

MOCK TEST PAPER – I
FINAL (OLD) COURSE: GROUP – II
PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT
ANSWERS

Part I: MULTIPLE CHOICE QUESTIONS

1. (b) Terminate the risk
2. (c) Reliability
3. (d) (i) – (B), (ii) – (C), (iii) – (A), (iv) – (D)
4. (b) Reciprocal Agreement
5. (d) Users' interface design of the vendor
6. (b) Evaluating audit planning and assessment
7. (a) Software as a Service (SaaS)
8. (b) (iii), (iv)
9. (b) (i), (iv)
10. (a) Executives work in a decision space that is often characterized by lack of precedent.
11. (c) (i) – (C), (ii) – (B), (iii) – (A)
12. (c) Determine the maintenance regime to ensure the plan remains up-to-date.
13. (b) Structured English is the use of Binary language consisting of 0's and 1's with the syntax of structured programming.
14. (d) Maintenance of privacy.
15. (b) Section 67B
16. (d) (i) – (B), (ii) – (D), (iii) – (C), (iv) – (A)
17. (d) Information Systems Requirements Plan.
18. (d) Experimental
19. (b) (i) – (A), (ii) – (B), (iii) – (C), (iv) – (A), (v) – (B), (vi) – (B), (vii) – (A)
20. (c) (i) – (B), (ii) – (C), (iii) – (C), (iv) – (B), (v) – (A)
21. (d) Determine whether the users have been involved in the planning and development of the project or not.
22. (d) Network as a Service (NaaS)

Part II: DESCRIPTIVE QUESTIONS

1. (a) The key management practices for implementing Risk Management are as follows:
 - **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis, and reporting.
 - **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.
 - **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, 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.
- (b) Fire damage is a major threat to the physical security of a computer installation. Some of the major ways of protecting the installation against fire damage are as follows:
- Both automatic and manual fire alarms may be placed at strategic locations and a control panel may be installed to clearly indicate this.
 - Besides the control panel, master switches may be installed for power and automatic fire suppression system. Different fire suppression techniques like Dry-pipe sprinkling systems, water based systems, halon etc., depending upon the situation may be used.
 - Manual fire extinguishers can be placed at strategic locations.
 - Fireproof Walls, Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials such as wastebaskets, curtains, desks, and cabinets should be used.
 - Fire exits should be clearly marked. When a fire alarm is activated, a signal may be sent automatically to permanently manned station.
 - All staff members should know how to use the system. The procedures to be followed during an emergency should be properly documented are Fire Alarms, Extinguishers, Sprinklers, Instructions / Fire Brigade Nos., Smoke detectors, and Carbon dioxide based fire extinguishers.
 - Less Wood and plastic should be in computer rooms.
 - Use a gas based fire suppression system;
 - To reduce the risk of firing, the location of the computer room should be strategically planned and should not be located in the basement or ground floor of a multistorey building.
 - Regular Inspection by Fire Department should be conducted.
 - Fire repression systems should be supplemented and not replaced by smoke detectors.
 - **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance.
 - **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).
 - **Wiring Placed in Electrical Panels and Conduit:** Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room.
- (c) The set of skills that is generally expected to be an Information Systems Auditor include the following:
- Sound knowledge of business operations, practices and compliance requirements;
 - Should possess the requisite professional technical qualification and certifications;

- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policy and procedural controls;
- Ability to understand technical and manual controls relating to business continuity; and
- Good knowledge of Professional Standards and Best Practices of IT controls and security.

Therefore, the audit process begins by defining the scope and objectives to adapt the standards and benchmarks for developing information model for collecting and evaluating evidence to execute the audit.

2. (a) Risks that affect a system and are taken into consideration at the time of assessment can be classified into following categories:

- **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is off-site. ATM in an example of the same. Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.
- **Control Risk:** Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.
- **Detection Risk:** Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

(b) **Differential Backup:** Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation - Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken.

On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.

Advantages

- Much faster backups than full backups.
- More efficient use of storage space than full backups since only files changed since the last full backup will be copied on each differential backup run.
- Faster restores than incremental backups.

Disadvantages

- Backups are slower than incremental backups.
- Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.
- Restores are slower than with full backups.
- Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.

- (c) When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls - A Disaster Recovery Plan (DRP) and Insurance.

Disaster Recovery Plan (DRP): A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan, and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel. BCP (Business Continuity Planning) Controls: These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. The controls include Critical Classification, alternative procedures, Back-up and Recovery, Systematic and Regular Testing and Training, Monitoring and Escalation Processes, Internal and External Organizational Responsibilities, Business Continuity Activation, Fallback and Resumption plans, Risk Management Activities, Assessment of Single Points of Failure and Problem Management.

Insurance: Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, facilities, storage media, valuable papers, and records etc.

3. (a) Many Decision Support Systems (DSS) are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems. Below are several illustrations of these systems:

- **Cost Accounting System:** The healthcare industry is well known for its cost complexity. Managing costs in this industry require controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help healthcare enterprises calculate product costs for individual procedures or services. One healthcare organization, for example, combines a variety of DSS applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.
- **Capital Budgeting System:** Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as

net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One DSS designed to support decisions about investments in automated manufacturing technology is AutoMan which allows decision makers to consider financial, non-financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system, accountants, managers, and engineers identify and prioritize these factors. Then they can evaluate up to seven investment alternatives at once.

- **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized DSS to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as create additional one-and five-year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
 - **General Decision Support System:** Some planning languages used in Decision Support Systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker's tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice which supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The DSS then asks the user to compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert choice analyzes these judgments and presents the decision maker with the best alternative.
- (b) Different audit organizations go about Information Systems auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into six stages.
- (i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.
 - (ii) **Planning and preparation:** During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.
 - (iii) **Fieldwork:** This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.
 - (iv) **Analysis:** This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.
 - (v) **Reporting:** Reporting to the management is done after analysis of evidence is gathered and analyzed.
 - (vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.
- (c) Major objectives of National Cyber Security Policy 2013 published by Government of India are as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of T all sectors of the economy.
 - To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, and people).
 - To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
 - To enhance and create National and Sectorial level 24x7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution and crisis management through effective predicative, protective, response and recovery actions.
 - To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Center (NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources.
 - To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, and pilot development of secure ICT products/processes in general and specifically for addressing National Security requirements.
 - To improve visibility of the integrity of Information and Communication Technology products and services and establishing infrastructure for testing and validation of security of such products.
 - To create a workforce of 500,000 professional skilled in cyber security in the next 5 years through capacity building, skill development and training.
 - To provide fiscal benefits to businesses for adoption of standard security practices and processes.
 - To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft.
 - To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention.
 - To create a culture of cyber security and privacy enabling responsible user behavior and actions through an effective communication and promotion strategy.
 - To develop effective public private partnerships and collaborative engagements through technical and operational and contribution for enhancing the security of cyberspace, and
 - To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.
4. (a) The major Bring Your Own Device (BYOD) risks can be classified as under:
- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the

devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.

- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
 - **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that most employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.
 - **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats.
- (b) **Information Technology General Controls (ITGC)** are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. IT General Controls are the foundation for the overall IT control environment as they provide the assurance that systems operate as intended and that output is reliable. Failure to ensure these controls are designed and operating effectively means that there will not be any assurance over the IT Application Controls.
- Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entity-wide, system, and business process application levels. The effectiveness of general controls at the entity-wide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the entity-wide and system levels, business process controls generally can be rendered ineffective by circumvention or modification. The most common ITGCs are as follows:
- Logical access controls over infrastructure, applications, and data.
 - System development life cycle controls.
 - Program change management controls.
 - Data center physical security controls.
 - System and data backup and recovery controls.
 - Computer operation controls.
- (c) A **BCP manual** is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations. An incident or disaster affecting critical business operations can strike at any time. Successful organizations have a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity.

The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liaisioning teams between the functional area(s) affected and other departments providing support services.

BCM is business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that:

- Proactively improves an enterprise's resilience against the disruption of its ability to achieve its key objectives;
- Provides a rehearsed method of restoring an enterprise's ability to supply its key products and services to an agreed level within an agreed time after a disruption; and
- Delivers a proven capability to manage a business disruption and protect the enterprise's reputation and brand.

5. (a) [Section 7] Retention of Electronic Records

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if -

- (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
- (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
- (c) the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record:

PROVIDED that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records, or information in the form of electronic records.

(b) Auditors might use System Control Audit Review File (SCARF) to collect following types of information:

- **Application System Errors:** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and Procedural Variances:** Organizations must adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception:** SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample:** As some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.

- **Snapshots and Extended Records:** Snapshots and extended records can be written into the SCARF file and printed when required.
 - **Profiling Data:** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
 - **Performance Measurement:** Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.
- (c) (i) **Database Administrator (DBA):** The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.
- (ii) **Information Systems (IS) Auditor:** As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. S/he should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.
- (iii) **Project Leader:** The project leader is dedicated to a project, who has to ensure its completion and fulfillment of objectives. S/he reviews the project status more frequently than a Project Manager and the entire project team reports to him/her.
6. (a) **Analysis of the Present System:** Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. There should be enough information assembled so that a qualified person can understand the present system without visiting any of the operating departments. Survey of existing methods, procedures, data flow, outputs, files, input, and internal controls that should be intensive in order to fully understand the present system and its related problems. The following areas should be studied in depth:
- **Reviewing Historical Aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts enable to identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate 'what system changes have occurred in the past including operations' that have been successful or unsuccessful with computer equipment and techniques.
 - **Analyzing Inputs:** A detailed analysis of present inputs is important since they are basic to the manipulation of data. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of various sources from where the data are initially captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, 'what is contained in it', 'who prepared it', 'from where the form is initiated', 'where it is completed', the distribution of the form and other similar considerations. If the analyst investigates these questions thoroughly, s/he will be able to determine how these inputs fit into the framework of the present system.
 - **Reviewing Data Files:** The analyst should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval, these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all on-line and off-line files, which are maintained in the

organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.

- **Reviewing Methods, Procedures and Data Communications:** Methods and procedures transform input data into useful output. A method is defined as a way of doing something; a procedure is a series of logical steps by which a job is accomplished. A procedure review is an intensive survey of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to eliminate unnecessary tasks or to perceive improvement opportunities in the present information system. A system analyst also needs to review and understand the present data communications used by the organization. S/he must review the types of data communication equipment including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must understand how the data-communications network is used in the present system so as to identify the need to revamp the network when the new system is installed.
- **Analyzing Outputs:** The outputs or reports should be scrutinized carefully by the system analysts in order to determine 'how well they will meet the organization's needs. The analysts must understand what information is needed and why, who needs it and when and where it is needed. Additional questions concerning the sequence of the data, how often the form reporting is used, how long is it kept on file, etc. must be investigated. Often, many reports are a carry-over from earlier days and have little relevance to current operations. Attempts should be made to eliminate all such reports in the new system.
- **Reviewing Internal Controls:** A detailed investigation of the present information system is not complete until internal control mechanism is reviewed. Locating the control points helps the analyst to visualize the essential parts and framework of a system. An examination of the present system of internal controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.
- **Modeling the Existing System:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top-down manner; the processes must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps to disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- **Undertaking Overall Analysis of the Existing system:** Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of the present work volume; the current personnel requirements; the present costs-benefits of each of these must be investigated thoroughly.

(b) The five key principles of COBIT 5 are as follows:

- **Principle 1: Meeting Stakeholder Needs:** Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organization, risk appetite, etc.), and requires a customized governance and management system. Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals

cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

- **Principle 2: Covering the Enterprise End-to-End:** COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone - internal and external that is relevant to governance and management of enterprise information and related IT.
 - **Principle 3: Applying a Single Integrated Framework:** There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.
 - **Principle 4: Enabling a Holistic Approach:** Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.
 - **Principle 5: Separating Governance from Management:** The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.
- (c) Some of the important characteristics of Cloud Computing are as follows:
- **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
 - **Agility:** The cloud works in the distributed mode environment that allows sharing of resources among users and tasks, while improving efficiency and agility (responsiveness).
 - **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
 - **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
 - **Services in Pay-Per-Use Mode:** Service Level Agreements (SLAs) between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
 - **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
 - **Performance:** It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
 - **Maintenance:** The cloud computing applications are easier because they are not to be installed on each user's computer and can be accessed from different places.