits of IT Governance achieved at highest level in an organization.*
Answer - The benefits, which are achieved by implementing/improving governance or management of enterprise IT, would depend on the specific and unique environment of every enterprise. At the highest level, these could include: [I(uv) I(mtca) MEB]

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

For every defined benefit, it is critical to ensure that: [RU ROBOT]

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

4. Governance of Enterprise IT (GEIT): Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of relevant IS controls within an enterprise 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.

Question: What do you understand by GEIT? Also explain its key benefits.
Answer - Benefits of GEIT : These are given as follows:

- It provides a consistent approach integrated and aligned with the enterprise governance approach.
- It confirms compliance with legal and regulatory requirements.
- 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 ensures that the governance requirements for board members are met.

Key Governance Practices of GEIT: The key governance practices of GEIT are as under:

· Evaluate the Governance System:

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

· **Direct the Governance System**:

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

· **Monitor the Governance System**:

o Monitor the effectiveness and performance of the enterprise's governance of IT.
o Assess whether the governance system and implemented mechanisms are operating effectively and provide appropriate oversight of IT.

5. Corporate Governance

- ✓ Corporate Governance has been defined as the system by which business corporations are directed and controlled.
- ✓ The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.

Best practices of corporate governance include the following

- o Mechanism for the interaction & cooperation among the B.O.D, senior management and the auditors;
- o Implementing strong internal control systems including internal and external audit functions,
- o Special monitoring of risk exposures where conflicts of interest are likely to be particularly great,
- o Clear assignment of responsibilities and decision-making authorities,
- o Financial & managerial incentives to act in an appropriate manner offered to senior management, business line management and employees (in the form of compensation and promotion).
- o Appropriate information flows internally and to the public.

Enterprise Risk Management (ERM) 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.

ERM in an IT environment

- o Enterprise risk management deals with risks and opportunities affecting value creation or preservation.
- o 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.
- o 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

Internal Control

The SEC's final rules define "Internal control over Financial Reporting" as a "process designed by, or under the supervision of,
the company's principal executive and principal financial officers, or
persons performing similar functions, and
effected by the company's board of directors, management and other personnel,
to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally **accepted accounting principles** and includes those policies and procedures that:

· pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions

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

6. Internal Controls as per COSO: According to COSO, Internal Control is comprised of five interrelated components:

- Control Environment: An organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process.
- Risk Assessment: 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.
- Information and Communication: 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.

7. Role of IT in Enterprises: It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives. IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services .

8. IT Steering Committee:

- ✓ Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee
- ✓ to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives.
- ✓ led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.
- ✓ The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management.

The key functions of the committee would include of the following:
(set – ensure – facilitate – approve & monitor - review – decide – report)

- To sets priorities according to size and scope of IT function within its scope;
- To ensure plans of the IT department are aligned with enterprise goals and objectives;
- 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 approve and monitor key projects by measuring result of IT projects in terms of ROI, etc.
- To review and approve major IT deployment projects in all their stages;
- To review and approve standards, policies and procedures;
- To review the status of IS plans and budgets and overall IT performance;
- To make decisions on all key aspects of IT deployment and implementation;
- To report to the Board of Directors on IT activities on regularly.

9. IT Strategy Planning: IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation. Management should ensure that IT long and shortrange plans are communicated to business process owners and other relevant parties across the enterprise.

- 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	Management Control	Operational Control
the process by which top management determines overall organizational purposes& objectives and how they are to be achieved.	the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.	the process of assuring that specific tasks are carried out effectively and efficiently.

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

1) **Enterprise Strategic Plan**:
   - The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate.
   - It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise.
   - It includes a statement of mission

2) **Information Systems Strategic Plan**:
   - The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment.
   - Some of the enablers of the IS Strategic plan are:
     - o Enterprise business strategy,
     - o Definition of how IT supports the business objectives,
     - o Inventory of technological solutions and current infrastructure,
     - o Monitoring the technology markets,
     - o Timely feasibility studies and reality checks,
     - o Existing systems assessments,
     - o Enterprise position on risk, time-to-market, quality, and
     - o Need for senior management buy-in, support and critical review.

3) **Information Systems Requirements Plan:**
   - The information system requirements plan defines information system architecture for the information systems department.
   - The architecture specifies the major organization functions needed to support planning, control and operations activities and the data classes associated with each function.
   - Some of the key enablers of the information architecture are:
     - o Automated data repository and dictionary,
     - o Data syntax rules,
     - o Data ownership and criticality/security classification,
     - o An information model representing the business, and
     - o Enterprise information architectural standards.

4) **Information Systems Applications and Facilities Plan:**
   - the information systems management can develop information systems applications & facilities plan. This plan includes:
     - o Specific application systems to be developed and an associated time schedule,
     - o Hardware and Software acquisition/development schedule,
     - o Facilities required, and
     - o Organization changes required.
   - Senior management is responsible for developing and implementing long and short-range plans that enable achievement of the enterprise mission and goals.
   - Senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the enterprise's long- and short-range plans.

10. Objective of IT Strategy:
The primary objective of IT strategy is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.

11. Key Management Practices for Aligning IT Strategy with Enterprise Strategy: (DACU CD)

- ✓ Define the target IT capabilities (understanding of the enterprise environment and requirements)
- ✓ Assess the current environment, capabilities and performance (performance of current internal business and IT capabilities and external IT services)
- ✓ Conduct a gap analysis (gaps between the current and target environments)
- ✓ Understand enterprise direction (Consider the current enterprise environment and also consider the external environment of the enterprise.)
- ✓ Communicate the IT strategy and direction (Create awareness and understanding of the business and IT objectives and direction)
- ✓ Define the strategic plan and road map (how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets.)

12. Business Value from use of IT: 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.

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

- o Evaluate Value Optimization,
- o Direct Value Optimization and
- o Monitor Value Optimization.

14. Related Terms: Various terminologies relating to risk management are given as follows:
Asset: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. It is the purpose of Information Security Personnel to identify the threats against the assets, 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.
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 which ability to inflict harm to the organization resulting in compromise in the system, and/or its quality.
Exposure: An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example; loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.
Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.
Attack: An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability (i.e. CIA). In software terms, an attack is a malicious intentional act, usually an external act that has the intent of exploiting vulnerability in the targeted software or system.
Risk: Formally, Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset,

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.

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

· Strong authentication protocols to validate users; and

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

The relationship and different activities among these aforementioned terms may be understood by the following Fig. 1.1:

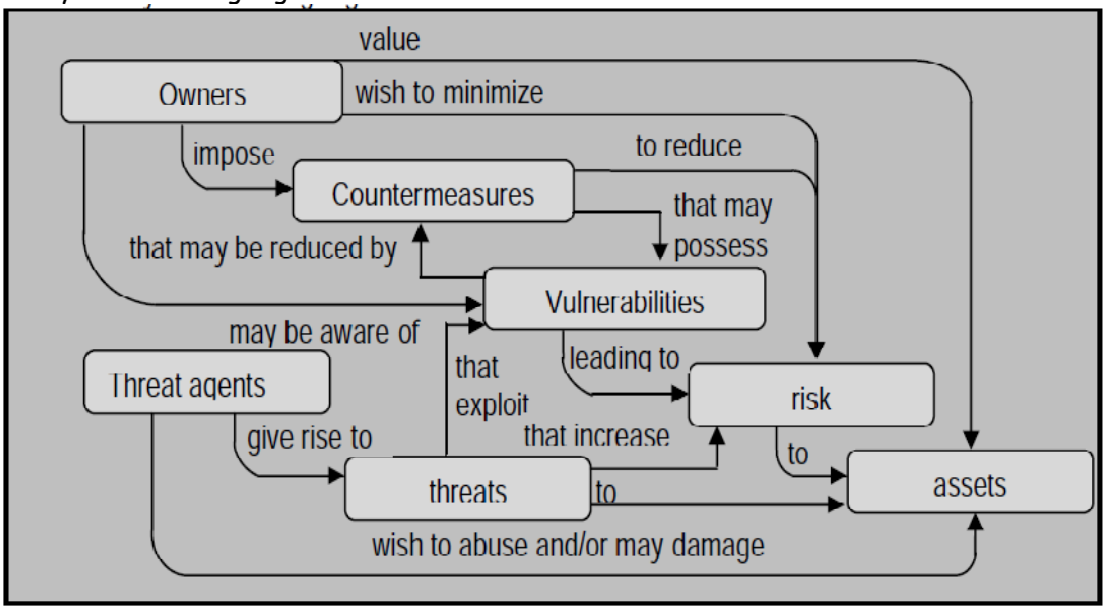


Fig. 1.1: Risk and Related Terms*

➢ **Some of the common sources of risk are:**

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

risk has the following characteristics:

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

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.

15. Risk Management Strategies:

Major risk management strategies are:

Tolerate/Accept the risk,	Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
Terminate/Eliminate the risk,	It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
Transfer/Share the risk,	Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
Treat/mitigate the risk	Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
Turn back.	Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

16. Risk Management: A pictorial representation of various activities relating to risk management is given :-

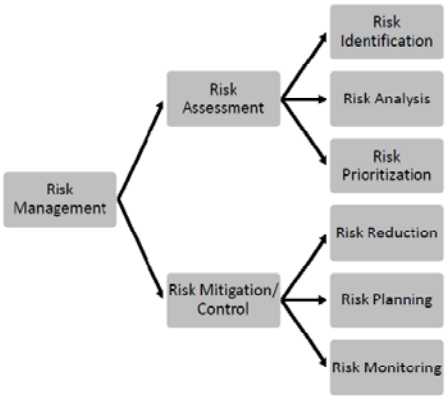


Fig. 1.2: Risk Management

17. Key Governance Practices of Risk Management: The key governance practices for evaluating risk management are to evaluate risk management, direct risk management and monitor risk management.

18. Key Management Practices of Risk Management: Key Management Practices for implementing Risk Management:

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

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

· **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.

· **Articulate Risk**: Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.

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

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

19. Metrics of Risk Management: Some of the key metrics are:
· 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.

20. Key Management Practices of IT Compliance: COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise.
The practices are: Identify External Compliance Requirements, Optimize Response to External Requirements, Conform External Compliance and Obtain Assurance of External Compliance.

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 as under

- **Compliance with External Laws and Regulations:** These metrics are given as follows:
  - o Cost of IT non-compliance, including settlements and fines;
  - o Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;
  - o Number of non-compliance issues relating to contractual agreements with IT service providers; and
  - o Coverage of compliance assessments.

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

21. COBIT 5 – A GEIT Framework : COBIT 5 helps enterprises to manage IT related risk and ensure compliance, security and privacy. Cobit % 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.

Need for Enterprises to Use COBIT 5
- Increased value creation from use of IT;
- User satisfaction with IT engagement and services;
- Support compliance with relevant laws, regulations and contractual requirements;
- Development of more business-focused IT solutions and services; and
- Increased enterprise wide involvement in IT-related activities.

- COBIT 5 Process Reference Model

COBIT 5 includes a process reference model, which defines and describes in detail a number of governance and management processes. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation. Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is one of the most important and critical steps towards good governance. It also provides a framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers, and integrating best management practices.

22. **Five Principles of COBIT 5**

Principle 1: Meeting Stakeholder Needs	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 & creates value for its stakeholders through the use of IT.
Principle 2: Covering the Enterprise End to End	It does not focus on IT function, it considers all IT related governance and management enablers to be enterprise-wide & end to end including each & everything
Principle 3: Applying a Single Integrated Framework	There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 framework aligns with them at a high level & serve as an overarching framework to simplify complexity.
Principle 4: Enabling a Holistic Approach	COBIT 5 defines a set of 7 enablers to support the implementation of a comprehensive governance and management system for enterprise IT.
Principle 5: Separating Governance from Management	The COBIT 5 recognizes that these two disciplines (governance and management)are involved in different types of activities, serve different purposes and requires different organizational structures to fulfil their individual needs. COBIT 5 help translate these needs into specific, actionable, and customized goods that creates real values.

23. **Seven Enablers of COBIT 5:** The COBIT 5 framework describes seven categories of enablers, which are shown in Fig. 1.4:

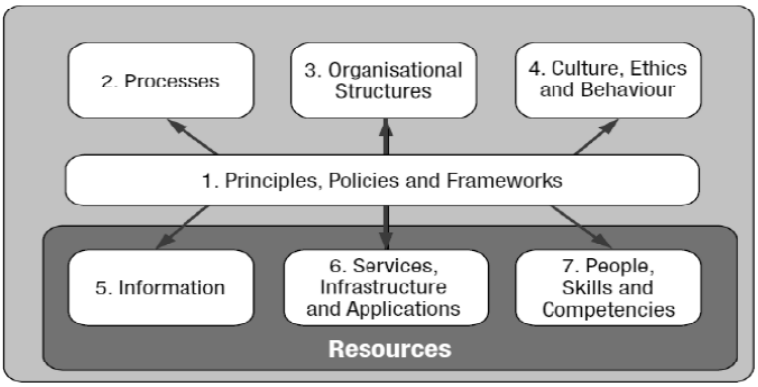


Fig. 1.4: Seven Enablers of COBIT 5*

Principles, policies and frameworks	are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
Processes	describe organized set of practices and activities to achieve certain objectives & produce a set of outputs in support of achieving overall IT-related goals.
Organizational structures	are the key decision-making entities in an enterprise.
Culture, ethics and behaviour	Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
Information	Information is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
Services, infrastructure and applications	include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
Skills and competencies	are linked to people and are required for successful completion of all activities for making correct decisions and taking corrective actions.

24. **Using COBIT 5 for IS Assurance:** The following Fig. 1.5 provides sample examples of the different assurance needs, which can be performed by using COBIT 5.

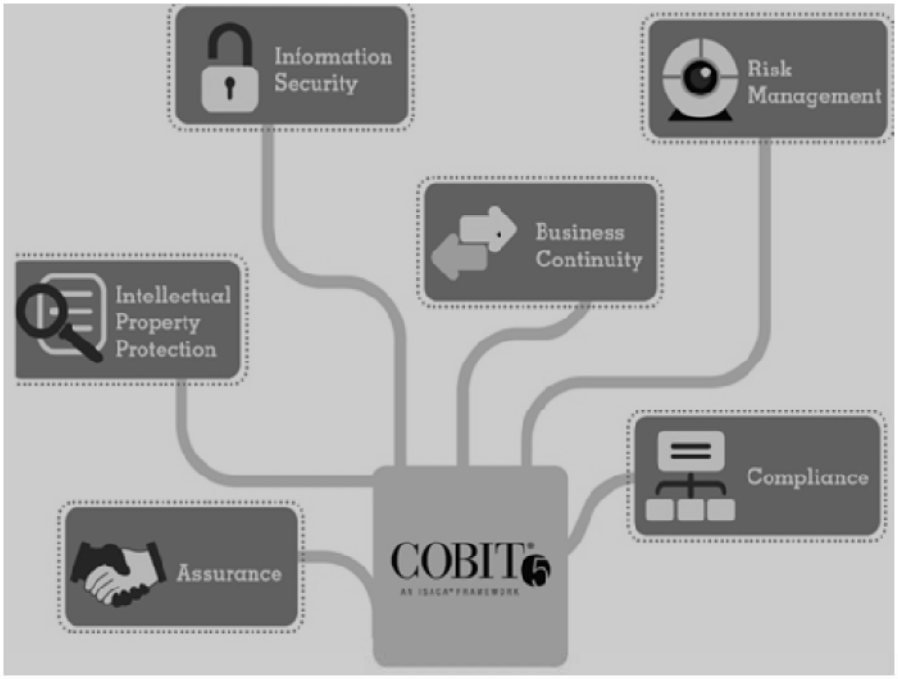


Fig. 1.5: Assurance Needs of COBIT 5*

25. **Sample Areas of GRC for Review by Internal Auditors:** Major areas, which can be reviewed by internal auditors as part of review of Governance, Risk and Compliance are given as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process.
- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

· Interpretation: Determining whether risk management processes are effective based on the internal auditor's assessment.

· 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.

· Evaluate Risk Exposures: The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems.

· Evaluate Fraud and Fraud Risk: The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

· Address Adequacy of Risk Management Process: During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

Question : *Discuss the areas, which should be reviewed by internal auditors as a part of the review of Governance, Risk and Compliance.*

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

· **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

· **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- o Promoting appropriate ethics and values within the organization;
- o Ensuring effective organizational performance management and accountability;
- o Communicating risk and control information to appropriate areas of the organization; and
- o Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

· **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation and effectiveness of the organization's ethics related objectives, programs and activities. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

· **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

· **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that:

- o Organizational objectives support and align with the organization's mission;
- o Significant risks are identified and assessed;
- o Appropriate risk responses are selected that align risks with the organization's risk appetite; and
- o Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

· **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.

· **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:

- o achievement of the organization's strategic objectives;
- o reliability and integrity of financial and operational information;
- o effectiveness and efficiency of operations and programs;
- o safeguarding of assets; and
- o compliance with laws, regulations, policies, procedures, and contracts.

· **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

· **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

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

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

27. **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:

- ✓ Monitor Internal Controls,
- ✓ Review Business Process Controls Effectiveness,
- ✓ Perform Control
- ✓ Self-assessments,
- ✓ Identify and Report Control Deficiencies,
- ✓ Ensure that assurance providers are independent and qualified,
- ✓ Plan Assurance Initiatives,
- ✓ Scope assurance initiatives and Execute assurance initiatives.

Question : *Discuss the key management practices for assessing and evaluating the system of internal controls in an enterprise in detail.*

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

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

· **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centres, and network operations centres. This provides the business with the assurance of control effectiveness to meet requirements related to business, regulatory and social responsibilities.

· **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of selfassessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.

· **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.

· **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards

· **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.

· **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.

· **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.