

MOCK TEST PAPER II
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

KHELKOOD Ltd. is one of the largest manufacturers as well as exporter of sports equipment in India and has been maintaining an e-commerce portal for selling its products online. The management does not want to earn a bad reputation in the industry and in this line has decided to put into place certain Logical and Physical Access controls to restrict system access to authorised users, wherein employees having access rights only to information they need to do their jobs and prevent them from accessing information which doesn't pertain to them, and in-turn help the organization secure desirable results. To this, the company has well implemented Physical Identification mechanism wherein a secret number has been assigned to each authorised individual to authorize him/her to access the server rooms.

Even though proper Access Controls have been defined and well implemented, an internal auditor of the company Mr. B, highlighted before the Audit Committee the technical difficulties in reconciling the amounts of sales received through various payment gateways available at its e-commerce website.

In response to investigate the potential fraud involved, the Directors of the company engaged an independent auditing firm ABC Ltd. to identify the gaps in the payment gateway. The summary inspection report submitted by ABC Ltd. identified that Mr. A was an authorised user who facilitated a hacker Mr. Z with unauthorized access to payment gateway of KHELKOOD Ltd. Mr. Z carried out a fraud related to slicing of small amounts of money from every computerized transaction done through the portal. Apart from other actions undertaken, the management has resolved to book Mr. A and Mr. Z for dishonesty and fraud under the provisions 43 and 66 of the Information Technology Act, 2000. Learning a lesson from this experience, the company further initiated the process of adopting Enterprise Risk Management (ERM) tools to mitigate possible risks that could prevent the company from operating in most effective manner and at the same time acts disruptive to other business processes.

Based on the above scenario, answer the Multiple-Choice Question No(s) 1 to 4.

1. Referring to the case, identify the activity that stands outside the purview of Mr. B while auditing the physical access mechanism of the company?
 - (a) Risk Management
 - (b) Risk Assessment
 - (c) Controls Assessment
 - (d) Review of Documents
2. Referring to the summary inspection report provided by ABC Ltd., which technical exposure has the hacker Mr. Z been involved in?
 - (a) Data Diddling

- (b) Salami Technique
 - (c) Rounding Down
 - (d) Trap Doors
3. What is the maximum punishment for which the hacker Mr. Z can be booked under the IT Act, 2000?
- (a) Imprisonment for a term which may extend to 5 years or with a fine which may extend to 3 lakhs or with both.
 - (b) Imprisonment for a term which may extend to 5 years or with a fine equal to damages incurred or with both.
 - (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.
 - (d) Imprisonment for a term which may extend to 3 years or with a fine equal to damages incurred or with both.
4. With owning an e-commerce website, the company KHELKWOOD Ltd. has been benefited in terms of various factors as mentioned below except one. Identify it.
- (a) Unlimited marketplace
 - (b) Efficient business relationships
 - (c) Easy maintenance of storage warehouse
 - (d) Lower cost of doing business

The Question No.(s) 5 to 8 are independent questions carrying weightage of 2 mark each.

5. An undergraduate student gets a question during his examination wherein he is supposed to categorize the below mentioned examples under the titles Vulnerability, Exposure and Risk.
- (i) Leaving the front door unlocked.
 - (ii) Opting for short passwords.
 - (iii) Loss of reputation.
 - (iv) Leakage of corporate information.
- What do you think shall be his choice in case he has to pick the correct set of statements?
- (a) (i) – Vulnerability, (ii) – Vulnerability, (iii) – Exposure, (iv) – Risk
 - (b) (i) – Risk, (ii) – Vulnerability, (iii) – Exposure, (iv) - Risk
 - (c) (i) – Risk, (ii) – Vulnerability, (iii) – Risk, (iv) - Exposure
 - (d) (i) – Exposure, (ii) – Vulnerability, (iii) – Risk, (iv) - Exposure
6. During System Designing phase of the Systems Development Life Cycle (SDLC), following activities are carried out:
- (i) Deals with the organization of applications in terms of hierarchy of modules and sub-modules.
 - (ii) Determine the ways in which users will interact with a system.
 - (iii) The logical design is transformed into unit which can further be decomposed into implementation units such as programs and modules.
 - (iv) Determining the scope ranging from local to global structure.

The sub-activities can be categorized under the following titles:

- (A) Design of database
- (B) Physical Design
- (C) User interface Design
- (D) Architectural Design

Identify the correct match set.

- (a) (i) – (C), (ii) – (A), (iii) – (B), (iv) – (D)
 - (b) (i) – (D), (ii) – (B), (iii) – (A), (iv) – (C)
 - (c) (i) – (D), (ii) – (C), (iii) – (B), (iv) – (A)
 - (d) (i) – (A), (ii) – (C), (iii) – (D), (iv) – (B)
7. The Information Technology Act, 2000 has been enacted with the following objectives except one. Identify it.
- (a) To facilitate electronic storage of data.
 - (b) To facilitate electronic filing of documents with Government departments.
 - (c) To give legal recognition for keeping of books of accounts by banker's in electronic form.
 - (d) To ensure the independence of Information Systems' Auditors.
8. In Network as a Service (NaaS) instance of Infrastructure as a Service (IaaS) Model of Cloud Computing, which of the following does not fall under its purview?
- (a) To create virtual networks.
 - (b) To provide the virtual storage for the data.
 - (c) To deploy custom routing protocols.
 - (d) To create virtual routers and protocols.

(8 x 2 = 16 Marks)

Question No(s). 9 to 22 carries 1 mark each.

9. COBIT 5 Process Reference Model includes a total of 37 Governance and Management processes as mentioned below:
- (i) Governance Processes (EDM01 to EDM05)
 - (ii) Management Processes (APO01 to APO15)
 - (iii) Management Processes (BAI01 to BAI10)
 - (iv) Management Processes (MEA01 to MEA04)
 - (v) Management Processes (DSS01 to DSS07)
 - (vi) Governance Processes (BAI01 to BAI10)
- Identify the incorrect set of statements.
- (a) (ii), (iv), (v), (vi)
 - (b) (i), (ii), (iii), (vi)
 - (c) (ii), (iii), (iv), (v)
 - (d) (ii), (iii), (iv), (vi)

10. Consider the following statements on classification of Information Systems.
- (i) Open Systems interact with other systems in its environment.
 - (ii) A software that performs on a set of instructions is a Deterministic System.
 - (iii) Random arrangement of independent ideas or constructs is referred as Abstract System.
 - (iv) Automated systems are probabilistic systems in terms of probable behaviour.
 - (v) The watch is an example of Open System.
- Identify the incorrect set of statement(s).
- (a) (iii), (iv), (v)
 - (b) (i), (ii), (iv)
 - (c) (i), (iii), (v)
 - (d) (ii), (iv), (v)
11. The Information Systems' Controls are classified as under:
- (i) Preventive
 - (ii) Detective
 - (iii) Corrective
- The characteristics of these controls are as follows:
- (A) Minimizing the impact of the threat.
 - (B) Understanding the possible threats.
 - (C) Correcting the error arising from a problem.
 - (D) Reporting an unlawful activity.
- Match the characteristics with their corresponding controls and choose the correct option:
- (a) (A) – (i), (B) – (ii), (C) – (iii), (D) – (i)
 - (b) (B) – (i), (C) – (ii), (A) – (iii), (D) – (ii)
 - (c) (B) – (i), (D) – (ii), (A) – (iii), (C) – (iii)
 - (d) (C) – (i), (A) – (ii), (B) – (iii), (D) – (i)
12. Which of the following statement is correct about Differential Backups?
- (a) The restores in Differential Backups are slower than Incremental backups.
 - (b) Differential Backups have efficient use of storage space than full backups.
 - (c) Differential Backups capture files that are created or changed since the last backup, regardless of backup type.
 - (d) Comparing with Full backup, Differential backups are slower in processing.
13. Sometimes post-implementation of a new information system, the company proposes to carry out certain evaluations to assess the efficacy of all the elements of the new system to see if further improvements are required to be carried out to optimize the benefit delivered. Which of the following activity does not belong to post-implementation review process?
- (a) Evaluation of the development process primarily concerned with whether the system was developed on schedule and within budget.
 - (b) Evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties.

- (c) Evaluation of information system against legal feasibility to check for the violation of local legal requirements and applicable statutes.
 - (d) Evaluation of the information system in terms of information it provides or generates.
14. Following are the various categories of Information Systems Audit.
- (i) Systems and Application
 - (ii) Information Processing Facilities
 - (iii) Systems Development
 - (iv) Management of IT and Enterprise Architecture
 - (v) Telecommunications, Intranets and Extranets
- The descriptions of these audits are provided below:
- (A) To verify that the processing facility is controlled.
 - (B) To verify that the controls are in place in the client, server, and communication lines.
 - (C) To verify that the systems under development meet organization's objectives.
 - (D) To verify that the systems and applications are appropriate, efficient, and adequately controlled.
 - (E) To verify that IT management has developed an organizational structure and procedures.
- Match the audit with its description and choose the correct set:
- (a) (i)-(A),(ii)-(D),(iii)-(B),(iv)-(E),(v)-(C)
 - (b) (i)-(E),(ii)-(D),(iii)-(C),(iv)-(B),(v)-(A)
 - (c) (i)-(E),(ii)-(C),(iii)-(D),(iv)-(B),(v)-(A)
 - (d) (i)-(D),(ii)-(A),(iii)-(C),(iv)-(E),(v)-(B)
15. Under Information Technology Act, 2000, _____ means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.
- (a) Private Key
 - (b) Public Key
 - (c) Cryptography Key
 - (d) Security Key
16. In case a company outsources or creates application with one Cloud computing vendor and the company finds it difficult to change it to another Cloud computing vendor, which problem is this condition referring to?
- (a) Interoperability
 - (b) Threshold Policy
 - (c) Software Isolation
 - (d) Incident Response
17. Which of the following Section of Information Technology Act, 2000 has been declared as unconstitutional by Supreme Court?
- (a) Section 66B
 - (b) Section 66C
 - (c) Section 66A
 - (d) Section 66F

18. Identify the incorrect statement about the Public Cloud in Cloud Computing.
 - (a) There is no limit for the number of users in Public Cloud.
 - (b) Public Cloud is considered to be highly scalable.
 - (c) Public Cloud follows loose Service Level Agreements (SLAs).
 - (d) The public cloud is offered to the users on a pay-as-you-go basis.
19. Which of the following is not an example of Information Technology General Controls (ITGC)?
 - (a) System Development Life Cycle Controls
 - (b) Data Centre Physical Security Controls
 - (c) Computer operation Controls
 - (d) Supervisor review and sign-off of a document
20. The different phases of developing a Business Continuity Plan in an enterprise are as follows:
 - (i) Testing Program
 - (ii) Business Impact Analysis
 - (iii) Maintenance Program
 - (iv) Initial Plan Testing and Plan Implementation
 - (v) Plan development
 - (vi) Pre-planning Activities
 - (vii) Vulnerability assessment and general definition of requirements
 - (viii) Detailed definition of requirements

Choose the correct set showing the sequential order of aforementioned phases.

 - (a) (vi), (vii), (ii), (viii), (v), (i), (iii), (iv)
 - (b) (i), (ii), (vii), (viii), (v), (vi), (iii), (iv)
 - (c) (ii), (iii), (iv), (vi), (v), (i), (vii), (viii)
 - (d) (i), (iii), (v), (vii), (ii), (iv), (vi), (viii)
21. Which of the following statement is not true about Data Dictionary.
 - (a) Data Dictionary is a computer file about data.
 - (b) A Data Dictionary can help to establish audit trails required by auditors and accountants.
 - (c) Each computer record of a data dictionary contains information about a single data item used in a business information system.
 - (d) Data Dictionary is commonly used in operations research, specifically in decision analysis to help identify the best strategy.
22. Various Controls as mentioned below can be categorized into either Information Systems Managerial Controls or Information Systems Application Controls.
 - (i) Managerial Controls - System Development Management Controls
 - (ii) Application Controls - Security Management Controls
 - (iii) Managerial Controls - Operations Management Control
 - (iv) Application Controls - Output Controls
 - (v) Application Controls - Security Management Controls

Identify the incorrect set of statements.

- (a) (ii), (iv)
- (b) (ii), (v)
- (c) (iii), (iv)
- (d) (i), (iii)

(14 x 1 = 14 marks)

Part II: DESCRIPTIVE QUESTIONS

Total Marks: 70 Marks

Question No. 1 is compulsory.

Attempt any four questions out of remaining five questions.

1. (a) The IT Steering Committee in an enterprise is led by a member of Board of Directors and comprises of functional heads from all the key departments of the enterprise including audit and IT department. Discuss the key functions that are performed by the IT Steering Committee. (6 Marks)
- (b) As an internal auditor of ABC Ltd., you are deputed as a part of the SDLC Team so as to suggest them various Logical Access Controls that are required to be implemented in order to safeguard the company's Application and Monitoring System. What shall be the probable suggestions? (5 Marks)
- (c) Discuss the role of Information Systems Auditor in reviewing the Physical Access Controls in an organization. (3 Marks)
2. (a) Information Systems (IS) Auditing is related to risks, controls, and assurance. Identify various factors that are crucial for an enterprise to decide the need of Information Systems Auditing. (6 Marks)
- (b) If an organization XYZ deploys a third-party site KH Ltd. for its backup and recovery purposes, describe several issues that are required to be covered in the contract by security administrators of both the parties – XYZ and KH Ltd. (5 Marks)
- (c) Two types of error named Transcription and Transposition can corrupt a data code and cause processing errors. Differentiate between these errors with examples. (3 Marks)
3. (a) Different Information Systems perform numerous operational and managerial support roles in businesses and cater to varied groups of people. Discuss different types of Information Systems and the group of people they serve. (6 Marks)
- (b) Define Audit Trail and its objectives in brief. (5 Marks)
- (c) Elaborate the key issues that are related to electronic information that may impact an enterprise or an auditor. (3 Marks)
4. (a) Differentiate between On-premise Private Cloud and Outsourced Private Cloud. (6 Marks)
- (b) The major controls of the boundary system are the access control mechanisms that link the authentic users to authorized resources, they are permitted to access. To enable so, various Boundary Control Techniques are adopted. Describe these techniques. (5 Marks)
- (c) Write a short note on Business Impact Assessment (BIA). (3 Marks)

5. (a) Identify and define the act of Information Technology Act, 2000 that defines Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security. **(6 Marks)**
- (b) The process of continuous auditing enables auditors to shift their focus from the “Traditional transaction audit” to the “System and Operations audit”. Discuss in brief various techniques used for the purpose of continuous auditing and their advantages. **(5 Marks)**
- (c) From the perspective of an Information Systems Auditor, state various advantages of System Development Life Cycle (SDLC) methodology. **(3 Marks)**
6. (a) A System Analyst plays a vital role in the System Designing phase of Systems Development Life Cycle (SDLC). Discuss various factors which s/he should consider while designing user input/output forms of the proposed system. **(6 Marks)**
- (b) Describe various components of COBIT 5. **(5 Marks)**
- (c) Mobile Computing is a versatile technology that provides numerous tangible benefits. Discuss them. **(3 Marks)**