

**MOCK TEST PAPER
FINAL COURSE GROUP – II**

PAPER-6: INFORMATION SYSTEMS CONTROL AND AUDIT

Time Allowed: 3 Hours

Maximum Marks: 100 Marks

Part I: MULTIPLE CHOICE QUESTIONS

Total Marks: 30 Marks

Question Nos. 1 to 8 are based on the case scenario given below:

XYZ University was established in the year 1965 in India and is now one of the premier universities in India. At present, there are 30 affiliated colleges under its umbrella. These colleges operate independently with XYZ University having some level of control or influence over their academic policies, standards or programs. In the recent past, the XYZ University proposes that irrespective of the fact whether the affiliated colleges have their own Library Management System or not, each college must have a commonly shared Online Library Management System (LMS) under its brand name. The management of XYZ University envisaged that –

- The shared LMS can streamline working practices allowing all the affiliated colleges to share their e-learning resources with each other. These resource files are provided as a service through different networks using Cloud Computing.
- Students and researchers will be provided a common platform so that all stakeholders like students and faculties of these affiliated colleges can search e-library collections in a consistent way and accordingly access and share their e-learning resources such as e-books, e-lectures, webinars, videos and powerpoint presentations etc.
- The e-learning resource pool is continuously enhanced with many lectures, webinars and powerpoint presentations of experts, faculties and motivational speakers getting added into it on regular basis.
- The resource pool is updated in terms of addition of relevant e-resources and deletion of irrelevant and redundant content periodically.
- Each college is required to pay on the basis of quantum of the data accessed by its students, faculties and other authorized users. The data may include text, images, sounds and videos.
- Each authorised stakeholder of these colleges will have a unique username and password through which they can have access to these files in only readable mode with no access rights to modify, download, print and email any of them.

To acquire the requisite system, the competent vendors initially were requested to submit their Request for Proposals (RFP) for the requirements highlighted by the XYZ University. The RFPs were duly considered and finally the vendor KIO Ltd. was selected. The XYZ University acquires the customized Online Library Management System through a third-party vendor KIO Ltd.

The responsibility of the vendor KIO Ltd. involves the customization, implementation and maintenance of the system by providing 24x7 support. The centralized database is maintained on a server located in the campus area of XYZ University with well-placed air-conditioners, fire extinguishers, water and smoke detectors. The dedicated IT Team members of KIO Ltd. have full access control to modify, print, read and email of e-resource files as per the request generated.

Based on the above case, answer the following questions:

1. The online LMS of XYZ University is accessed by the registered stakeholders of its affiliated colleges through a unique username and password. The passwords can be changed by the stakeholders. However, the password policy of the application system is not strong enough and allows weak passwords also. Which of the following precisely defines this feature of the application system?
 - (a) Threat
 - (b) Vulnerability
 - (c) Risk
 - (d) Likelihood
2. The online Library Management System (LMS) of XYZ university possesses the characteristics of _____, _____, _____ and _____ systems.
 - (a) Manual, Deterministic, Open, Abstract
 - (b) Automated, Probabilistic, Closed, Physical
 - (c) Automated, Deterministic, Closed, Abstract
 - (d) Automated, Deterministic, Open, Physical
3. To achieve an objective of restricting the individual access privileges to online LMS and data of XYZ university to only authorized users of different affiliated colleges including librarians, faculties, students and IT Support Team members; the Logical Access Controls are required to be well implemented. Which of the following factor will not play any considerable role while defining Logical Access Controls for online LMS?
 - (a) Confidentiality and Authorization of User
 - (b) Virus prevention and detection to the LMS
 - (c) Controlled visitors' access to the library
 - (d) User training and tools for monitoring compliance
4. Let us assume that the IT Team members of KIO Ltd. runs a data backup software on online LMS of XYZ University on first Monday of every month to perform a complete backup of all the resource files containing audio, video and powerpoint files. On Tuesday, the backup software scans the backup selection and sends only new files and changes of existing files. You would now have a second version of the changed files and this process continues. Which type of data backup is this methodology referring to?
 - (a) Incremental Backup
 - (b) Differential Backup
 - (c) Full Backup
 - (d) Mirror Backup
5. After performing the standard selection criterion, the XYZ University selected KIO Ltd. for its proposed online LMS. Identify the statement that shall not have formed part of the contract between XYZ University and the vendor KIO Ltd.
 - (a) The description of the rights and responsibilities of both the parties.
 - (b) Assurances about software and data security.
 - (c) The programming languages used in the development of source code.
 - (d) Assurances for the performance.

6. The installation of water and smoke detectors, air-conditioners and fire extinguishers near the server room located in the campus of XYZ university are done to ensure that _____ controls are well implemented.
 - (a) Environmental
 - (b) Physical
 - (c) Managerial
 - (d) Application
7. Mr. A, the in-charge of IT team of KIO Ltd. is responsible for the maintenance of online LMS of XYZ University. While on duty, he receives an urgent call from his senior on his mobile phone and leaves his system unattended. Finding this an appropriate opportunity, a mischievous student Mr. X accesses Mr. A's computer system in his absence and downloads many resource files from e-learning pool of LMS and further shares some of these files in the public domain. Under which section of the IT Act, 2000; Mr. X will be held liable for his misdeed?
 - (a) Section 15
 - (b) Section 43
 - (c) Section 43A
 - (d) Section 45
8. The e-resource files are accessible to stakeholders of each affiliated college of XYZ university on pay-as-per-usage basis. Which type of Cloud Computing Service Model provides such facility?
 - (a) Platform as a Service
 - (b) Data as a Service
 - (c) Software as a Service
 - (d) Infrastructure as a Service

(8 x 2 = 16 Marks)

Question Nos. 9 to 22 carries 1 mark each.

9. Identify the statement that is not included in "Internal Control report of Management" which itself forms part of Company's Annual report.
 - (a) A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company.
 - (b) A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting.
 - (c) The assessment of effectiveness of the company's internal control that includes disclosure of any material weaknesses in the company's internal control over financial reporting identified by management.
 - (d) A statement that the registered private accounting firm that audited the financial statements included in the monthly report has issued an attestation report on management's assessment of the company's internal control over financial reporting.
10. It is a well-known fact the Explicit and Tacit are two broad types of knowledge. Identify the statement that does not hold true for Explicit knowledge and Tacit knowledge.
 - (a) Explicit knowledge is that which can be formalized easily and as a consequence is easily available across the organization.
 - (b) Tacit knowledge is unarticulated and represented as intuition, perspective, beliefs, and values that individuals form based on their experiences.
 - (c) Explicit knowledge is personal, experimental and context - specific.

- (d) Explicit knowledge is articulated, and represented as spoken words, written material and compiled data.
11. The access control mechanism of an Online application's boundary system allows only the authentic users to access authorized resources. This access control mechanism has three sequential steps_____, _____ and _____.
- (a) Identification, Authentication, Authorization
 - (b) Authentication, Documentation, Authorization
 - (c) Authorization, Authentication, Identification
 - (d) Identification, Authorization, Documentation
12. Which of the following statement is incorrect w.r.t Incremental Data Backup?
- (a) With Incremental backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup only.
 - (b) Incremental Backup restores are slower than a full backup and differential backup.
 - (c) The use of storage space in incremental backup is efficient as the files are not duplicated.
 - (d) Incremental backups are faster than Differential Backups.
13. After the Request for Proposals (RFPs) are received by an enterprise from various vendors, which of the following factor is not considered as a valid criterion for vendor's selection?
- (a) Presentation by the selected vendor
 - (b) Financial stability of the selected vendor
 - (c) Market feedback of the selected vendor
 - (d) Geographical location of the selected vendor
14. The Quality Assurance Management controls involve various functions that ensure that the development, implementation, operation and maintenance of information systems conform to quality standards. With such scope of the controls in mind, what do you think is not true about Quality Assurance Management Controls?
- (a) Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.
 - (b) Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.
 - (c) Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.
 - (d) Auditors check whether the organizations that have been audited have appropriate, high-quality disaster recovery plan in place or not.
15. The Section 69 of Information Technology Act, 2000 is related to _____.
- (a) Powers to issue directions for interception or monitoring or decryption of any information through any computer resource
 - (b) Preservation and Retention of information by intermediaries
 - (c) Power of the Controller to give directions
 - (d) Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

16. Every business decision is accompanied with a set of threats and so is BYOD program too. The risk exemplified and hidden in "Lack of Device Visibility" is related to _____ risk in which the IT practice team is unaware about the number of devices being connected to the network.
- (a) Network
 - (b) Device
 - (c) Application
 - (d) Implementation
17. While giving presentation on the topic COBIT 5, Mr. Ravi mentioned about specific process named MEA - Monitor, Evaluate and Assess and raised a query for the audience to identify the statement which does not fall under the purview of MEA.
- (a) To enable the management to identify management deficiencies and inefficiencies and to initiate improvement actions.
 - (b) To continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews.
 - (c) To evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.
 - (d) To plan, organize and maintain standards for internal control assessment and assurance activities.
18. Which of the following is not a characteristic of Computer Based Information Systems?
- (a) All systems work for predetermined objectives and the system is designed and developed accordingly.
 - (b) A system has number of non-related and independent subsystems or components. The subsystems can function in isolation and do not depend on other subsystems.
 - (c) If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
 - (d) The work done by individual subsystems is integrated to achieve the central goal of the system.
19. In order to identify the Systems maintenance needs on a timely basis, the management of a company establishes formal mechanisms to monitor the status of their operational programs. Which of the following does not fall under this scope of system maintenance?
- (a) Repair maintenance in which program errors are corrected.
 - (b) Adaptive maintenance in which program is modified to meet changing user requirements.
 - (c) Perfective maintenance in which the program is tuned to decrease the resource consumption.
 - (d) Adaptive maintenance in which the program is tuned to decrease the resource consumption.
20. Following are various data backup options in case any disaster occurs in an enterprise. Which of the following backup options is most expensive to be maintained because of its critical activities and minimum tolerance of downtime?
- (a) Cold Site
 - (b) Warm Site
 - (c) Hot Site
 - (d) Reciprocal Agreement

21. Mr. X is a member of System Development Team who visits his client company XYZ Ltd. frequently to interview its employees to gather the details regarding the drawbacks of the existing systems in the company XYZ Ltd. and understand their future requirements. Identify the role Mr. X is performing?
 - (a) Programmer
 - (b) Business Analyst
 - (c) Project Leader
 - (d) Project Manager
22. In an organization ABC Ltd.; the adherence of policies, procedures and standards as defined by the management are required to be followed. An accountant Mr. X, due to enmity, misused his access rights and made changes in the credit points earned by the salesperson Mr. A on every sale of his customer. During the audit, the auditor Mr. B suspected this discrepancy and preferred to embed an audit software module into the accountant Mr. X's host application software to determine the frequency with which the he had made the changes in the credit points of Mr. A. Which of the following audit tool is used by Mr. B in this case?
 - (a) Integrated Test Facility (ITF)
 - (b) System Control Audit Review File (SCARF)
 - (c) Snapshots
 - (d) Audit Hooks

Part II: DESCRIPTIVE QUESTIONS

Total Marks: 70 Marks

Question No. 1 is compulsory.

Attempt any four questions out of remaining five questions.

1. (a) We know that IT Governance refers to the system in which Directors of the enterprise evaluate, direct and monitor IT management to ensure the effectiveness, accountability and compliance of IT. ABC Ltd. claims to have well implemented and achieved the benefits of IT Governance in its enterprise. As an auditor of ABC Ltd., mention the key practices that you may adopt to determine the status of IT Governance in the enterprise. Also, enlist the benefits that you think are reaped by ABC Ltd. through the implementation of IT Governance. **(6 Marks)**
 - (b) Environmental exposures to various Information resources are primarily due to fire damage, power spikes, water damage etc. and can be reduced with the help of environmental controls. From the perspective of environmental exposures and controls, determine various categories of Information Systems resources. **(5 Marks)**
 - (c) The effectiveness of an Information System's controls is evaluated through an Information Systems Audit. Explain the term "Information Systems Audit". **(3 Marks)**
2. (a) Existence of an audit trail is a key financial audit requirement; since without an audit trail, the auditor may have extreme difficulty in gathering sufficient, appropriate audit evidences to validate the figures in the client's accounts. However, there are many concerns that are involved in the performance of evidence collection and understanding the reliability of controls. Discuss them. **(6 Marks)**
 - (b) While developing the Business Continuity Management (BCM), discuss the competencies that are necessary for an employee to acquire so that (s)he be assigned specific management responsibilities within the system. **(5 Marks)**
 - (c) Recognize the impact of cyber frauds on enterprises. **(3 Marks)**

3. (a) A System which is defined as a group of interconnected components and working towards the accomplishment of a common goal; are classified based on various parameters like elements, interactive behaviour, degree of human intervention and working output. Define all these systems in brief. **(6 Marks)**
- (b) Consider yourself to be an auditor of ABC Ltd. organization. You have to play a major role in evaluating the performance of various controls implemented under Managerial Controls in the organization. Discuss how will you assess the activities of Planning, Organizing, Leading and Controlling performed by the senior management. **(5 Marks)**
- (c) State various steps that enterprises need to take to ensure the compliance with cyber laws. **(3 Marks)**
4. (a) Cloud Computing has become a rapidly evolving technology in the world today. However, in spite of its many benefits, it has many security and implementation issues. Discuss the major issues related to the implementation of Cloud Computing. **(6 Marks)**
- (b) The data that is presented to an application as input data must be validated for accuracy and completeness before the data and instruction being input into an application system. Identify the controls responsible to do so and explain them. **(5 Marks)**
- (c) Explain the advantages of Business continuity to an enterprise. **(3 Marks)**
5. (a) If in case Mr. Mohan intentionally makes available Mr. Suman's electronic Signature to his competitors; under which Section of Information Technology Act, 2000 is Mr. Mohan be held guilty. Also discuss the said Section in detail. **(6 Marks)**
- (b) The Planning phase is considered as one of the primary and important phases in an Information System Audit which ensures that the audit is performed in an effective manner. Discuss the important points that are considered in the Planning phase. **(5 Marks)**
- (c) Differentiate between Black Box Testing and White Box Testing. **(3 Marks)**
6. (a) An enterprise XYZ is in the process of deployment or implementation of the requisite new system in its real operating environment. The implementation of this system would involve several activities. Discuss them in detail. **(6 Marks)**
- (b) The Enterprise Governance constitutes the entire accountability framework of an organization as it involves establishing accountability for decision-making. The enterprise Governance has two dimensions – Corporate Governance and Business Governance. Discuss them. **(5 Marks)**
- (c) Identify the Section of Information Technology Act, 2000 that describes the punishment for cyber terrorism. Describe the Section also. **(3 Marks)**