MOCK TEST PAPER 1

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 4 are based on case scenario whereas Question nos. 5 to 8 are independent questions. Each question carries 2 marks.

Healthcare is an area where any nation's Government must invest as the growth of any nation is directly related to health of its population. With the growing population, the demand in the Indian healthcare industry has drastically changed in terms of IT requirements of hospitals also. The challenges existing within the current healthcare system must be catered to. In current situation, some challenges are insufficient good quality care mainly in rural areas; lack of equipped health centers with specialized doctors, nurses and infrastructure like beds, equipment and diagnostic labs; manual processing of patient's records and appointments; non-availability of medicines and treatment etc. Under this situation, automation is the only solution that makes processing in hospitals hassles free to maintain and monitor the quality of medical services in a holistic manner. The automation comes with a challenge to secure the sensitive information of the patients undergoing treatment in a hospital.

Owing to the facts of the 'health industry, one of the reputed hospital named ABC Hospital, having a network of five hospitals under it in Delhi/NCR, has well implemented the automation of its business processes. All the hospitals use a user-friendly ERP package named "SafeHealthWiz" and are well connected with each other using a central database.

1. Due to security breach, the database of all the patients of ABC hospital got available in public domain. Under which section of IT Act, 2000; the hospital is bound to compensate for the failure to protect the critical details of its patients.

    (a) Section 43

    (b) Section 43A

    (c) Section 44

    (d) Section 45

2. All the five branches of hospital in Delhi/NCR are interconnected to each other with a central database. The patients may visit any of these five branches with no hassle to carry their past prescription. Using technology, the complete medical history of the patient is available in any of these branches of the hospital. What do you think is the technology behind such a concept?

    (a) Cloud Computing

    (b) Bring Your Own Device

    (c) Grid Computing

    (d) Mobile Computing

1

3. During the Data Backup process from Central Server, an IT supervisor noticed that many invoices from Faridabad branch of ABC hospital involved slicing of small amounts of money from a computerized transaction or account. Which type of technical exposure does it refer to?

   (a) Data Diddling

   (b) Salami Technique

   (c) Bomb

   (d) Worm

4. The management of the ABC hospital entered into a contract where they hired a third party for the backup and recovery process for each of its branch. The IT security administrator must ensure that the following is incorporated in the contract except _____.

   (a) The conditions under which the site can be used.

   (b) The facilities and services the site provider agrees to make available.

   (c) How soon the site will be made available subsequent to a disaster.

   (d) The frequency for which the site provider agrees to make itself available for a particular time period.

5. The students of an institute are usually required to create documents like charts, graphs, handouts; preparing documents, dictation and editing of texts etc. Which of the following Information System is suitable for carrying out these tasks?

   (a) Transaction Processing System

   (b) Office Automation System

   (c) Management Information System

   (d) Decision Support System

6. Though Mr. X, an accountant is involved in the system development work; which of the following is not an expected skillset to be acquired by the accountant in order to perform his duties?

   (a) Expert in Book-keeping

   (b) Understanding of the business objectives

   (c) Understanding of system development methodologies

   (d) Conducting cost-benefit analysis

7. Which of the following statements are not correct w.r.t. Management and its levels?

   (a) Senior management is responsible for strategic planning and objectives, thus setting the course in the lines of business that the company will pursue.

   (b) The numbers of management levels are fixed to three irrespective of its size and structure.

   (c) Middle management develops the tactical plans, activities and functions that accomplish the strategic objectives.

   (d) Supervisory management oversees and controls the daily activities and functions of the tactical plan.

8. The key management practices involved in the implementation of Risk Management in an enterprise is as follows:

   (i) Analyze Risk

   (ii) Articulate Risk

(iii) Respond to Risk

(iv) Collect Data

(v) Maintain a Risk Profile

(vi) Define a Risk Management Action Portfolio

Choose the correct sequence for the implementation of these practices.

(a) (i)-(iii)-(v)-(ii)-(iv)-(vi)

(b) (iv)-(i)-(v)-(ii)-(vi)-(iii)

(c) (i)-(ii)-(iii)-(iv)-(v)-(vi)

(d) (i)-(iv)-(vi)-(iii)-(v)-(ii)   **(8 x 2 = 16 Marks)**

Question Nos. 9 to 22 carries 1 mark each.

9. Which of the following is not an Enterprise's management practice required aligning IT Strategy with Enterprise Strategy?

(a) Defining the target IT Capabilities

(b) Assessing the current environment, capabilities and performance

(c) Communicating the IT strategy and Direction

(d) Mitigating the risk

10. In an interview, a candidate was asked to mention about all components of Enterprise Resource Planning (ERP) Model that can be implemented through a methodology. Identify the correct answer that may be given by the candidate.

(a) Software Component, Process Flow, Customer mindset, Change Management

(b) Software Component, Process Flow, Business applications, Change Management

(c) Software Component, Process Flow, Customer mindset, Hardware component

(d) Software Component, Process Flow, Business applications, Hardware component

11. Identify the correct statement out of the following:

(a) To have a proper backup procedure in an enterprise is a best example of Preventive Control.

(b) Logical Access Controls are related to logical security of the tangible Information resources and intangible resources stored on tangible media etc.

(c) Piggybacking is defined as an act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions.

(d) An internetwork device Bridge connects heterogeneous Local Area Networks (LANs).

12. Which of the following statement is incorrect w.r.t Differential Backup?

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

(b) Differential backup is faster and more economical in using the backup space.

(c) Differential backups are faster than Incremental backups.

(d) With Mirror backups, when a file that is deleted, that file is eventually also deleted in the mirror backup.

3

13. In an organization, as most of the Information Systems require some modification after development; the System Maintenance phase becomes one of an important aspect of SDLC. There are different categories of Maintenance which are Scheduled, Adaptive, Corrective, Rescue, Preventive and Perfective. Which of the following statement is not correct about these categories of Maintenance?

    (a) Scheduled Maintenance is planned to ensure operational continuity and avoid of anticipated risks.

    (b) Rescue Maintenance deals with the undetected malfunctions that require immediate troubleshooting solution.

    (c) Adaptive Maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system.

    (d) Corrective Maintenance deals with fixing bugs in the code or defects found during the executions.

14. Which of the following statement is incorrect w.r.t Auditing of Information Systems?

    (a) The Planning Phase in IS Audit ensures that the audit of performed in an effective manner.

    (b) The IS Audit process evaluates the adequacy of internal controls regarding both specific computer program and the data processing environment.

    (c) The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks.

    (d) According to SA-234, Audit Documentation refers to the record of audit procedures performed, relevant audit obtained and conclusions the auditor reached.

15. Which of the following definition is incorrect in purview of Information Technology Act, 2000?

    (a) Electronic Form with reference to Information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.

    (b) Addressee means a person including intermediary who is intended by the originator to receive the electronic record.

    (c) Cyber Cafe means any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.

    (d) Asymmetric Crypto System means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

16. Below are the facts related to Community Cloud however, there is one statement which is incorrect? Identify that statement.

    (a) As the complete cloud is being shared by several organizations or community, it becomes highly expensive.

    (b) Community Cloud is suitable for organizations that cannot afford a private cloud and cannot rely on the cloud either.

    (c) Community Cloud has better security then Public Cloud.

    (d) The cloud is distributive, and no single company has full control over the whole cloud.

17. Which of the following statement is incorrect?

    (a) Every enterprise regardless of its size needs to have an internal control system built into its enterprise structure.

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

4

(c) Vulnerabilities of software can originate from the flaws on the software's design, defects in its implementation, or problems in its operation.

(d) The GRC framework which has been a regulatory requirement not only for listed enterprises but also for all types of enterprises stands for Governance, Risk and Control.

18. Which of the following statement is not correct about Management Information Systems (MIS)?

(a) An MIS usually takes 1 to 3 years and sometimes even longer period to get established firmly within a company.

(b) MIS cannot be implemented without using a computer.

(c) An MIS is integrated that takes a comprehensive view or a complete look at the interlocking subsystems that operate within a company.

(d) An MIS can be broken down into meaningful subsystems that set the stage for the phasing plan.

19. Which of the following statement is incorrect w.r.t. various controls implemented in an enterprise/organization?

(a) The surprise check of raw materials stock by a supervisor in a manufacturing company is an example of Corrective Control.

(b) The Contingency Planning done by an enterprise is an example of Corrective Control.

(c) Firewalls are installed in an organization as a part of Preventive Control.

(d) Duplicate checking of calculations in financial transactions of an enterprise is an example of Detective Control.

20. In the Business Impact Analysis (BIA) Matrix also known as Risk Assessment Matrix; risks are placed on the matrix based on the following two criterions:

(a) Likelihood, Vulnerability

(b) Vulnerability, Consequences

(c) Likelihood, Consequences

(d) Vulnerability, Threat

21. During System Testing in Systems Development Life Cycle (SDLC), the software and other system elements are tested as a whole. Which of the following is not type of System Testing?

(a) Security Testing

(b) Performance Testing

(c) Recovery Testing

(d) Alpha Testing

22. Which of the following is the correct sequence of steps involved in Information System Audit?

(a) Scoping, Planning, Reporting, Close, Fieldwork, Analysis

(b) Analysis, Planning, Reporting, Scoping, Fieldwork, Close

(c) Planning, Scoping, Analysis, Reporting, Fieldwork, Close

(d) Scoping, Planning, Fieldwork, Analysis, Reporting, Close **(14 x 1 = 14 Marks)**

5

Total Marks: 70 Marks

Question No. 1 is compulsory.

Attempt any four questions out of remaining five questions.

1. (a) "COBIT 5 is the only business framework for the governance and management of enterprise Information Technology". The key principles of COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimizes information and technology investment and use for the benefit of stakeholders. Explain in detail these principles.

    (6 Marks)

    (b) Discuss various Personal Computer risks and security measures that may be adopted to mitigate these risks. **(5 Marks)**

    (c) Recognize various factors that influence an organization towards control and audit of its computers. **(3 Marks)**

2. (a) Audit of environmental controls requires the Information Systems Auditor to conduct physical inspections and observe practices. Determine broadly the checklist that he shall follow. **(6 Marks)**

    (b) Explain various plans that need to be designed as a part of Business Continuity Management (BCM) process. **(5 Marks)**

    (c) Elaborate the term "Segregation of Duties (SoD)"? **(3 Marks)**

3. (a) An employee of an organization has to prepare a detailed presentation on different types of Information Systems serve in an automated environment. Elaborate them and the groups these systems serve. **(6 Marks)**

    (b) Discuss various critical factors that should be considered by an IS Auditor as part of his/her preliminary review during Information Systems Audit. **(5 Marks)**

    (c) State the Section of Information Technology Act, 2000 that deals with "Tampering with Computer Source Document". **(3 Marks)**

4. (a) Mobile Computing has become a rapidly evolving technology in the world today. However, it has its own limitations. Discuss them. **(6 Marks)**

    (b) Identify the controls that are designed to reduce the impact of an error once it has been detected. Elaborate its characteristics as well. **(5 Marks)**

    (c) List the maintenance tasks that are undertaken in the development of Business Continuity Plan (BCP). **(3 Marks)**

5. (a) The Securities and Exchange Board of India (SEBI) is the regulator for the securities market in India. State various norms that SEBI recommends for conducting Systems Audit. **(6 Marks)**

    (b) From an IS auditor perspective, discuss various categories of Information Systems Audit that he can perform in an automated environment of an organization. **(5 Marks)**

    (c) Explain in brief the term "Program Debugging"? **(3 Marks)**

6. (a) Detailed investigation of the existing system is an important part of Systems Development Life Cycle (SDLC) in order to fully understand it and its related problems. Identify the areas that are required to be studied during this activity. **(6 Marks)**

    (b) Explain the key management practices required for aligning IT strategy with enterprise strategy.

    (5 Marks)

    (c) Discuss competence of an IS Auditor as suggested by Reserve Bank of India (RBI). **(3 Marks)**