

MOCK TEST PAPER – II

FINAL (OLD) COURSE: GROUP – II

PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT

ANSWERS

MULTIPLE CHOICE QUESTIONS

1. (a) Risk Management
2. (b) Salami Technique
3. (c) Imprisonment for a term which may extend to 3 years or with a fine which may extend to 5 lakh rupees or with both.
4. (c) Easy maintenance of storage warehouse
5. (a) (i) – Vulnerability, (ii) – Vulnerability, (iii) – Exposure, (iv) – Risk
6. (c) (i) – (D), (ii) – (C), (iii) – (B), (iv) – (A)
7. (d) To ensure the independence of Information Systems' Auditors.
8. (b) To provide the virtual storage for the data.
9. (a) (ii),(iv),(v),(vi)
10. (a) (iii), (iv), (v)
11. (c) (B) – (i), (D) – (ii), (A) – (iii), (C) – (iii)
12. (b) Differential Backups have efficient use of storage space than full backups.
13. (c) Evaluation of information system against legal feasibility to check for the violation of local legal requirements and applicable statutes.
14. (d) (i)-(D),(ii)-(A),(iii)-(C),(iv)-(E),(v)-(B)
15. (b) Public Key
16. (a) Interoperability
17. (c) Section 66A
18. (c) Public Cloud follows loose Service Level Agreements (SLAs).
19. (d) Supervisor review and sign-off of a document
20. (a) (vi), (vii), (ii), (viii), (v), (i), (iii), (iv)
21. (d) Data Dictionary is commonly used in operations research, specifically in decision analysis to help identify the best strategy.
22. (b) (ii), (v)

DESCRIPTIVE QUESTIONS

1. (a) The key functions of the IT Steering committee include the following:
 - To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
 - To establish size and scope of IT function and sets priorities within the scope;
 - To review and approve major IT deployment projects in all their stages;
 - To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
 - To review the status of IS plans and budgets and overall IT performance;
 - To review and approve standards, policies and procedures;
 - To make decisions on all key aspects of IT deployment and implementation;
 - To facilitate implementation of IT security within enterprise;
 - To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
 - To report to the Board of Directors on IT activities on a regular basis.
- (b) Various Logical Access Controls that are required to be implemented in order to safeguard the company's Application and Monitoring System Access Control are as follows:
 - **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users and ensure that sensitive output is sent only to authorized terminals and locations. For example: read, write, delete, and execute.
 - **Sensitive system isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.
 - **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
 - **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events, and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.
 - **Clock synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

- (c) The role of Information Systems Auditor in auditing physical access controls includes the following:
- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
 - **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
 - **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.
2. (a) Various factors that are crucial for an enterprise to decide the need of Information Systems Auditing 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, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (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:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.
- (b) 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.

These issues are often poorly specified in reciprocal agreements. Moreover, they can be difficult to enforce under a reciprocal agreement because of the informal nature of the agreement.

(c) Transcription Errors: These fall into three classes:

- o Addition errors occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766.
- o Truncation errors occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327.
- o Substitution errors are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.

Transposition Errors: There are two types of transposition errors.

- o Single transposition errors occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.
- o Multiple transposition errors occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

Any of these errors can cause serious problems in data processing if they go undetected. For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account. A similar error in an inventory item code on a purchase order could result in ordering unneeded inventory and failing to order inventory that is needed. These simple errors can severely disrupt operations.

3. (a) Different type of Information Systems are as follows:

- **Operational-Level Systems:** Operational-level systems or Operational Support Systems (OSS) ensure that business procedures are followed. Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use. Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database. The main objective of OSS is to improve the operational efficiency of the enterprise. These information systems support operational managers in tracking elementary activities that can include tracking customer orders, invoice tracking, etc.
- **Knowledge-Level Systems:** These systems support the business to integrate new knowledge into the business and control the flow of paperwork and enable group working. It helps the organization's knowledge and data workers and is especially in the form of workstations. It is the fastest growing application in business today. Office Automation System (OAS) and Knowledge Management System (KMS) are examples of Knowledge Level Systems. These systems support discovery, processing and storage of knowledge and data workers.
- **Management-Level Systems:** These systems support the middle managers in monitoring, decision-making and administrative activities and are helpful in answering questions like - Are things working well and in order? These provide periodic reports rather than instant information on operations. For example - a college control system gives report on the number of leaves availed by the staff, salary paid to the staff, funds generated by the fees, finance planning etc. These types of systems mainly answer "what if" questions. For example - What would be quality of teaching if college has to achieve top ranking in academics? These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems. MSS supports managers in effective decision making by

providing relevant and required information at the right time to the right people. Management Information System and Decision Support Systems are types of Management Level systems.

- **Strategic Level Systems:** These systems are for strategic managers to track and deal with strategic issues, assisting long-range planning. These systems support the senior level management to tackle and address strategic issues and long-term trends, both inside organization and the outside world. These answer questions like what products should be launched to increase the profit and capture the market. It helps in long term planning. A principle area is tracking changes in the external conditions (market sector, employment levels, share prices, etc.) and matching these with the internal conditions of the organization.
- (b) Audit Trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity. Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

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 also 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.
- (c) The key issues of electronic information impacting enterprises and auditors are as follows:
- **Authenticity:** How do we implement a system that ensures that transactions are genuine and authorized?
 - **Reliability:** How do we rely on the information, which does not have physical documents?
 - **Accessibility:** How do we gain access and authenticate this information, which is digital form?

4. (a) The differences between On-premise Private Cloud and Outsourced Private Cloud are as follows:

	On-Premise Private Cloud	Outsourced Private Cloud
Management	It is managed by the organization itself.	It is managed by the third party. Everything is same as usual private cloud except that here the cloud is outsourced.
Service Level Agreements (SLAs)	SLAs are defined between the organization and its users. Users have broader access rights than general public cloud users and service providers are able to efficiently provide the service because of small user base and mostly efficient network.	These are usually followed strictly as it is a third-party organization.
Network	Network management and network issue resolving are easier. The networks usually have high bandwidth and low latency.	The cloud is fully deployed at the third-party site and organizations connect to the third party by means of either a dedicated connection or through Internet.
Security and Data Privacy	Comparatively, it is more resistant to attacks than any other cloud and the security attacks are possible from an internal user only.	Cloud is relatively less secure and the security threat is from the third party and the internal employee.
Location	The data is usually stored in the same geographical location where the cloud users are present. In case of several physical locations, the cloud is distributed over several places and is accessed using the Internet.	The cloud is located off site and when there is a change of location the data need to be transmitted through long distances.
Performance	The performance depends on the network and resources and can be controlled by the network management team.	The performance of the cloud depends on the third party that is outsourcing the cloud.

- (b) Major Boundary Control Techniques are as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. Three techniques of cryptography are Transposition (permute the order of characters within a set of data), Substitution (replace text with a key-text) and Product Cipher (combination of transposition and substitution).
- **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are minimum password length, avoid usage of common dictionary words, periodic change of passwords, hashing of passwords and number of entry attempts.
- **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or

a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission, and storage.

- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use, and card return or card termination phases.
 - **Biometric Devices:** Biometric identification like thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.
- (c) **Business Impact Assessment (BIA):** A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:
- o identify critical systems, processes and functions;
 - o assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and
 - o assess the “pain threshold,” that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

5. (a) **Section 69B** is the section of Information Technology Act, 2000 that defines the “Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security”.

[Section 69B] Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

- (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
- (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorised under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
- (3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
- (4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section, -

- (i) "computer contaminant" shall have the meaning assigned to it in Section 43;
- (ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

(b) Many audit techniques that are available are as follows:

- (i) **Snapshots:** Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.
- (ii) **Integrated Test Facility (ITF):** The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness. This test data would be included with the normal production data used as input to the application system. In such cases the auditor has to decide what would be the method to be used to enter test data and the methodology for removal of the effects of the ITF transactions.
- (iii) **System Control Audit Review File (SCARF):** The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.
- (iv) **Continuous and Intermittent Simulation (CIS):** This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a Database Management System (DBMS). During application system processing, the DBMS reads an application system transaction which is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, the next steps are performed or otherwise it waits to receive further data from the DBMS. CIS replicates or simulates the application system processing. Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces. Exceptions identified by CIS are written to an exception log file. The advantage of CIS is that it does not require modifications to the application system and yet provides an online auditing capability.

Some of the advantages of continuous audit techniques are as under:

- **Timely, Comprehensive and Detailed Auditing** – Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability** – As evidence are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives** - Continuous audit techniques provide information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users** – Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

(c) From the perspective of an Information Systems (IS) Auditor, the following are the possible advantages:

- The IS auditor can have clear understanding of various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his/her examination, can state in his/her report about the compliance by the IS management of the procedures, if any, set by the management.
- The IS Auditor, if has a technical knowledge and ability of different areas of SDLC, can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

6. (a) The factors affecting Input/ Output Form Designs are as follows:

Characteristics	Input Design	Output Design
Content: Refers to the actual pieces of data to be gathered to produce the required output to be provided to users.	The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. New documents for collecting such information may be designed.	The contents of a weekly output report to a sales manager might consist of salesperson's name, sales calls made by each sales person during the week, and the amount of each product sold by each salesperson to each major client category.
Timeliness: Refers to when users need outputs, which may be required on a regular, periodic basis - perhaps daily, weekly, monthly, at the of quarter or annually.	Data needs to be inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system.	A sales manager, may be requiring a weekly sales report. Other users, such as airline agents, require both real- time information and rapid response times in order to render better client service.
Format: Input format refers to the manner in which data are physically arranged. Output format refers to the arrangement referring to data output on a printed report or in a display screen.	After the data contents and media requirements are determined, input formats are designed on the basis of few constraints like - the type and length of each data field as well as any other special characteristics (number decimal places etc.).	Format of information reports for the users should be so devised that it assists in decision-making, identifying and solving problems, planning and initiating corrective action and searching.
Media: Input-output medium refers to the physical device used for input, storage or output.	This includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives may include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based computers and voice input etc. A suitable medium may be	A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape/disk and voice output.

	selected depending on the application to be computerized.	
Form: Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non-quantitative, text, graphics, video and audio.	Forms are pre-printed papers that require people to fill in responses in a standardized way. Forms elicit and capture information required by organizational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.	The form of the output should be decided keeping in view the requirements for the concerned user. For example - Information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for stores.
Input Volume/ Output Volume: Refers to the amount of data that has to be entered in the computer system at any one time. The amount of data output required at any one time is known as output volume.	In some decision-support systems and many real-time processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.	It is better to use high-speed printer or a rapid-retrieval display unit, which are fast and frequently used output devices in case the volume is heavy.

(b) The components of COBIT 5 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.

(c) The benefits of Mobile Computing are as follows:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.