1

Concepts of Governance and Management of Information Systems

Basic Concepts

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, 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.

2. **Enterprise Governance Dimensions:** Enterprise Governance has two dimensions**:**

- **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 concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. 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.
- **Business Governance or Performance:** 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.

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

Key Governance Practices of GEIT: The key governance practices of GEIT are - Evaluate the Governance System of Enterprise IT, Direct the Governance System, and Monitor the Governance System.

5. Corporate Governance, Enterprise Risk Management and Internal Controls: 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.

Enterprise Risk Management (ERM) is a process, affected 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.

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 and directors of the company;
- 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 Committee of Sponsoring Organizations (COSO): Per COSO, Internal Control is comprised of five interrelated components: **Control Environment, Risk Assessment, Control Activities, Information and Communication,** and **Monitoring**.

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.

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. 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.

9. 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:** In the context of Information systems, strategic planning refers to the planning undertaken by top management towards meeting long-term objectives of the enterprise. IT 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 Control:** Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise.
- **Operational Control:** Operational control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

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. Classification of strategic Planning: IT Strategy planning in an enterprise could be broadly classified into the following categories:

- Enterprise Strategic Plan,
- Information Systems Strategic Plan,
- Information Systems Requirements Plan, and
- Information Systems Applications and Facilities Plan.

12. Key Management Practices for Aligning IT Strategy with Enterprise Strategy: The key management practices, which are required for aligning IT strategy with enterprise strategy are to understand enterprise direction, assess the current environment, capabilities and performance, define the target IT capabilities, conduct a gap analysis, define the strategic plan and road map and communicate the IT strategy and direction.

13. 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, Direct Value Optimization and Monitor Value Optimization.

14. Risk Management: Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources.

15. 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. 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 threat exploits a 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 afore-mentioned terms may be understood by the following Fig. 1.1:

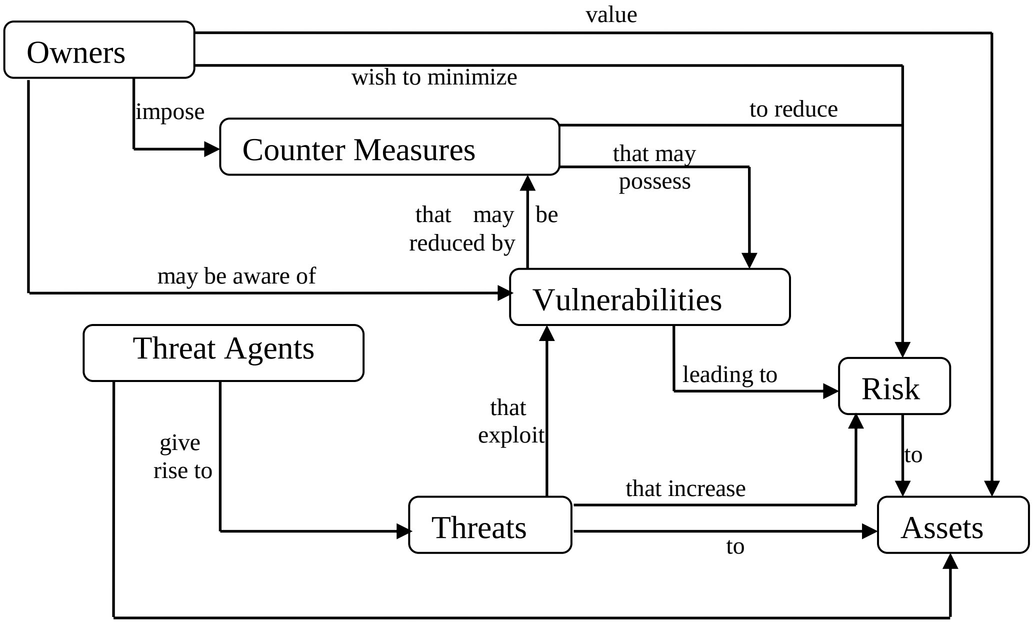

Fig. 1.1: Risk and Related Terms*

* Source: http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF p.14

16. Risk Management Strategies: Major risk management strategies are Tolerate/Accept the risk, Terminate/Eliminate the risk, Transfer/Share the risk, Treat/ mitigate the risk and Turn back.

17. Key Governance Practices of Risk Management: The key governance practices for evaluating risk management is 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, Analyze Risk, Maintain a Risk Profile, Articulate Risk, Define a Risk Management Action Portfolio and Respond to Risk.

19. Metrics of Risk Management: 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.

20. COBIT 5 - A GEIT Framework: 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.

21. Components in COBIT: The components of COBIT are Framework, Process Descriptions, Control Objectives, Management Guidelines, and Maturity Models.

22. Five Principles of COBIT 5: These principles are shown in Fig. 1.2:

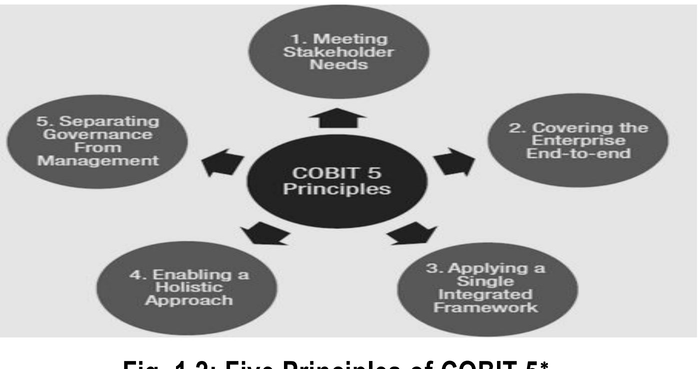
1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Fig. 1.2: Five Principles of COBIT 5*

* Source: www.isaca.org

23. COBIT 5 Process Reference Model: COBIT 5 includes a Process Reference Model, which defines and describes in detail several governance and management processes of enterprise IT into two main process domains- **Governance** and **Management** as shown in Fig. 1.3. 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.

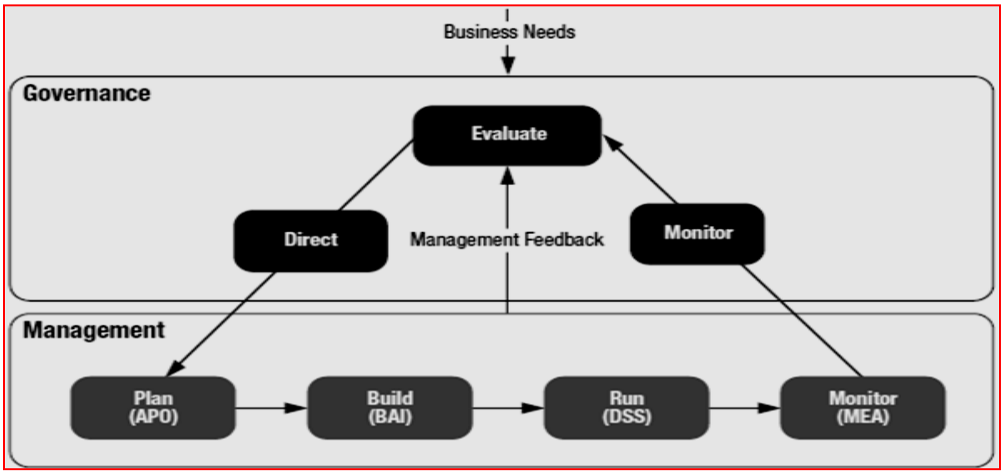

Fig. 1.3: Key Areas of Governance and Management*

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

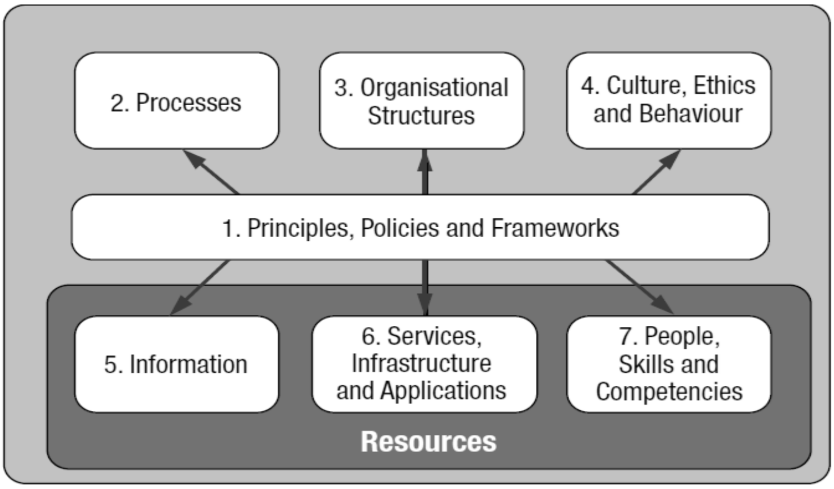
2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Fig. 1.4: Seven Enablers of COBIT 5*

* Source: www.isaca.org

25. Risk Management in COBIT 5: A pictorial representation of various activities relating to risk management is given in Fig. 1.5:

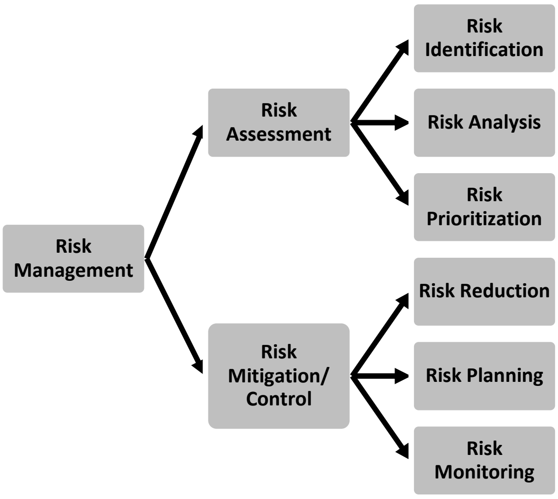

Fig. 1.5: Risk Management

26. 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.

27. Using COBIT 5 for Information System Assurance: The Fig. 1.6 provide sample examples of the different assurance needs, which can be performed by using COBIT 5.

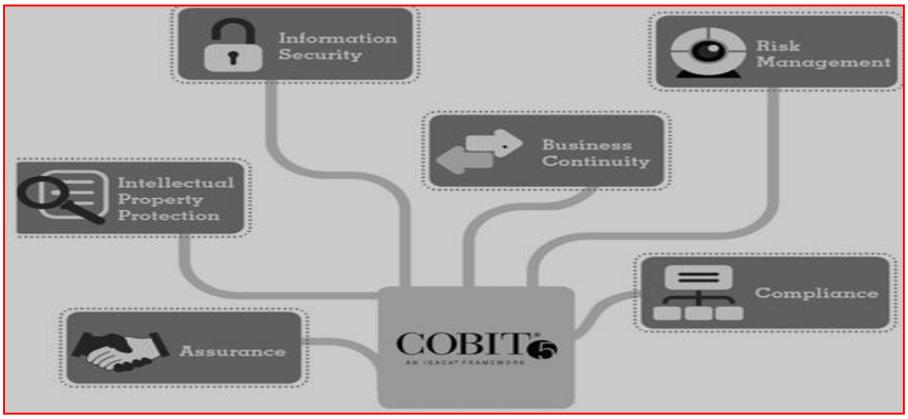

Fig. 1.6: Assurance Needs of COBIT 5*

* Source: www..isaca.org

28. 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.

29. 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.

30. 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 1

Explain the key benefits of IT Governance achieved at highest level in an organization.

Or

'IT has to provide critical inputs to meet the information needs of all the stakeholders.' Define IT Governance and list out its benefits.

Answer

One of the well-known definitions of IT Governance is that "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".

The benefits, which are achieved by implementing/improving governance or management of enterprise IT, would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

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

Question 2

Write short notes on the following regarding Governance Dimensions:

(i) Conformance or Corporate Governance Dimension

(ii) Performance or Business Governance Dimension

Answer

(i) Conformance or Corporate Governance Dimension: 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.

(ii) Performance or Business Governance Dimension: The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward-looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. 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 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 with status like other board committees and which will report to the board.

Question 3

What do you understand by GEIT? Also, explain its key benefits.

Answer

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.

Major benefits of GEIT are given as follows:

- 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.

Question 4

Explain the key functions of IT Steering Committee in brief.

Answer

The key functions of the IT Steering Committee would include 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 between IT and its users; and
- To report to the Board of Directors on IT activities on a regular basis.

Question 5

Discuss the key management practices, which are required for aligning IT strategy with enterprise strategy.

Answer

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

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).
- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals, extent of stakeholder satisfaction with scope of the planned portfolio of programs and services and the percentage of IT value drivers, which are mapped to business value drivers.

Question 6

'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.

Answer

The key metrics, which can be used for such evaluation, are given as follows:

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

Question 7

Write short note on the following:

(i) *Risk*
(ii) *Threat*
(iii) *Exposure*
(iv) *Attack*
(v) *Internal Controls as per COSO*
(vi) *Principles of COBIT 5*
(vii) *Vulnerability*
(viii) *Likelihood of threat*
(ix) *Countermeasure*
(x) *Residual Risk*
(xi) Metrics of Risk Management

Answer

(i) **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.

(ii) **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 of the system, its quality and ability to inflict harm to the organization.

(iii) **Exposure:** It is the extent of loss the organization 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, loss of resources.

(iv) **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 act, usually an external act that has the intent of exploiting vulnerability in the targeted software or system.

(v) As per 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.

(vi) 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 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.

(vii) Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats and can be exploited by the attackers. The weakness may be in information system/s, cryptographic 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 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'.

(viii) Likelihood of threat: 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.

(ix) Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system to a threat is referred as countermeasure. For example, the 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.

(x) Residual Risk: Any risk remaining after the counter measures are analyzed and implemented is called Residual Risk. Residual risk must be kept at a minimal, acceptable level. If 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 has been managed.

(xi) Metrics of Risk Management: Enterprises must 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.***

Question 8

Briefly explain various risk management strategies.

Answer

Risk Management Strategies: When risks are identified, and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Various risk management strategies are explained as follows:

- **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.
- **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.

Question 9

Describe key management practices for implementing risk management.

Answer

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 consider 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.

Question 10

Discuss various categories of enablers under COBIT 5.

Answer

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

1. Principles, policies and frameworks are the vehicle to translate the desired 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 are very often underestimated as a success factor in governance and management activities.
5. Information is pervasive throughout any organization and includes all information produced and used by 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. Skills and competencies are linked to people and are required for successful completion of all activities for making correct decisions and taking corrective actions.

Question 11

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:
  - 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.

- **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:
  - 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.
- **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:
  - 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.
- **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 managing risks.

Question 12

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 centers, and network operations centers. 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 self-assessment 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.

Question 13

What do you understand by IT Governance? Write any three benefits of IT Governance.

Or

'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits.

Answer

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.

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.

Question 14

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?

Answer

The key management practices complying with COBIT 5 for assessing and evaluating the system of IT internal controls in an enterprise are given as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the IT 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 centers, and network operations centers.

- **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.
- **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.

Question 15

The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective.

Answer

The key Management Practices for implementing IT Risk Management are given as follows:

- **Collect Data:** To enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** To develop useful information to support risk decisions.
- **Maintain a Risk Profile:** To maintain an inventory of known risks and risk attributes.
- **Articulate Risk:** To inform IT- related exposures and opportunities to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** To manage opportunities and reduce risk to an acceptable level as a portfolio.

- **Respond to Risk:** To respond limit the magnitude of loss from IT related events in a timely manner.

Question 16

Discuss key management practices required for aligning IT Strategy with Enterprise Strategy.

Answer

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 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 based on 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.

Question 17

What is the role of IT in enterprises? Explain the different levels of managerial activity in an enterprise.

Answer

Role of IT in Enterprises is as under:

- ***In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to Decision Support Systems to online transactions/services.***

- *IT has not only automated the business processes but also transformed the way business processes are performed. 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 the value creation and facilitates benefit realization from the IT investments.*
- *Extensive organization restructuring or Business Process Re-Engineering may be facilitated through IT deployments.*

The different levels of managerial activity in an enterprise are as under:

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

Question 18

Briefly describe the key management practices provided by COBIT 5 for ensuring IT compliances.

Answer

COBIT 5 provides key management practices for ensuring IT 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.***

Exercise

1. *What are the key governance practices that are required to implement GEIT in an enterprise?*
2. *Discuss key management practices, which are needed to be implemented for evaluating 'whether business value is derived from IT' in an organization.*
3. *'COBIT 5 provides various management practices for ensuring compliance with external compliances as relevant to the enterprise'. Explain these practices in brief.*
4. *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.*
5. *Write short notes on the following:*

   (i) Role of IT in enterprises

   (ii) Integrating COBIT 5 with other frameworks

   (iii) Sample areas of review for assessing and managing risks

   (iv) Evaluating IT Governance Structure and Practices by Internal Auditors.

   (v) Components of COBIT 5

   (vi) Benefits of COBIT 5