

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

*Candidates are also required to answer any **five** questions
from the remaining **six** questions.*

Question 1

XYZ Limited is an international public-private partnership based organization established in the year 2011. The organization is engaged in development of pandemic medicines and also acts as an angel investor for many start-up companies and supports them by providing technical training, mentorship, fund raising and financing for development of medicines. In the recent past, the top management reviewed the adequacy of the controls on the data security, business continuity management, and disaster recovery procedure and found that standard operating procedures of the organization are not aligned with the current best practices used in the industry. Hence, the top management appointed Mr. A as Information System (IS) auditor for conducting internal IS audit. Mr. A used risk based approach for auditing the various information systems and submitted the IS audit report to the top management. Mr. A has indicated the various shortcomings in the IS audit report, some of them are as under:

- There is no formal IT governance framework and IT policy has not been updated and documented since 2011. Failure to regularly review and approve GEIT documentation has resulted in outdated, inaccurate and incomplete IT plans. Incorrect IT plan documentation have resulted in incorrect or ineffective actions being taken by the personnel in response to emergency or disaster causing additional harm to customers, employees, loss of assets and the reputational damage. The organization does not have consistent vulnerability management program. The network of organization's infrastructure is not documented and kept up-to date to facilitate risk assessment and identification of potential issues for security.*
- The organization has not undertaken formal risk assessment activity since its inception for updating control procedures for improving security to various business processes. Failure to understand the key risks, their impact on activities and resources critical for delivering services, limits the effectiveness and completeness of IT plan for maintaining continuity of operation and safely executing recovery operations from disaster.*
- Roles and responsibilities in relation to business continuity planning and disaster recovery planning have not been clearly defined. Employees are not trained and tested on performance of emergency management, business continuity and disaster recovery operations.*

For achieving the state of art technological status aligned with best practices in industry for adequacy of controls for security, business continuity planning and disaster recovery planning, Mr. A has suggested to use COBIT 5 framework, periodic review and update of policies, IT plans and strengthening of document & record control process in the organization. He has also

suggested for conducting risk assessment at least once in a year to design better control system for improving the security of IT operations specifically preventing the theft of information of the latest R&D results.

Read the above carefully and answer the following questions:

- (a) *Risk management is the process of assessing the risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. You have been assigned to implement Risk Management for the organization. Describe briefly various key management practices for implementing Risk Management in the above organization. (6 Marks)*
- (b) *The methodology for developing a Business Continuity Plan can be sub-divided into different phases. During vulnerability assessment and general definition of requirements phase, this phase addresses measures to reduce the probability of occurrence. You are requested to suggest the various management key tasks, which are included in this phase. (5 Marks)*
- (c) *Mr. A has followed the Risk Based Approach for auditing the Information Systems of the organization. Explain briefly key steps that can be followed for a risk-based approach to make an audit plan for information systems. (3 Marks)*

Answer

- (a) The key Management Practices for implementing Risk Management in an organization 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 Information Technology 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) The Vulnerability assessment and general definition of requirement phase methodology for developing a Business Continuity Plan (BCP) includes the following key tasks:
- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
 - The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement if none exist.
 - Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
 - Define the scope of the planning effort.
 - Analyze, recommend, and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
 - Develop a Plan Framework.
 - Assemble Project Team and conduct awareness sessions.
- (c) The steps that can be followed for a risk-based approach to make an audit plan for information systems are as follows:
- Inventory the information systems in use in the organization and categorize them.
 - Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
 - Assess what risks affect these systems and the severity of the impact on the business.
 - Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Question 2

- (a) *With the advancements in the technology, cyber frauds are also increasing day-by day across the world. What are the major reasons behind the rise of such frauds in an enterprise? Also, explain briefly the impacts of cyber frauds on enterprises.* **(6 Marks)**
- (b) *Management Information System (MIS) supports the managers at different levels to take decisions to fulfill the organizational goals. Explain briefly any five major characteristics of an effective MIS.* **(5 Marks)**
- (c) *Explain different types of Audit during System Development process.* **(3 Marks)**

Answer

(a) Major reasons behind the rise of cyber frauds in an enterprise are as follows:

- Failure of internal control system,
- Failure of organizations to update themselves to new set of risk, and
- Smart fraudsters who are able to target the weaknesses in system, lacunae's in internal controls, even before the organization realizes that such gaps are there.

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- **Loss of credibility or Competitive Edge:** News that an organizations database has been hit by fraudsters leads to loss of competitive advantage and lose credibility. There have been instances where share prices of such companies went down, as the news of such attack percolated to the market.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
- **Sabotage:** The above situation may lead to misuse of such information by enemy country.

(b) Major characteristics of an effective Management Information Systems (MIS) are as follows:

- **Management Oriented:** It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.
- **Management Directed:** Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- **Integrated:** The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied

together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.

- **Common Data Flows:** It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
 - **Heavy Planning Element:** An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
 - **Sub System Concept:** Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
 - **Common Database:** Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.
 - **Computerized:** Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.
- (c) Different types of Audit that may be conducted during System Development process are as follows:
- **Concurrent Audit:** Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
 - **Post -implementation Audit:** Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they

might be evaluating whether the system needs to be scrapped, continued, or modified in some way.

- **General Audit:** Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

Question 3

- (a) *XYZ bank is required to update its Information Systems to release new product in the market. The technical team of the bank calculates and proposes a timeline of 18 months to update the system and release the new version of the software, but top management wants to release the product in the market as soon as possible. The top management appoints you as a consultant to advise suitable systems development methodology to the technical team of the bank for the same. You are requested to explain; why Agile Model should be adopted for systems development methodology?* **(6 Marks)**
- (b) *Electronic door locks are always preferred by many enterprises as controls for Physical Access Exposures. Describe briefly any five advantages of electronic door locks over bolting and combinational locks.* **(5 Marks)**
- (c) *Describe briefly any three major benefits of an Expert System.* **(3 Marks)**

Answer

- (a) Agile Model should be adopted as systems development methodology because of its following strengths as identified by many experts and practitioners:
- Agile model is an organized set of software development methodologies based on the iterative and incremental development where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.
 - Agile methodology promotes adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change.
 - Agile Model is a conceptual framework that promotes foreseen interactions throughout the development life cycle.
 - Agile methodology has the concept of an adaptive team which enables to respond to the changing requirements, even late in development.
 - The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.
 - Face to face communication and continuous inputs from customer representative leaves a little space for guesswork.
 - The documentation is crisp and to the point to save time.

- The end result is generally the high-quality software in least possible time duration and satisfied customer.
- (b) Following are some advantages of Electronic Door locks over bolting and combinational locks:
- Through the special internal code, cards can be made to identify the correct individual.
 - Individuals access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to particular doors or to particular hours of the day.
 - Degree of duplication is reduced.
 - Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted, silent or audible alarms can be automatically activated.
 - An administrative process, which may deal with issuing, accounting for and retrieving the card keys, are also part of security. The card key becomes an important item to retrieve when an employee leaves the firm.
 - Biometric Door Locks are extremely secure where an individual's unique body features such as voice, retina, fingerprint or signature are used to activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.
- (c) The key benefits of Expert Systems are as follows:
- Expert Systems preserve knowledge that might be lost through retirement, resignation, or death of an acknowledged company expert.
 - Expert Systems put information into an active form so it can be summoned almost as a real-life expert might be summoned.
 - Expert Systems assist novices in thinking the way experienced professionals do.
 - Expert Systems are not subjected to human feelings such as fatigue, being too busy, or being emotional.
 - Expert Systems can be effectively used as a strategic tool in the areas of marketing products, cutting costs and improving products.

Question 4

- (a) *ABC Limited is a software development company providing on-line marketing solutions including web design, content management and e-commerce solutions and various support services. The top management has assigned you to conduct Information System (IS) Audit of the company. Explain briefly various steps to be followed by you for conducting the IS Audit.*
- (6 Marks)**

- (b) *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. In the above context, explain briefly the five key principles of COBIT 5.*

(5 Marks)

- (c) *In case of development of Business Continuity Plan (BCP), what are the objectives of performing BCP tests? Describe briefly any three objectives.*

(3 Marks)

Answer

- (a) Various steps to be followed for conducting Information Systems Audit are as follows:
- (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 this stage, 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.
- (b) Five 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 the required processes and other enablers to support business value creation through 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.

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 structure and serve different purposes.
- (c) In case of Development of Business Continuity Plan (BCP), the objectives of performing BCP tests are to ensure that:
- the recovery procedures are complete and workable.
 - the competence of personnel in their performance of recovery procedures can be evaluated.
 - the resources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
 - the manual recovery procedures and IT backup system/s are current and can either be operational or restored.

- the success or failure of the business continuity training program is monitored.

Question 5

- (a) *Control is a system that prevents, detects or corrects unlawful events. Various controls are adapted as per requirement and accordingly, their audit become necessary. You are appointed as an IS auditor to advise the various management factors influencing an organization towards controls and audit of computers. Explain these factors. (6 Marks)*
- (b) *Systems Requirements Analysis phase analyses the typical system requirements, in view of its functionalities, deliverables etc. You have been assigned the task to suggest various objectives, which are performed in this phase in order to generate the deliverable, Systems Requirements Specifications (SRS). Explain these objectives in brief. (5 Marks)*
- (c) *Describe any three benefits of Governance of Enterprise IT (GEIT). (3 Marks)*

Answer

- (a) Various factors influencing an organization toward controls and audit of computers are as follows:
- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
 - **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations, and correction of the processes. These high-level decisions require accurate data to make quality decision rules.
 - **Costs of Computer Abuse:** Unauthorised access to computer systems, malware, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets like hardware, software, data, information etc.
 - **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
 - **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
 - **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
 - **Controlled evolution of computer Use:** The use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

- (b) The following objectives are performed in System Requirements Analysis phase in order to generate the deliverable Systems Requirements Specification (SRS):
- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
 - To analyze requirements to detect and correct conflicts and determine priorities;
 - To gather data or find facts using tools like interviewing, research/document collection, questionnaires, observation;
 - To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
 - To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
 - To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.
- (c) The benefits of Governance of Enterprise IT (GEIT) are 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 6

- (a) ABC is a global consultation and IT service providing company in the area of information and cyber security. The company is seeking your advice for adopting an ISO-27001 standard. Explain briefly various reasons for adoption of the ISO-27001 standard and also key benefits of ISO-27001 to be achieved by the company. **(6 Marks)**
- (b) Describe the various characteristics of Infrastructure as a Service (IaaS) model of Cloud Computing. **(5 Marks)**
- (C) The Security and Exchange Board of India (SEBI) is the regulator for the securities market in India. What are the requirements of systems audit, which SEBI had mandated for exchanges? **(3 Marks)**

OR

Enterprises need to take steps to ensure compliance with cyber laws. Explain briefly any three key steps for ensuring compliance with cyber laws in an enterprise.

Answer

(a) A company may adopt ISO 27001 standard for the following reasons:

- It is suitable for protecting critical and sensitive information.
- It provides a holistic, risk-based approach to secure information and compliance.
- It demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
- It demonstrates security status according to internationally accepted criteria.
- It creates a market differentiation due to prestige, image and external goodwill.
- If a company is certified once, it is accepted globally.

The key benefits of ISO 27001 standard are as follows:

- It can act as an extension of the current quality system to include security.
- It provides an opportunity to identify and manage risks to key information and systems assets.
- It provides confidence and assurance to trading partners and clients and acts as a marketing tool.
- It allows an independent review and assurance to stakeholder on information security practices.

(b) The characteristics of Infrastructure as a Service (IaaS) model of Cloud Computing are as follows:

- **Web access to the resources:** The IaaS model enables the IT users to access infrastructure resources over the Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.
- **Centralized management:** The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.
- **Elasticity and Dynamic Scaling:** Depending on the load, IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.
- **Shared infrastructure:** IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.
- **Metered Services:** IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

- (c) For Systems Audit, Security and Exchange Board of India (SEBI) had mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.
- The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.
 - Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange/Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.
 - Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit and previous audit.
 - The scope of the Audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.
 - Audit has to be conducted and the Audit report be submitted to the Auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit reports in consideration and cover any open items therein.
 - The Auditee management provides their comment about the Non-Conformities (NCs) and observations. For each NC, specific time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.

OR

Enterprises need to take steps to ensure compliance with cyber laws. Some key steps for ensuring compliance are given below:

- Designate a Cyber Law Compliance Officer as required.
- Conduct regular training of relevant employees on Cyber Law Compliance.
- Implement strict procedures in HR policy for non-compliance.
- Implement authentication procedures as suggested in law.
- Implement policy and procedures for data retention as suggested.
- Identify and initiate safeguard requirements as applicable under various provisions of the Act such as Sections 43A, 69, 69A, 69B, etc.
- Implement applicable standards of data privacy on collection, retention, access, deletion etc.
- Implement reporting mechanism for compliance with cyber laws.