Duration: **120 Minutes**

Total Marks: **80 marks**

Read the following instruction carefully before responding to the questions given in the examination paper.

- Ensure that you have filled up the basic details asked in Answer sheet.
- Use this same sheet to answer the question.
- The question paper is divided into 4 main sections. All sections are **compulsory**.
- Candidate need to score minimum 70 % of the total marks (i.e. 56 out of 80) to pass this examination. You must achieve a minimum of 40% in each of the 4 sections.
- Total duration of this examination is 120 minutes. Candidates who require special assistance may inform our office for support at least 7 days in advance.
- You must write answers by ball pen. Answers written by pencil will not be considered for evaluation.
- There is no negative marking system applicable in this examination.
- Students cannot retain the examination paper after the examination.
- Use of applicable ISO standard while responding to questions, is permitted.

For Official Use Only (To be filled in by the Evaluators)

Section	Marker 1	Marker 2	Maximum
1			10
2			20
3			20
4			30
Total			**80**

Pass Marks (70% overall): 56 Marks **Final Result: Pass / Fail**

Name of Marker 1._____ Signature of Marker 1:_____

Name of Marker 2._____ Signature of Marker 2:_____

Sections	Description	Max Marks
Section-1	It consists of 10 multiple choice questions. Circle the correct answer to indicate which you judge to be the best answer or to state the number of a clause from ISO 27001. You must only give one answer for each question. If you have made a mistake, please clearly strike through your mistake and re-circle the correct answer	**10 Marks**
Section-2	It comprises of 4 questions. Write brief answers in the space provided	**20 Marks**
Section-3	It comprises of 2 questions. Write detailed answers in the space provided	**20 Marks**
Section-4	It comprises of 3 questions. This section consists of 3 scenarios for which Non-conformity reports (NCR's) maybe required to be completed. a. If you consider there is insufficient objective evidence to write an NCR then complete the observation report and state why it is not non-conformity and what you would do next. b. If you consider that the incident is non-conformity with sufficient objective evidence, then complete the non-conformity report by categorizing as major or minor.	**30 Marks**

Section 1

10 multiple-choice question where the participant needs to encircle the letter of his choice corresponding to the best answer. (Each question is worth ONE mark.)

1. The Property that information is not made available or disclosed to unauthorized individuals, entities or processes is
   A Integrity
   B Availability
   C Confidentiality
   D All of the above
   E None of the above

2. A supplier audit is referred to as
   A First party audit
   B Second party audit
   C Third party audit
   D Accredited audit

3. Document describing the control objectives and controls that are relevant and applicable to the organization is called
   A Statement of Applicability (SOA)
   B Asset Register
   C Risk Treatment Plan
   D Business Continuity Plan
   E All of the above

4. Security Risk is a function of:
   A Asset Value
   B Vulnerability
   C Threat
   D All of the above
   E None of the above

5. Competence of auditor is demonstrated by
   A Education
   B Work Experience
   C Auditor Training
   D Auditing Experience
   E All of the above

6. The requirements for documented information is specified in Clause_____of the standard

7. As per the standard, internal audits are to be conducted
   A Quarterly
   B Annually
   C Planned intervals
   D None of the above

8. An audit is a
   A Fact finding process
   B Fault finding process
   C Improvement process
   D All of the above

9. From an information security audit perspective, an asset is
   A Anything which is expensive
   B Hardware
   C Personnel
   D B & C
   E All of the above

10. Reporting of information security events through appropriate management channels is required by the standard as per control _____

Section 2

Write a brief answer to each of the following four questions using only the space provided.
(Each question is worth 5 marks.)

2.1 Identify the clauses and controls applicable for Human Resource?

2.2 How many categories & controls are available in ISO 27001:2022? List the security domains in ISMS?

2.3 Explain the phases of audit execution and the agenda of the opening meeting?

2.4 List down all the competencies that you would expect in an auditor?

Section 3

Write a brief answer to each of the following two questions using only the space provided.
(Each question is worth 10 marks.)

3.1 Prepare a checklist to conduct an audit for Information Security Incident Management. Also mention appropriate Clause / Control with each.

3.2 What is ISMS? What are the advantages of Information Security Management System?

Section 4

This section consists of three scenarios for which Non-conformity reports (NCR's) **may or may not be** needed to be completed. (Each question is worth 10 marks.). Please read general instructions regarding section 4.

4.1 Incident 1:

During an audit, auditor was checking supplier agreements for all suppliers providing services to the company. All agreements were in place except for the housekeeping team. On further investigation, it was found that the lady running housekeeping service was a close friend of the MD and they knew each other since long. Not to offend the MD, Chief Information Security Officer was reluctant to get the same signed from her.

If you think there is evidence of non-conformity, complete this report:

NON CONFORMITY REPORT	
Company Audited	Date:
Auditor	Auditee:
Area Under Review	
Clause/Control No:	Category : Major / Minor
Non-Conformity Details:	

OR

If you consider there is insufficient objective evidence to write an NCR then state the reasons for your decision and state what you would do next.

4.2 Incident 2:

During HR audit, the auditor asked the HR executive as to where he keeps his files. The HR executive mentioned that they were provided with a folder on file server with their name to keep all their work related files. Auditor checked his network drive mapping and found that he could connect to the HR executive's folders and also folders which were of his Manager.

If you think there is evidence of non-conformity, complete this report:

NON CONFORMITY REPORT	
Company Audited	Date:
Auditor	Auditee:
Area Under Review	
Clause/Control No:	Category : Major / Minor
Non-Conformity Details:	

OR

If you consider there is insufficient objective evidence to write an NCR then state the reasons for your decision and state what you would do next.

4.3 Incident 3:

During an audit, the auditor observed that the Engineer from the Supplier responsible for Hardware maintenance carried the laptop from the office premise without creating an entry in the outward register maintained by the Physical Security Guard. When auditor questioned the Physical Security guard, he said that recording was not required since the engineer was from a known supplier and he usually carries laptops for repairs.

If you think there is evidence of non-conformity, complete this report:

NON CONFORMITY REPORT	
Company Audited	Date:
Auditor	Auditee:
Area Under Review	
Clause/Control No:	Category : Major / Minor
Non-Conformity Details:	

OR

If you consider there is insufficient objective evidence to write an NCR then state the reasons for your decision and state what you would do next.
