PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

*Question No. **1** is compulsory.*

*Candidates are required to answer any **four** questions*

*from the remaining **five** questions.*

Question 1

ABC Limited is a marketing company having multiple branches across India. The company is planning to expand its business by opening new branches in India as well as in abroad. With such expansion of business and related activities thereon, the company wants to ensure Information Technology compliance with the help of implementation of COBIT 5. The company has invited proposals from various vendors for the purchase of hardware and software to support the proposed expansion. The Board of Directors wants to follow the best practices in areas of Governance, which are adopted across the industry, in the activities of the company.

You are appointed as a consultant in the company. Please answer the following queries raised by the management of ABC Limited.

(a) What are the various methods to validate the vendor's proposal received in respect of the hardware and software purchase? ***(6 Marks)***

(b) As the consultant of the company, you are asked to explain the major benefits of Governance to the Board of Directors. ***(5 Marks)***

(c) COBIT 5 provides key management practices for ensuring compliance with external compliance as relevant to the enterprise. Explain the key management practices to help the management of the company to ensure IT compliance. ***(3 Marks)***

Answer

(a) Some of the methods to validate the vendor's proposal received in respect of the hardware and software purchase are as follows:

- **Checklists:** It is the simplest and a subjective method for validation and evaluation. The various criteria are put in check list in the form of suitable questions against which the responses of the various vendors are validated. For example - Support Service Checklists may have parameters like Performance; System development, Maintenance, Conversion, Training, Back-up, Proximity, Hardware and Software.
- **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting a final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Thus, even for a small business, the evaluators must consider such issues as the company's data processing needs, its in-house computer skills, vendor reputations, software costs, and so forth.
- **Public Evaluation Reports:** Several consultancies as well as independent agencies

compare the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by several buyers in the past. For those criteria, however, where published reports are not available, reports would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts.

- **Benchmarking problems related Vendor's Solutions:** Benchmarking problems related to vendors' proposals are accomplished by sample programs that represent at least a part of the buyer's primary work load and include considerations and can be current applications that have been designed to represent planned processing needs. That is, benchmarking problems are oriented towards testing whether a solution offered by the vendor meets the requirements of the job on hand of the buyer.
- **Testing Problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to translate the source code into the object code, response time for two or more jobs in multi-programming environment, overhead requirements of the operating system in executing a user program, length of time required to execute an instruction, etc. The results, achieved by the machine can be compared and price performance judgment can be made. It must be borne in mind, however that various capabilities to be tested would have to be assigned relative weight-age.

(b) Major benefits of Governance can be summarized as follows:

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

(c) The key management practices provided by COBIT 5 to help the management of the company to ensure IT compliance are 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.

Question 2

(a) In order to cope up with the new technology usage in an enterprise, the auditor shall be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria. In light of this, discuss the issues involved in the performance of evidence collection and understanding the reliability of controls. ***(6 Marks)***

(b) The intuitive character of executive decision-making is reflected strongly in the types of information found most useful to executives. Briefly explain the characteristics of the types of information used in executive decision-making. ***(5 Marks)***

(c) Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. List any three 'disadvantages and limitations' of the use of continuous audit techniques. ***(3 Marks)***

Answer

(a) The performance of evidence collection and understanding the reliability of controls involves issues like-

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained on-line and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client's computer system may save data on detachable storage device by

summarising transactions into monthly, weekly or period end balances.

- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of Electronic Data Interchange (EDI) will result in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made in terms of its legal jurisdiction, what are the terms of the contract and which are the parties to the contract. Furthermore, the laws regarding the admissibility of computer evidence varies from one country to another and from one court to another.

(b) The characteristics of the types of information used in executive decision-making are as follows:

- **Lack of structure:** Many of the decisions made by executives are relatively unstructured. These types of decisions are not as clear-cut as deciding how to debug a computer program or how to deal with an overdue account balance. Also, the questions like 'which data are required' or 'how to weigh available data when reaching a decision' are generally not always obvious.
- **High degree of uncertainty:** Executives work in a decision space that is often characterized by a lack of precedent. For example, when the Arab oil embargo hit in mid 1970s, no such previous event could be referenced for advice. Executives also work in a decision space where results are not scientifically predictable from actions.

If prices are lowered, for instance, product demand will not automatically increase.

- **Future orientation:** Strategic-planning decisions are made to shape future events. As conditions change, enterprises must change also. It is the executive's responsibility to make sure that the organization keeps pointed toward the future. Some key questions about the future external environment include: "How will future technologies affect what the company is currently doing? What will the competition (or the government) do next? What products will consumers demand five years from now?"
- **Informal Source:** Executives, more than other types of managers, rely heavily on informal source for key information. For example, lunch with a colleague in another firm might reveal some important competitor strategies. Informal sources such as television might also feature news of momentous concern to the executive – news that he or she would probably never encounter in the company's database or in scheduled computer reports.
- **Low level of detail:** Most important executive decisions are made by observing broad trends. This requires the executive to be more aware of the large overview than the tiny items. Even so, many executives insist that the answers to some questions can only be found by mucking through details.

(c) Following are some of the disadvantages and limitations of the use of the continuous audit system:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

Question 3

(a) You are appointed as consultant in an organization for its program development and implementation. The management has requested you to briefly describe the various phases of Program Development Life Cycle. ***(6 Marks)***

(b) Explain the Tactical Layer of Application Security Layer and the audit issues relating to the tactical layer with respect to the application security control auditing. ***(5 Marks)***

(c) Define the following terms with reference to Information Technology Act.

(i) *Electronic Form*

(ii) *Information*

(iii) *Key Pair* ***(3 Marks)***

Answer

(a) The primary objective of Program Development Life Cycle phase within the Systems Development Life Cycle is to produce or acquire and to implement high-quality programs. This includes the following phases:

- **Planning:** Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
- **Control:** The Control phase has two major purposes:
  - Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations.
  - Control over software development, acquisition, and implementation tasks should be exercised to ensure that the software released for production use is authentic, accurate, and complete.
- **Design:** A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
- **Coding:** Programmers must choose a module implementation and integration strategy like Top-down, Bottom-up and Threads approach; a coding strategy that follows the percepts of structured programming, and a documentation strategy to ensure program code is easily readable and understandable.
- **Testing:** These tests are to ensure that a developed or acquired program achieves its specified requirements. These are as follows:
  - **Unit Testing –** which focuses on individual program modules;
  - **Integration Testing –** Which focuses in groups of program modules; and
  - **Whole-of-Program Testing** – which focuses on whole program.
- **Operation and Maintenance:** Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used are as follows:
  - **Repair Maintenance:** in which program errors are corrected;
  - **Adaptive Maintenance:** in which the program is modified to meet changing user requirements; and
  - **Perfective Maintenance:** in which the program is tuned to decrease the resource consumption.

(b) **Tactical Layer of the Application Security Layer:** Also, known as Management Layer, it is the second layer in application security that includes supporting functions such as security administration, IT risk management and patch management.

Various audit issues relating to the Tactical Layer are related to security administration that includes -

- Timely updates to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
- **IT Risk Management:** An auditor should understand the risk associated with each application and obtain a report on periodic risk assessment on the application or self-assessment/ compliance reports on the application. This includes the following activities:
  - Assessing risk over key application controls;
  - Conducting a regular security awareness programme on application user;
  - Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to gauge the users' understanding about application security;
  - Reviewing application patches before deployment and regularly monitoring critical application logs;
  - Monitoring peripheral security in terms of updating antivirus software.
- **Interface Security:** This relates to application interfaced with another application in an organization. An auditor needs to understand that data flow to and from the application. Security of the interfaced data is also important, especially when unencrypted methods of transmission are used for data transmission.
- **Audit Logging and Monitoring:** Regular monitoring the audit logs is required. The same is not possible for all transactions, so must be done on an exception reporting basis.

(c) The definition of the following terms with reference to Information Technology Act is as follows:

(i) "**Electronic Form**" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

(ii) "**Information**" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

(iii) "**Key Pair**", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify

a digital signature created by the private key.

Question 4

(a) Explain the characteristics of Software as a Service In cloud computing. ***(6 Marks)***

(b) Discuss various levels of classification of information in an organization. ***(5 Marks)***

(c) PQR Insurance Company Limited is providing insurance services to Indian citizens. What are the requirements of IRDA for System Audit in respect of this company? ***(3 Marks)***

Answer

(a) Characteristics of Software as a Service (SaaS) are as follows:

- **One-to-Many:** SaaS services are delivered as one-to-many models where a single instance of the application can be shared by multiple customers.
- **Web Access:** SaaS services allow the end users to access the application from any location of the device if connected to the Internet.
- **Centralized Management:** Since SaaS services are hosted and managed from the central location, the SaaS providers perform the automatic updates to ensure that each customer is accessing the most recent version of the application without any user-side updates.
- **Multi-device Support:** SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones, and thin clients.
- **Better Scalability:** Most of the SaaS services leverage Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) for its development and deployment and ensure a better scalability than traditional software.
- **High Availability:** SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented.
- **Application Program Interface (API) Integration:** SaaS services have the capability of integrating with other software or service through standard APIs.

(b) Classification of Information are as follows:

- **Top Secret:** Highly sensitive internal information e.g. pending mergers or acquisitions; investment strategies; plans or designs; that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.
- **Highly Confidential:** Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants

etc., patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.

- **Proprietary:** Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level should be high.
- **Internal Use only:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should controlled but normal.
- **Public Documents:** Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should minimal.

(c) The requirements of Insurance Regulatory and Development Authority of India (IRDA) for System Audit in respect of PQR Insurance Company Ltd are as follows:

- All insurers shall have their systems and process audited at least once in three years by a CA firm.
- In doing so, the current internal or concurrent or statutory auditor is not eligible for appointment.
- CA firm must be having a minimum of 3-4 years' experience of IT systems of banks or mutual funds or insurance companies.

Question 5

(a) Briefly explain the components of BCM process. ***(6 Marks)***

(b) You are appointed to audit the Information Systems of XYZ Limited. Please enlighten the management about various categories of Information Systems Audits. ***(5 Marks)***

(c) Write a short note on Business Intelligence. ***(3 Marks)***

Answer

(a) The components of Business Continuity Management (BCM) Process are as follows:

- **BCM – Process:** The management process enables the business continuity, capacity and capability to be established and maintained. The capacity and capability are established in accordance to the requirements of the enterprise.
- **BCM – Information Collection Process:** The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will

determine the selection of appropriate BCM strategies in the next process.

- **BCM – Strategy Process:** Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will consider the processes and technology already present within the enterprise.
- **BCM – Development and Implementation Process:** Development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- **BCM – Testing and Maintenance Process:** BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.
- **BCM – Training Process:** Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

(b) Information Systems Audit has been categorized into five types:

(i) **Systems and Application:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

(iii) **Systems Development:** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (end-point device), server, and on the network connecting the clients and servers.

(c) **Business Intelligence** (BI) refers to applications and technologies that are used to collect and provide access and analyze data and information about company's operations. A complete Business Intelligence provides consistent and standard information essential in enterprise operations and consists of range of tools. Some BI applications are used to

analyze performance or internal operations e.g. EIS (Executive Information System), business planning, finance and budgeting tools. Some BI applications are used to store and analyze data, for example - Data mining, Data Warehouses, Decision Support System etc. Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools.

Question 6

(a) Explain the sections contained in a well-documented Systems Requirement Specifications (SRS). ***(6 Marks)***

(b) In the present day, the enterprises not only need to protect there IS assets against cyber-attack but also need to take steps to ensure compliance with cyber laws as well. What are the key steps for ensuring such compliance? ***(5 Marks)***

(c) Write a short note on the Audit of Quality Assurance Management Controls. ***(3 Marks)***

OR

Write any three major strengths of Agile Model of Software Development. ***(3 Marks)***

Answer

(a) A well-documented Systems Requirement Specification (SRS) may normally contain the following sections:

- **Introduction:** Goals, Objectives, software context, Scope and Environment of the computer-based system.
- **Information Description:** Problem description; Information content, flow and structure; **Hardware**, software, human interfaces for external system elements and internal software functions.
- **Functional Description:** Diagrammatic representation of functions; processing narrative for each function; Interplay among functions; Design constraints.
- **Behavioral Description:** Response to external events and internal controls.
- **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.
- **Appendices:** Data flow/Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review:** The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer. The review reflects the development team's understanding of the existing processes. Only, after ensuring that the document represents existing processes accurately, the user should sign the document. This is a technical requirement of the contract between users and development team/organization.

(b) Enterprises not only need to protect their Assets against cyber-attack but also need to take steps to ensure compliance with cyber laws as well. Some key steps for ensuring such 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.

(c) Audit of Quality Assurance Management Controls is as follows:

- Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
- Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.
- Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

Or

Some of the strengths of Agile Model of Software Development as identified by experts and practitioners include the following:

- Agile methodology has the concept of an adaptive team, which enables to respond to the changing requirements.
- 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.