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 Appliances Ltd., is a popular marketing company, which has branches in any locations. It does all its business activities on-line such as exchanging information relating to the buying and selling of goods, distribution information and providing customer support. With the increase in business activities and increase in regulations, the company is facing several problems with its existing information system. It realizes that the existing Information System has to be improved and proper controls have to be incorporated. It wishes to enhance the existing Information System and put in sufficient measures to ensure security of data and protect the company against breaches caused by security failures. The company has decided to use a third party site for backup and recovery procedures. To develop the new system the company formed a full-fledged System Development team. The team followed all the phases in the SDLC and implemented the new system successfully.

The company was also satisfied with the post-implementation audit report. Answer the following questions based on the above:

(a) As a system development team member, explain the areas that should be studied in depth to understand the present system.

(b) Discuss the activities that deal with the Systems Development Management Controls in the IT set-up.

(c) What are the issues that the security administrators should consider when drafting the contract with a third party for a backup and recovery site?

(d) As an IS auditor, how do you evaluate the performance of the following Managerial Controls: [i] Data Resource Management Controls and [ii] Security Management Controls. ***(5 x 4 = 20 Marks)***

Answer

(a) As a System development team member, following areas should be studied to understand the present system:

- **Reviewing Historical Aspects:** The historical facts of an organization enable the system analyst 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.
- **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. 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.
- **Reviewing Methods, Procedures and Data Communications:** Methods and procedures transform input data into useful output. 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 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 it is kept on file, etc. must be investigated.
- **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 equipment 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 activities that deal with Systems Development Management Controls in the IT setup are as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.
- **User Specification Activities:** Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals.
- **Technical Design Activities:** The technical design activities in the Systems Development Life Cycle (SDLC) translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase.
- **Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.
- **Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined

results to identify programming and logic errors. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests

- **User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s). The formal test and acceptance of the system should consider being the most important control over the SDLC.

(c) If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as -

- how soon the site will be made available subsequent to a disaster;
- the number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- the priority to be given to concurrent users of the site in the event of a common disaster;
- the period during which the site can be used;
- the conditions under which the site can be used;
- the facilities and services the site provider agrees to make available; and
- What controls will be in place and working at the off-site facility?

(d) **(i)** To evaluate the performance of Data Resource Management Controls under Managerial Controls, an IS Auditor -

- Should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.
- Might employ test data to evaluate whether access controls and update controls are working.

(ii) To evaluate the performance of Security Management Controls under Managerial Controls, an IS Auditor -

- must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;
- checks whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and

- Checks whether the organizations have opted for an appropriate insurance plan or not.

Question 2

(a) What are the key management practices to be implemented for evaluating Business Value from the use of IT? State any three-key metrics which can be used for such evaluation.

(b) State any six objectives of the National Cyber Security Policy 2013 issued by the Government of India.

(c) Briefly explain any four features of Electronic mail. ***(6 + 6 + 4 = 16 Marks)***

Answer

(a) The key management practices, which need to be implemented for 'evaluating business value is derived from the use of Information Technology (IT)', are highlighted as under:

- **Evaluate Value Optimization:** Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.
- **Direct Value Optimization:** Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.
- **Monitor Value Optimization:** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

Some of the key metrics, which can be used for such evaluation, are as follows:

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

(b) Major objectives of the National Cyber Security Policy 2013 policy issued by the Government of India are as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in 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 Information and Communication Technologies (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 & 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 & 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.

(c) Various features of Electronic mail are stated below:

- **Electronic Transmission:** The transmission of messages with email is electronic and message delivery is very quick, almost instantaneous. The confirmation of transmission is also quick and the reliability is very high.
- **Online Development and Editing:** The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication and facilitates the storage of messages on magnetic media, thereby reducing the space required to store the messages.
- **Broadcasting and Rerouting:** Email permits sending a message to many target recipients. Thus, it is easy to send a circular to all branches of a bank using Email resulting in a lot of saving of paper. The email could be rerouted to people having direct interest in the message with or without changing or and appending related information to the message.
- **Integration with other Information Systems:** The E-mail has the advantage of being integrated with the other information systems that helps in ensuring that the message is accurate and the information required for the message is accessed quickly.
- **Portability:** Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal Computer/tablet/smart phones equipped with the relevant communication hardware, software and link facilities.
- **Economical:** Email is one of the most economical modes for sending and receiving messages. Since the speed of transmission is increasing, the time and cost on communication media per page is very less. Thus, email is very helpful not only for formal communication but also for informal communication within the enterprise.

Question 3

(a) Based on the Institute of Internal Auditors (IIA) guidance, briefly explain any six sample areas which can be reviewed by Internal Auditors as part of the review of GRC.

(b) List the components of the Information Security Policy.

(c) What is meant by the Core Banking System (CBS)? List its elements. ***(6 + 6 + 4 Marks)***

Answer

(a) Based on the Institute of Internal Auditors (IIA) guidance, the sample areas which can be reviewed by Internal Auditors as part of review of Governance, Risk and Compliance (GRC) are as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the objectives like promoting appropriate ethics and values within the organization; ensuring effective organizational performance management and accountability; communicating risk and control information to appropriate areas of the organization; and coordinating the activities of and communicating information among the board, external and internal auditors, and management.
- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **Interpretation:** This determines whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that organizational objectives support and align with the organization's mission; significant risks are identified and assessed; appropriate risk responses are selected that align risks with the organization's risk appetite; and relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.
- **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.
- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the achievement of the organization's strategic objectives; reliability and integrity of financial and operational information; effectiveness and efficiency of

operations and programs; safeguarding of assets; and compliance with laws, regulations, policies, procedures, and contracts.

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

(b) The components of the Information Security Policy are as follows:

- Purpose and Scope of the Document and the intended audience;
- The Security Infrastructure;
- Security policy document maintenance and compliance requirements;
- Incident response mechanism and incident reporting;
- Security organization Structure;
- Inventory and Classification of assets;
- Description of technologies and computing structure;
- Physical and Environmental Security;
- Identity Management and access control;
- Information Technology (IT) Operations management;
- IT Communications;
- System Development and Maintenance Controls;
- Business Continuity Planning;
- Legal Compliances; and
- Monitoring and Auditing Requirements.

(c) **Core Banking System (CBS)** - Core Banking is a banking services provided by a group of networked bank branches where customers may access their bank account and perform basic transactions from any of the member branch offices. Core Banking System (CBS) may be defined as a back-end system that processes daily banking transactions, and posts updates to accounts and other financial records. These systems typically include deposit, loan and credit-processing capabilities, with interfaces to general ledger

systems and reporting tools. Core banking functions differ depending on the specific type of bank. Banks make these services available across multiple channels like ATMs, Internet banking, and branches.

Elements of core banking include the following:

- Making and servicing loans.
- Opening new accounts.
- Processing cash deposits and withdrawals.
- Processing payments and cheques.
- Calculating interest.
- Customer Relationship Management (CRM) activities.
- Managing customer accounts.
- Establishing criteria for minimum balances, interest rates, number of withdrawals allowed and so on.
- Establishing interest rates.
- Maintaining records for all the bank's transactions.

Question 4

(a) While developing a Business Continuity Plan what are the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement'?

(b) What is the definition of the following terms III the Information Technology, Act? [i] Computer resource [ii] Digital signature [iii] Electronic record [iv] Private key [v] Public key and [vi] Secure System.

(c) What are the key steps to be followed in a risk based approach to make an audit plan?

(6 + 6 + 4 = 16 Marks)

Answer

(a) Following key tasks should be covered in the second phase 'Vulnerability Assessment and General Definition of Requirements' while developing a Business Continuity Plan (BCP).

- 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 required emergency plans and disaster prevention measures where 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 the 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.

(b) The definitions as per Information Technology Act, 2000 (Amended) are as follows:

(i) "**Computer Resource**" means computer, communication device, computer system, computer network, data, computer database or software.

(ii) "**Digital Signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the Act.

(iii) "**Electronic Record**" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

(iv) **"Private Key"** means the key of a key pair used to create a digital signature.

(v) **"Public Key"** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

(vi) **"Secure System"** means computer hardware, software, and procedures that are reasonably secure from unauthorized access and misuse; provide a reasonable level of reliability and correct operation; are reasonably suited to performing the intended functions; and adhere to generally accepted security procedures.

(c) The steps that can be followed for a Risk-based approach to make an audit plan 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 5

(a) How can Audit Trails be used to support security objectives? Briefly explain.

(b) With respect to Top Management and in IS management control, the major activities that the senior management must perform are: Planning, Organising, Leading and Controlling in the Information System functions. Explain the role of the IS auditor in any three of the above-mentioned activities.

(c) What is BCP? What are the three areas it should cover? ***(6 + 6 + 4 = 16 Marks)***

Answer

(a) Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact, detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances; the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(b) With respect to Top Management and Information Systems Management Control, the major activities that the senior management must perform are Planning, Organizing, Leading and Controlling in the Information System functions. The Role of Information Systems (IS) auditor at each activity is discussed below:

- **Planning:** Auditors need to evaluate whether top management has formulated a high-quality Information System's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.
- **Organizing:** Auditors should be concerned about how well top management acquires and manages staff resources for three reasons:
  - The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.
  - Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.
  - Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.
- **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources of evidence to evaluate how well top managers communicate with their staff. The formal sources include IS plans, documents standards and policies whereas the informal sources of evidence include interviews with IS staff about their level of satisfaction with the top management. Auditors must try to assess both the short-run and long-run consequences of poor communications within the information systems function and to assess the implications for asset safeguarding, data integrity, system effectiveness, and system efficiency.
- **Controlling:** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

(c) Business Continuity Planning (BCP): It is the creation and validation of a practical logistical plan for how an enterprise will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called business continuity plan.

Alternate Definition of BCP: It refers to the ability of enterprises to recover from a disaster and continue operations with least impact. It is imperative that every enterprise has a business continuity plan as relevant to the activities of the enterprise.

Business Continuity Planning should cover the following areas:

- **Business Resumption Planning:** This is the operation's piece of business continuity planning.

- **Disaster Recovery Planning:** This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- **Crisis Management:** This is the overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

Question 6

(a) What does RAD refer to? Briefly explain any five features of RAD.

(b) What are the various types of Application Controls? Explain each control with reference to their performance and the reliability.

(c) Briefly explain the various Output Controls. ***(6 + 6 + 4 = 16 Marks)***

Answer

(a) Rapid Application Development (RAD): RAD refers to a type of software development methodology; which uses minimal planning in favor of rapid prototyping. The planning of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements.

The key features of RAD include the following:

- Key objective is fast development and delivery of a high-quality system at a relatively low investment cost,
- Attempts to reduce inherent project risk by breaking a project into smaller segments and providing more ease-of-change during the development process.
- Aims to produce high quality systems quickly, primarily using iterative Prototyping, active user involvement, and computerized development tools. Graphical User Interface (GUI) builders, Computer Aided Software Engineering (CASE) tools, Database Management Systems (DBMS), Fourth generation programming languages, Code generators and object-oriented techniques etc.
- Key emphasis is on fulfilling the business need while technological or engineering excellence is of lesser importance.
- Project control involves prioritizing development and defining delivery deadlines or "time boxes." If the project starts to slip, emphasis is on reducing requirements to fit the time box, not in increasing the deadline.
- Generally, includes Joint Application Development (JAD), where users are intensely involved in system design, either through consensus building in structured workshops, or through electronically facilitated interaction.

- Active user involvement is imperative.
- Iteratively produces production software, as opposed to a throwaway prototype.
- Produces documentation necessary to facilitate future development and maintenance.
- Standard systems analysis and design techniques can be fitted into this framework.

(b) Various types of Application Controls are as follows:

- Boundary Controls,
- Input Controls,
- Communication Controls,
- Processing Controls,
- Database Controls, and
- Output Controls

These controls enhance the performance and provide greater reliability.

1. **Boundary Controls:** This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. The major controls of the boundary system are the access control mechanisms. Access controls mechanism links the authentic users to the authorized resources, they are permitted to access. The access control mechanism has three steps of Identification, Authentication and Authorization with respect to the access control policy. Major Boundary Control techniques are Cryptography, Passwords, Personal Identification Numbers (PIN), Identification Cards and Biometric Devices.
2. **Input Controls:** These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Controls relating to data input are critical. It might be necessary to reprocess input data in the event, master files are lost, corrupted, or destroyed. Controls relating to instructions are often in the form of changes to data, which are recorded in the audit trail. Thus, source documents or transaction listings are to be stored securely for longer periods for reasons – compliance with statutory requirements. Input controls are divided into Source Document Controls, Data Coding Controls, Batch Controls, and Validation Controls which use different control procedures to achieve the objective.
3. **Communication Controls:** These controls emphasize upon exposures in the communication subsystem; controls over physical components, communication line errors, flows, and links; topological controls, channel access controls, controls over subversive attacks, internetworking controls, and communication architecture controls.

4. **Processing Controls:** The processing subsystem is responsible for computing, sorting, classifying, and summarizing data. Its major components are the Central Processor in which programs are executed, the real or virtual memory in which program instructions and data are stored, the operating system that manages system resources, and the application programs that execute instructions to achieve specific user requirements. Processor Controls, Real Memory Controls, Virtual Memory Controls and Data Processing Controls together ensure fast and reliable processing of the data.
5. **Database Controls:** The controls that protect the integrity of a database when application software acts as an interface to interact between the user and the database are called Update Controls and Report Controls. Major update controls are Sequence Check between Transaction and Master Files; Ensuring of processing of all records on files, processing of multiple transactions for a single record in the correct order and maintenance of a suspense account. Major Report Controls are Standing Data, Print-Run-to Run Control Totals, Print Suspense Account Entries and Existence/Recovery Controls.
6. **Output Controls:** These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer's hard disk. Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent. Various Output Controls are Storage and logging of sensitive, critical forms, Logging of output program executions, Spooling/queuing, Controls over printing, Report distribution and collection controls and Retention controls.

(c) Various Output Controls are as follows:

- **Storage and logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.
- **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data may be compromised.
- **Spooling/queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user can continue working, while the print operation is getting completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents

waiting to be printed on a printer; this should not be subject to unauthorized modifications.

- **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained for reports that were generated and to whom these were distributed. Where users have to collect reports, the user should be responsible for timely collection of the report, especially if it is printed in a public area. A log should be maintained about reports that were printed and collected. Uncollected reports should be stored securely.
- **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

Question 7

*Write short notes on any **four** of the following:*

(a) Components in COBIT

(b) Constraints in operating MIS

(c) Fact finding tools and techniques

(d) The services provided by the SaaS model of Cloud Computing

(e) Back-end architecture of cloud computing ***(4 x 4 = 16 Marks)***

Answer

(a) Components in COBIT are as follows:

- **Framework -**Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;
- **Process Descriptions -**A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

- **Management Guidelines -**Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes
- **Maturity Models -**Assess maturity and capability per process and helps to address gaps.

(b) Major constraints, which come in the way of operating Management Information Systems (MIS) are as follows:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depend upon the need and importance of a function for which MIS can be installed first.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.
- Non-availability of cooperation from staff is a crucial problem, which should be handled tactfully. This task should be carried out by organizing lecturers, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.

(c) Various fact-finding techniques/tools used by the system analyst for determining Systems' needs/requirements are as below:

- **Documents:** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people, who work with the current system, procedure manuals, program codes for the applications associated with the current system, etc. Documents are a very good source of information about user needs and the current system.
- **Questionnaires:** Users and managers are asked to complete questionnaire about the information systems when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.
- **Interviews:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide system developers with a larger picture of the problems and opportunities. Interviews also give analyst the opportunity to observe and record first-hand user reaction and to probe for further information.

- **Observation:** In general, and particularly in prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed.

(d) The services provided by Software as a Service (SaaS) Model of Cloud Computing are as follows:

- **Business Services:** SaaS providers provide a variety of business services to startup companies that include ERP, CRM, billing, sales, and human resources.
- **Social Networks:** Since the number of users of the social networking sites is increasing exponentially, cloud computing is the perfect match for handling the variable load.
- **Document Management:** Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.
- **Mail Services:** To handle the unpredictable number of users and the load on e-mail services, most of the email providers offer their services as SaaS services.

(e) Back End Architecture of Cloud Computing

The Cloud computing architecture consists of a Front End and a Back End connected to each other through a network, usually the Internet. The Front End is the side, the computer user sees and interacts through, and the Back End is the "cloud" section of the system, truly facilitating the services. Back End refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.