

Roll No.

Total No. of Printed Pages – 7

Total No. of Questions – 6

Maximum Marks – 70

GENERAL INSTRUCTIONS TO CANDIDATES

1. The question paper comprises two parts, Part I and Part II.
2. Part I comprises Multiple Choice Questions (MCQs).
3. Part II comprises questions which require descriptive type answers.
4. Ensure that you receive the question paper relating to both the parts. If you have not received both, bring it to the notice of the invigilator.
5. Answers to Questions in Part I are to be marked on the OMR answer sheet only. Answers to questions in Part II are to be written on the descriptive type answer book. Answers to MCQs, if written in the descriptive type answer book, will not be evaluated.
6. OMR answer sheet will be in English only for all candidates, including for Hindi medium candidates.
7. The barcoded sticker provided in the attendance register, is to be affixed only on the descriptive type answer book. No barcode sticker is to be affixed on the OMR answer sheet.
8. You will be allowed to leave the examination hall only after the conclusion of the exam. If you have completed the paper before time, remain in your seat till the conclusion of the exam.
9. Duration of the examination is 3 hours. You will be required to submit (a) Part I of the question paper containing MCQs, (b) OMR answer sheet thereon and (c) the answer book in respect of descriptive type answer book to the invigilator before leaving the exam hall, after the conclusion of the exam.
10. The invigilator will give you acknowledgement on Page 2 of the admit card, upon receipt of the above-mentioned items.
11. Candidate found copying or receiving or giving any help or defying instructions of the invigilators will be expelled from the examination and will also be liable for further punitive action.

PART – II

70 marks

1. Question paper – Part-II comprises 6 questions. Answer Question No. 1 which is compulsory and any 4 out of the remaining 5 questions.
2. Answers to the questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate has not opted for Hindi Medium, his/her answers in Hindi will not be evaluated.

JCT2

P.T.O.

(2)

JCT2

PART – II

1. XYZ Limited is an international public-private partnership based organisation established in the year 2011. The organisation is engaged in development of pandemic medicines and also acts as an angel investor for many start-up companies and supports them by providing technical training, mentorship, fund raising and financing for development of medicines. In the recent past, the top management reviewed the adequacy of the controls on the data security, business continuity management, and disaster recovery procedure and found that standard operating procedures of the organisation are not aligned with the current best practices used in the industry. Hence, the top management appointed Mr. A as Information System (IS) auditor for conducting internal IS audit. Mr. A used risk based approach for auditing the various information systems and submitted the IS audit report to the top management. Mr. A has indicated the various shortcomings in the IS audit report, some of them are as under :

- There is no formal IT governance framework and IT policy has not been updated and documented since 2011. Failure to regularly review and approve GEIT documentation has resulted in outdated, inaccurate and incomplete IT plans. Incorrect IT plan documentation have resulted in incorrect or ineffective actions being taken by the personnel in response to emergency or disaster causing additional harm to customers, employees, loss of assets and the reputational damage. The organization does not have consistent vulnerability management program. The network of organization's infrastructure is not documented and kept up-to date to facilitate risk assessment and identification of potential issues for security.

JCT2

(3)

JCT2

- The organisation has not undertaken formal risk assessment activity since its inception for updating control procedures for improving security to various business processes. Failure to understand the key risks, their impact on activities and resources critical for delivering services, limits the effectiveness and completeness of IT plan for maintaining continuity of operation and safely executing recovery operations from disaster.
- Roles and responsibilities in relation to business continuity planning and disaster recovery planning have not been clearly defined. Employees are not trained and tested on performance of emergency management, business continuity and disaster recovery operations.

For achieving the state of art technological status aligned with best practices in industry for adequacy of controls for security, business continuity planning and disaster recovery planning, Mr. A has suggested to use COBIT 5 framework, periodic review and update of policies, IT plans and strengthening of document & record control process in the organisation. He has also suggested for conducting risk assessment at least once in a year to design better control system for improving the security of IT operations specifically preventing the theft of information of the latest R & D results.

Read the above carefully and answer the following questions :

- (a) Risk management is the process of assessing the risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. You have been assigned to implement Risk Management for the organization. Describe briefly various key management practices for implementing Risk Management in the above organization. 6

JCT2

P.T.O.

(4)

JCT2

- (b) The methodology for developing a Business Continuity Plan can be sub-divided into different phases. During vulnerability assessment and general definition of requirements phase, this phase addresses measures to reduce the probability of occurrence. You are requested to suggest the management various key tasks, which are included in this phase. **5**
- (c) Mr. A has followed the Risk Based Approach for auditing the Information Systems of the organization. Explain briefly key steps that can be followed for a risk-based approach to make an audit plan for information systems. **3**
2. (a) With the advancements in the technology, cyber frauds are also increasing day-by-day across the world. What are the major reasons behind the rise of such frauds in an enterprise? Also explain briefly the impacts of cyber frauds on enterprises. **6**
- (b) Management Information System (MIS) supports the managers at different levels to take decisions to fulfill the organizational goals. Explain briefly any five major characteristics of an effective MIS. **5**
- (c) Explain different types of Audit during System Development process. **3**

JCT2

(5)

JCT2

3. (a) XYZ bank is required to update its Information Systems to release new product in the market. The technical team of the bank calculates and proposes a timeline of 18 months to update the system and release the new version of the software but top management wants to release the product in the market as soon as possible. The top management appoints you as a consultant to advise suitable systems development methodology to the technical team of the bank for the same. 6
- You are requested to explain; why Agile Model should be adopted for systems development methodology ?
- (b) Electronic door locks are always preferred by many enterprises as controls for Physical Access Exposures. Describe briefly any five advantages of electronic door locks over bolting and combinational locks. 5
- (c) Describe briefly any three major benefits of an Expert System. 3
4. (a) ABC Limited is a software development company providing on-line marketing solutions including web design, content management and e-commerce solutions and various support services. The top management has assigned you to conduct Information System (IS) Audit of the company. Explain briefly various steps to be followed by you for conducting the IS Audit. 6

JCT2

P.T.O.

(6)

JCT2

- (b) The five key principles for governance and management of enterprise IT in 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. 5

In the above context, explain briefly the five key principles of COBIT 5.

- (c) In case of development of Business Continuity Plan (BCP), what are the objectives of performing BCP tests ? Describe briefly any three objectives. 3

5. (a) Control is a system that prevents, detects or corrects unlawful events. Various controls are adapted as per requirement and accordingly, their audit become necessary. You are appointed as an IS auditor to advise the management various factors influencing an organization towards controls and audit of computers. Explain these factors. 6

- (b) Systems Requirements Analysis phase analyses the typical system requirements, in view of its functionalities, deliverables etc. You have been assigned the task to suggest various objectives, which are performed in this phase in order to generate the deliverable, Systems Requirements Specifications (SRS). Explain these objectives in brief. 5

- (c) Describe any three benefits of Governance of Enterprise IT (GEIT). 3

JCT2

(7)

JCT2

6. (a) ABC is a global consultation and IT service providing company in the area of information and cyber security. The company is seeking your advice for adopting an ISO-27001 standard. Explain briefly various reasons for adoption of the ISO-27001 standard and also key benefits of ISO-27001 to be achieved by the company. **6**
- (b) Describe the various characteristics of Infrastructure as a Service (IaaS) model of Cloud Computing. **5**
- (c) The Security and Exchange Board of India (SEBI) is the regulator for the securities market in India. What are the requirements of systems audit, which SEBI had mandated for exchanges ? **3**

OR

Enterprises need to take steps to ensure compliance with cyber laws. Explain briefly any three key steps for ensuring compliance with cyber laws in an enterprise.

JCT2