MOCK TEST PAPER 1

FINAL COURSE (OLD) GROUP - II

PAPER - 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Time Allowed: 3 Hours   Maximum Marks: 100 Marks

Division A: MULTIPLE CHOICE QUESTIONS

Total Marks: 30 Marks

Question Nos. 1 to 8 carries 2 marks each.

1. XYZ Bank has implemented Core Banking Solution (CBS) in all its branches. Since the Password policy is not implemented properly, users can keep short length login passwords for CBS access. This refers to _____ under Information Systems concepts.

    (a) Threat

    (b) Exposure

    (c) Vulnerability

    (d) Attack

2. Meteorological Department declares prediction of rains in the month of May based on which farmers decide to sow seeds in their fields. If the prediction goes wrong, farmers face severe problems of re-sowing seeds. Which characteristic of the information is failed here?

    (a) Confidentiality

    (b) Integrity

    (c) Availability

    (d) Reliability

3. XYZ Bank has implemented a strict password policy where by every user has minimum 8 characters' alpha-numeric login password and that password must be reset after 30 days to get access to Core Banking Solution (CBS). As per classification of IS Controls, which type of control is this?

    (a) Preventative Control

    (b) Detective Control

    (c) Corrective Control

    (d) Compensatory Control

4. ABC Ltd. carries out Fire drills in its company every 6 months whereby fire like situation is simulated and the preparedness of its organisation and its personnel for facing disaster is verified. This is ____ under the Business Continuity Management.

    (a) Emergency Plan

    (b) Test Plan

    (c) Back-up Plan

    (d) Recovery Plan

1

5. PQR Ltd. is a software development company. One of its employee, Mr. Rajesh has the responsibility to interact with users of the computer system and understand their requirements from the system. Which role is performed by Mr. Rajesh in the company?

   (a) Project Manager

   (b) Project Leader

   (c) Business Analyst

   (d) Programmer

6. ABC Company implemented ERP in its organization. The Sales Team requested IT Team to provide them access to Accounts / Finance Module which was denied by the IT Team. Which of the Application Security control was tested here?

   (a) Confidentiality

   (b) Integrity

   (c) Availability

   (d) Timeliness

7. PQR Ltd. is a Business Process Outsourcing (BPO) managing the health records for a renowned hospital in Mumbai. It was observed that one of the employee Mr. X of PQR Ltd. was sharing the confidential health records of the patients with an Insurance Company. Who will be held responsible under the IT Act for this offence?

   (a) Only Mr. X who was sharing records

   (b) Mr. X and Directors

   (c) Mr. X, Directors and Shareholders

   (d) Only Directors

8. ABC Ltd. is engaged in providing Data Processing services. It has received a big contract from an insurance company for its policy processing. ABC Ltd. has limited PCs at their office, so it approached Amazon Web Services to provide them access to Virtual Machines for data processing. ABC Ltd. is using which Cloud Computing Service Model?

   (a) Software as a Service (SaaS)

   (b) Platform as a Service (PaaS)

   (c) Infrastructure as a Service (IaaS)

   (d) Network as a Service (NaaS)   *(8 x 2 = 16 Marks)*

Question Nos. 9 to 22 carries 1 mark each.

9. Which of the following statement is incorrect?

   (a) IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

   (b) The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management.

   (c) The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises.

2

(d) The Project Manager should work independently from the Steering Committee in finalizing the detailed work plan and developing interview schedules.

10. In an organization, the Top management generally comprises of _____.

(a) owners/shareholders, Board of Directors, its chairman, managing director, or the chief executive

(b) heads of functions departments like purchase manager, production manager and marketing managers

(c) marketing managers, financial controller, and divisional sectional officers working under functional heads

(d) superintendents and supervisors

11. An Information Security policy addresses many issues that may involve the following:

(i) confidentiality, integrity and availability concerns

(ii) who may access what information and in what manner based on which access decision is made

(iii) maximized sharing versus least privilege and separation of duties

(iv) programming new system, maintaining old systems and providing general support software.

(a) (i), (ii), (iii)

(b) (i), (ii), (iv)

(c) (ii), (iii), (iv)

(d) (i), (ii), (iii), (iv)

12. Which of the following statement is incorrect?

(a) A Full Backup captures all files on the disk or within the folder selected for backup.

(b) The Mirror backup is clean and does not contain old and obsolete files.

(c) With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.

(d) Incremental Backup consumes the most storage space as compared to full and differential backups.

13. Which of the following activity is not involved in Database Designing during System Designing phase of System Development Life Cycle (SDLC)?

(a) Storage Structure Design

(b) Cost Analysis

(c) Physical Layout Design

(d) Conceptual Modeling

14. The audit trail of _____ maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

(a) Database Controls

(b) Output Controls

(c) Processing Controls

(d) Communication Controls

3

15. In Information Technology Act 2000; _____ is defined as a person in whose name the Electronic Signature Certificate is issued.

    (a) Controller

    (b) Intermediary

    (c) Originator

    (d) Subscriber

16. Which of the following issue is not related to security in Mobile Computing?

    (a) Confidentiality

    (b) Integrity

    (c) Bandwidth

    (d) Accountability

17. In Information Systems; an action, device, procedure, technique or other measure that reduces the vulnerability of a component in it is referred as _____.

    (a) Residual Risk

    (b) Counter Measure

    (c) Risk Management

    (d) Threat

18. Which of the following activity is not involved in Office Automation Systems (OAS)?

    (a) Document Creation

    (b) Filling, Search, Retrieval and Follow up

    (c) Receipts and Distribution

    (d) Decision Making

19. Which of the following is not a type of Application Control under controls based on Audit functions?

    (a) Boundary

    (b) Input

    (c) Security Administration

    (d) Output

20. Which of the following document is not classified as being part of the Business Continuity Management System?

    (a) The Risk Assessment Report

    (b) The Business Impact Analysis report

    (c) Local Authority Risk Register

    (d) Performance Analysis Report

21. Under which dimension, the Feasibility Study under System Development Life Cycle (SDLC) is not evaluated?

    (a) Technical

    (b) Legal

(c) Operational

(d) Incremental

22. Which of the following is not an example of Information Systems Audit Tool?

(a) Flowchart

(b) System Control Audit Review File (SCARF)

(c) Integrated Test Facility (ITF)

(d) Continuous and Intermittent Simulation (CIS)   *(14 x 1 = 14 Marks)*

Division B: DESCRIPTIVE QUESTIONS

Total Marks: 70 Marks

Question No. 1 is compulsory.

Attempt any four questions out of remaining five questions.

1. (a) There exists ISACA's globally accepted framework which is defined as a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies; and helps these enterprises to create optimal value from their information and technology. Identify the standard and discuss its components.   *(6 Marks)*

(b) An organization intends to adopt various methods to protect its hardware installations in its premises against fire damage. Describe major ways using which this objective can be achieved.

(5 Marks)

(c) "The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor". Prepare a list of the skill-set generally expected to have acquired by an IS auditor.   *(3 Marks)*

2. (a) Application security audit uses the Layered approach which is based on the activities being undertaken at various levels of management namely Operational, Tactical and Strategic. Discuss in brief various audit issues related to these layers.   *(6 Marks)*

(b) Discuss various processes that are mapped in Business Continuity Management (BCM).

(5 Marks)

(c) An IS auditor is responsible to evaluate certain factors while reviewing the adequacy of data security controls. List them.   *(3 Marks)*

3. (a) Because of the global competition, enterprises are always in greater need of efficient and timely provision of information to enhance the ability to make decisions based on relevant information. Determine the attributes of any useful and effective information.   *(6 Marks)*

(b) What do we understand by the term Audit Trail? Discuss Accounting and Operations Audit Trails w.r.t Processing Controls under Application Controls.   *(5 Marks)*

(c) What activities are required to be performed by the management of an organization wanting to adopt ISO 27001?   *(3 Marks)*

4. (a) In Cloud Computing, there is a cloud that is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. Identify the type of the cloud and prepare list of its characteristics and advantages.

(6 Marks)

5

(b) Source Document Controls are one of the type of Input Controls that are used to limit source document related frauds. Discuss various control procedures that should be put in place to account for each such source document. **(5 Marks)**

(c) Discuss about Business Continuity Planning (BCP) Manual. **(3 Marks)**

5. (a) A company ABC Ltd., communicated through email to competent manufacturer of garments, its willingness to purchase the dress material for the stitching of the uniforms of the staff constituting of 1000 people. The company invited the quotation of price for supply of dress material. X manufacturer offered the dress material @ Rs. 500 per meter within 2 months from the date of order. ABC Ltd. accepted the said offer via e-mail. In the meantime, M/s PRQ from an insider, came to know of the requirement of the ABC Ltd. With respect to the same, they through mail contacted the company with a proposal to supply the stitched uniforms with dress material @ Rs. 500.

ABC Ltd. accepted their proposal and revoked the agreement made with X manufacturer and communicated it through mail. X manufacturer filed a suit for the claim of the loss borne due to refusal of the agreement. ABC Ltd. took the plea that no formal agreement was entered and it was a communication mail between them and thus not giving rise to any legal obligations.

In the light of the given facts, examine the following legal position as per the IT Act, 2000-

(i) Validity of acceptance of offer by ABC Ltd. with X manufacturer as to the supply of dress material for the making of staff uniform.

(ii) Whether the contention of the ABC Ltd. that no formal agreement was entered between them, is acceptable?

(iii) Nature of the contract entered between ABC Ltd. and the M/s PRQ and its liability towards X manufacturer. **(2 x 3 = 6 Marks)**

(b) Continuous auditing enables auditors to shift their focus from the traditional "transaction" audit to the "system and operations" audit. Discuss its benefits. **(5 Marks)**

(c) The Waterfall model under System Development Methodology has major strengths due to which it is quite popular and handy among the fraternity. Discuss them. **(3 Marks)**

6. (a) Detailed investigation of the present system should be carried out by qualified persons and experts to fully understand the present system and its related problems. Determine the areas on which the detailed analysis should be done before the system analysis of the proposed system.

(6 Marks)

(b) Discuss the term "Information Technology (IT) Governance" and its benefits. **(5 Marks)**

(c) What are the requirements of Insurance Regulatory and Development Authority of India (IRDA) for System Controls? **(3 Marks)**