

MOCK TEST PAPER II
FINAL (OLD) 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:

Green Technologies India Limited (GTIL) in India is a medium sized company engaged in the development/acquirement/customization of required Information systems for various organizations leading in multifarious domains. The dynamics of the business environment has compelled the organizations to acquire timeliness, accurate, meaningful and action-oriented information to remain competitive.

The company is committed to follow the best practices suggested under System Development methodologies which are formalized, standardized, documented set of activities used to structure, plan and control the process of developing an information system. Each of the available methodologies like Waterfall Approach, Agile Methodology, Spiral Model, Prototyping, Rapid Application Development, and Incremental Model are best suited to specific kinds of projects, based on various technical, organizational, project and team considerations. GTIL team needs to ensure that Logical Access Controls are well built into each developed/customized application so as to provide protection to their clients' information and resources, wherever they reside.

Further, to meet its business objectives and ensure continuity of services and operations in case of any disaster, GTIL adapted and followed well-defined and time-tested plans and procedures for efficient transition to the backup arrangement of its business systems and services. The ISO 27001:2013 certification is also sought by some organizations as to have the certification that the information security has been implemented in the best possible way in their organization.

As GTIL requires various software, hardware, storage capacity etc. for the multifarious projects undertaken by the company; the Board of Directors of GTIL decides to use Cloud Computing Technology. The company is not required to own the infrastructure, software, or obtain license of new software; rather the Cloud Computing environment provides on- premise and cloud resource services, middleware and software components available on pay-per usage basis.

1. The GTIL has been using various System Development methodologies with each methodology having certain strengths and weaknesses. Below mentioned are some statements based on these technologies. Identify the correct one.
 - (a) The Spiral model combines the advantages of top-down and bottom-up concepts and is intended for large and complicated projects.
 - (b) The Prototyping Model is a series of mini-waterfalls where all phases of waterfall model are completed for a small part of the system before proceeding to the next level.
 - (c) The key objective of Waterfall Model is the fast development and delivery of a high-quality system at a relatively low investment cost.
 - (d) The Incremental model includes development of a small or pilot version of part or whole system and given to the users for working and suggestions based on their working experience.
2. To implement a computerized environment regardless of its size; GTIL needs to establish an Internal Control system to achieve the goal of asset safeguarding, data integrity, system efficiency and system effectiveness for its clients' organization. Below mentioned are some statements about the Internal Control System and its components.

- (i) The control activities of the Internal Control System are required to ensure that the transactions are authorized, duties are segregated, and adequate documents and records are maintained.
- (ii) A control environment must include an assessment of the risks associated with each business process.
- (iii) For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process and the owners of the business process.
- (iv) The control activities must be developed to manage, mitigate, and eliminate the risks completely associated with each business process.

Identify the set of valid statements:

- (a) (i), (ii), (iii), (iv)
 - (b) (i), (ii), (iii)
 - (c) (i), (ii), (iv)
 - (d) (ii), (iii), (iv)
3. GTIL well recognizes the need of Business Continuity Management in case of occurrence of any disaster which means maintaining the uninterrupted availability of all key business resources required to support essential business activities. Which of the following activity would have been the foremost step in Business Continuity Planning (BCP) Process?
- (a) Developing a planning framework
 - (b) Testing the functioning of each business process
 - (c) Checking for compliance with laws and regulations
 - (d) Identifying the mission/business-critical functions
4. Through cloud Computing, GTIL may require accessing the shared pool of resources such as compute, network, storage, database and application as an on-demand service based on the projects it takes for which following service models are available.
- A. Software as a Service (SaaS)
 - B. Platform as a Service (PasS)
 - C. Infrastructure as a Service (IaaS)

The utilities of these service models are defined below:

- (i) Provides the end-users the ability to develop and deploy an application on the development platform provided by the service provider.
- (ii) Provides computing services such as processing power, memory, storage, and networks for cloud users to run their application on-demand.
- (iii) Provides the end-users to access an application over the Internet that is hosted and managed by the service provider.

Match the aforementioned service models with their utilities and choose the correct option:

- (a) A – (i), B - (ii), C – (iii)
- (b) A – (iii), B - (i), C – (ii)
- (c) A – (ii), B - (i), C – (ii)
- (d) A – (iii), B - (ii), C – (ii)

5. The Logical Access Controls are one of the means of Information security to provide access to information resources in a need to know and need to do basis. Identify the control that does not fall under the category of Logical Access Controls.
 - (a) Operating System Access Control
 - (b) Application and Monitoring Systems Access Control
 - (c) User Access Management
 - (d) Quality Assurance Management Control
6. Below are the reasons for which a client organization of GTIL may require ISO 27001:2013 certification for its Information Systems. In this context, identify the invalid reason for which the certification may be sought by the company.
 - (a) ISO 27001 is suitable for protecting critical and sensitive information.
 - (b) It provides a holistic, risk-based approach to secure information and compliance.
 - (c) It is globally accepted, if certified.
 - (d) As it is a regulator for the securities market in India, it is responsive to the needs of investors and market intermediaries.
7. The GTIL client organizations may vary in their requirement of the information based on the nature of their business. However, the information broadly can still be categorized based on its requirement by the top, middle and lower-level management. Identify correct statements.
 - (i) The low-level operational information is essential to carry out day-to-day activities smoothly and efficiently.
 - (ii) The low-level operational information is used by managers for short term planning.
 - (iii) Middle management requires tactical information that helps in implementing decisions taken by the top management.
 - (iv) Executive Information System is used by top level management essential for long-term planning.

Identify the set of valid statements.

 - (a) (i), (ii), (iii), (iv)
 - (b) (i), (iii), (iv)
 - (c) (ii), (iii), (iv)
 - (d) (i), (ii), (iii)
8. During the audit of Information Systems developed by GTIL for any client organization, the role of auditor at each activity performed by the senior management of that organization is discussed below. In this context, which statement is misfit?
 - (a) To determine how well the top management acquires and manages staff resources.
 - (b) To examine variables that often indicate when motivation problems exist or suggest poor leadership.
 - (c) To determine whether programmer employee automated facilities to assist them with their coding work or not.
 - (d) To focus on the control activities to ensure that the Information systems function accomplishes its objectives at a global level.

(8 x 2 = 16 Marks)

Question Nos. 9 to 22 carries 1 mark each.

9. Which of the following is not a practice to be followed while determining the status of IT Governance in an enterprise?
 - (a) Who makes directing, controlling and executing decisions?
 - (b) How are the governance results monitored and improved?
 - (c) What information is required to make decisions?
 - (d) Can the proposed application be implemented with existing technology?
10. In a store house where the operations related to customer billing, discount rates on daily basis, attendance system of staff, inventory status etc. are to be registered on daily basis, which Information System is the best fit?
 - (a) Transaction Processing System under Operational Level Systems
 - (b) Management Information System under Operational Level Systems
 - (c) Transaction Processing System under Management Level Systems
 - (d) Decision Support System under Management Level Systems
11. Compromise or absence of Logical Access Controls in an organization may result in potential losses due to various technical exposures that may lead to total shutdown of the computer systems. Which of the following does not fall under the category of technical exposure?
 - (a) Data Diddling
 - (b) Piggybacking
 - (c) Worm
 - (d) Trojan Horse
12. Suppose the first Full Backup consisting the entire list of files and folders was taken on first Monday of the month. On Tuesday, the backup of only the files that have changed, and new files added since Monday was taken. On Wednesday, the backup included only the changes and new files that changed or got added since Tuesday's backup. Identify the backup adopted in this case.
 - (a) Full Backup
 - (b) Incremental Backup
 - (c) Differential Backup
 - (d) Mirror Backup
13. In SDLC, Post implementation review is a vital phase that evaluates the answer to the question "Did we achieve what we set out to do in business terms?". Typical evaluations include the following except one. Identify it.
 - (a) Development evaluation
 - (b) Operational evaluation
 - (c) Information Evaluation
 - (d) Document Evaluation
14. During auditing, an Auditor should verify the following aspects. However, which of the following is not checked by the Auditor while performing audit of environmental controls in an organization?
 - (a) The presence of water and smoke detectors.
 - (b) Upkeep of complaint/maintenance logs.

- (c) The location of fire extinguishers and firefighting equipment.
 - (d) Presence of Network Access Controls in organization.
15. Under Section 65 of Information Technology Act, 2000; the offence related to "Tampering with computer source documents is punishable with _____".
- (a) imprisonment upto 5 years or with fine which may extend upto 2 lakh rupees or with both.
 - (b) imprisonment upto 3 years or with fine which may extend upto 2 lakh rupees or with both.
 - (c) imprisonment upto 3 years or with fine which may extend upto 3 lakh rupees or with both.
 - (d) imprisonment upto 3 years or with fine which may extend upto 3 lakh rupees or with both.
16. In Cloud Computing, which one of the following is not the service provided by Infrastructure as a Service (IaaS) provider?
- (a) Compute
 - (b) Storage
 - (c) Load Balancers
 - (d) Programming Languages
17. Identify the incorrect statement regarding COBIT 5.
- (a) COBIT 5 has 10 BAI processes where BAI stands for Build, Acquire and Implement.
 - (b) COBIT 5 framework describes seven categories of enablers.
 - (c) COBIT 5 has total of 39 Governance and Management processes.
 - (d) COBIT has five key principles for governance and management of enterprise IT.
18. Which one of the following is not an application of Data Mining?
- (a) Finance Planning and Asset evaluation
 - (b) Web Analysis
 - (c) Teleconferencing and Video Conferencing Systems
 - (d) Text mining and Web Analysis
19. In a computer-based environment, Operations Management Controls are responsible for the daily running of hardware and software facilities and are performed over various functions mentioned below except one. Identify it.
- (a) Computer Operations
 - (b) Production Control
 - (c) Data Preparation and Entry
 - (d) Data Coding
20. The Business continuity Life Cycle is broken down into following activities:
- (i) Recovery Plan Implementation
 - (ii) Determination of recovery alternatives
 - (iii) Recovery Plan Validation
 - (iv) Risk Assessment
- Arrange these activities in sequential manner and choose the correct option.
- (a) (iv) – (iii) – (ii) – (i)
 - (b) (iv) – (ii) – (i) – (iii)

- (c) (iv) – (i) – (iii) – (ii)
- (d) (i) – (ii) – (iii) – (iv)
21. A variety of tasks during the SDLC are performed by special teams/committees/individuals based on requisite expertise as well as skills. Identify the resource person responsible to conduct interviews with users and understand their requirements and is a link between the user and the designer/programmer?
- (a) Project Manager
- (b) Project Leader
- (c) System Analyst
- (d) Team Leader
22. Various audit techniques / tools enable auditors to significantly reduce the time between occurrence of the client's events and the auditor's assurance services thereon. Identify the audit technique that involves embedding of audit software modules within a host application system to provide continuous monitoring of the system's transactions.
- (a) Integrated Test Facility
- (b) System Control Audit Review File
- (c) Continuous and Intermittent Simulation
- (d) Snapshots
- (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) It is expected that every organization shall possess a document that provides statement of the rules to employees regarding their organization's technology and information assets, which they need to abide. Identify the document referred here and discuss it in detail. **(6 Marks)**
- (b) In an organization ABC Ltd., its Steering Committee is led by member of Board of Directors comprising of functional heads from all key departments of the organization including the audit and IT department. List the key functions that are expected to be performed by the IT Steering Committee for ABC Ltd. **(5 Marks)**
- (c) Explain the term Inherent Risk. **(3 Marks)**
2. (a) Mr. Mohan, an Information Systems Auditor, has undertaken an audit assignment of ASP Ltd., has a vital role to play in evaluating the performance of various controls under Managerial Controls. Under Managerial Controls, discuss the audit trail that Mr. Mohan shall refer to while evaluating different activities involved in Programming Management Controls. **(6 Marks)**
- (b) Business Impact Analysis (BIA) is an essential component of any organization's business continuity plan to determine and evaluate the potential effects of an interruption to critical business operations because of a disaster, accident, or emergency. Explain BIA and its significance. **(5 Marks)**
- (c) In a computer network, the controls in terms of physical components affect the reliability of network communication. Explain in brief these controls. **(3 Marks)**

3. (a) As a middle manager of PQR Ltd., you rely completely on Management Information System (MIS) of your organization considered to be an effective tool in enabling you in decision making by providing relevant information to you in the form of reports, tables, graphs, charts etc. at the right time. Identify various characteristics that MIS possess to be so meaningful to you. **(6 Marks)**
- (b) Consider yourself to be an IS Auditor. As a part of your preliminary investigation of audit environment, you are expected to gain a good understanding of the technology environment and related control issues. In this context, discuss the key consideration points during your understanding the technology. **(5 Marks)**
- (c) Define the following technological terms as defined under Information Technology Act, 2000.
 - (i) Computer
 - (ii) Addressee **(3 Marks)**
4. (a) In Cloud Computing environment, different types of cloud are provided catering to specific requirements of the users. Identify and discuss the cloud having partial security and complex cloud management. **(6 Marks)**
- (b) Elaborate the concept of "Segregation of Duties" and its significance. **(5 Marks)**
- (c) List of the goals of Business Continuity Plan of any enterprise. **(3 Marks)**
5. (a) Mr. Y posted an obscene, defamatory, and annoying message of his colleague, a divorcee woman Ms. A, in the gmail message group. E-mails were forwarded to the victim Ms. A for information by the Mr. Y through a false e- mail account opened by him in the name of Ms. A. She complained about this to the local police, based on which, the police nabbed Mr. Y. Investigation revealed that Mr. Y was interested in marrying her and on her reluctance to marry him, he started harassing her through internet. Under which provision of Information Technology Act, 2000; is Mr. Y can be convicted and sentenced. Describe the Section. **(6 Marks)**
- (b) Explain the categories of Information Systems Audit. **(5 Marks)**
- (c) Management of an organization seeking a new system for its working environment should establish certain acquisition standards that address the security and reliability issues as per current state-of-the art development standards. List them. **(3 Marks)**
6. (a) During System Development Phase, the developers are involved in System Development phase responsible for converting the design specifications into a functional system under the planned operating system environments. Discuss in brief various aspects/activities that are involved during this phase. **(6 Marks)**
- (b) An enterprise governance in an organization constitutes the entire accountability framework as it involves accountability for decision-making and has two dimensions – Corporate Governance and Business Governance. Elaborate them in detail. **(5 Marks)**
- (c) Section 15 of Information Technology Act, 2000 describes on how the Electronic signature are deemed to be Secure Electronic Signature. Define the section in detail. **(3 Marks)**