A–1305

Total Pages : 4 **Roll No. .....**

MCS-601/MIT (CS)-201

(MCA/MSCCS)

Information Security Assurance : Framework, Standards & Industry best Practices

Examination February, 2026

Time : 2:00 Hrs. Max. Marks : 70

Note* :–** This paper is of Seventy (70) marks divided into Two (02) Sections 'A' and 'B'. Attempt the questions contained in these Sections according to the detailed instructions given therein. ***Candidates should limit their answers to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

Section–A

(Long Answer Type Questions) (2×19=38)

***Note* :–** Section 'A' contains Five (05) Long-answer type questions of Nineteen (19) marks each. Learners are required to answer any *two* (02) questions only.

1. (a) Explain the structure and purpose of ISO/IEC 27002 : 2013. Discuss how it supports the implementation of ISO/IEC 27001. (10)

   (b) Describe the changes introduced in ISO/IEC 27002 : 2015 compared to earlier versions. (09)

2. (a) Describe the major provisions of HIPAA, GLBA, and COPPA and their relevance to information security. (10)

   (b) Explain the common elements of compliance in information security programs and discuss organisational responsibilities. (09)

3. (a) Discuss NIST Cybersecurity Framework (CSF). Explain its core functions and how it integrates with ISO/IEC 27001. (10)

   (b) Explain the OWASP methodology and describe any five OWASP Top-10 risks with examples. (09)

4. (a) What is an ISMS Internal Audit ? Explain the complete audit lifecycle including planning, execution, reporting and follow-up. (10)

(b) Discuss the roles and responsibilities of auditors and auditees during an ISMS audit. (09)

5. (a) Define Business Continuity Management (BCM). Describe key components of an effective Business Continuity Plan. (10)

(b) What is Disaster Recovery Testing ? Explain types of DR tests and their importance. (09)

Section–B

(Short Answer Type Questions) (4×8=32)

***Note* :–** Section 'B' contains Eight (08) Short-answer type questions of Eight (08) marks each. Learners are required to answer any *four* (04) questions only.

1. Differentiate between ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27005.

2. Explain defense-in-depth with examples from administrative, technical, and physical controls.

3. Describe the key steps of risk treatment planning under ISO/IEC 27001.

4. What are Computer Assisted Audit Techniques (CAATs) ? Mention any two tools used in IS security audits.

5. Briefly explain Incident Response Plan (IRP) and its phases.

6. What is Cryptographic Hashing ? Explain its role in ensuring integrity.

7. Discuss the difference between Qualitative and Quantitative Risk Assessment.

8. Write short notes on the following :

   (a) Vulnerability Assessment

   (b) Penetration Testing

****