A–0830

Total Pages : 5 **Roll No. .....**

MCS-601/MIT(CS)-201

INFORMATION SECURITY ASSURANCE : FRAMEWORK, STANDARDS & INDUSTRY BEST PRACTICES

(MCA/MSCCS)

Examination, June 2025

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. Answer the following :

   (a) What is the importance of Information Security standards in an organization ? (5 marks)

   (b) Explain the structure and content of ISO/IEC 27002:2013. How does it contribute to an organization's security posture ? (7 marks)

   (c) Discuss the key changes from the ISO/IEC 27001:2005 standard to the ISO/IEC 27001:2013 standard. (7 marks)

2. Answer the following :

   (a) Discuss the concept of risk assessment in Information Security. (5 marks)

   (b) Explain the concept of FISMA (Federal Information Security Modernization Act) and its role in securing government systems. (7 marks)

   (c) What is the role of the NIST Cyber Security Framework in the development of an Information Security management strategy ? (7 marks)

3. Answer the following :

   (a) Explain the concept of Information Security Governance and its importance in an organization's overall security strategy. (5 marks)

(b) Discuss the various types of security threats organizations face and how they can be mitigated through preventive measures. (7 marks)

(c) What are the critical elements of Information Security controls in the context of maintaining confidentiality, integrity, and availability ?

(7 marks)

4. Answer the following :

(a) Explain the importance of conducting Information Security audits in organizations. (5 marks)

(b) Describe the audit process in ISMS. How does it help identify security gaps in an organization ?

(7 marks)

(c) What are the challenges faced during the auditing process and how can they be addressed ?

(7 marks)

5. Answer the following :

(a) Discuss the principles and best practices of Disaster Recovery Planning (DRP). (5 marks)

(b) Explain the relationship between Disaster Recovery and Business Continuity Planning.

(7 marks)

(c) How can an organization ensure that its disaster recovery plan remains effective and up to date ?

(7 marks)

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. What is the purpose of cryptographic algorithms in securing data ? Discuss the different types of cryptographic algorithms.

2. Explain the concept of Information Security Risk Management. What are the steps involved in performing a risk assessment ?

3. What is the role of OWASP in securing web applications ? Discuss the OWASP Top Ten risks.

4. What are the key components of a Business Continuity Plan ? How do they ensure the sustainability of an organization during a crisis ?

5. Discuss the significance of Information Security compliance standards and the role of frameworks like COBIT and PCI DSS in achieving compliance.

6. What is the role of ITIL in improving Information Security practices within an organization ?

7. Explain the concept of "Defense in Depth" in cybersecurity. How does it improve security resilience ?

8. Describe the key regulatory frameworks related to Information Security and their impact on organizational policies.

****