A–841

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

MCS-601/MIT (CS)-201

MCA/MSCCS

(Information Security Assurance : Framework, Standards and Industry Best Practices)

3rd/2nd Semester Examination, 2024 (June)

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. Explore the key provisions and requirements of the Sarbanes-Oxley Act (SOX). Why was SOX introduced, and how does it impact organizations ?

2. Provide an overview of COBIT and ITIL, including their domains and significance in Information Security Management.

3. Answer the following :

   (a) Discuss the components of an Information Security Management System (ISMS) and the planning involved. Explain the importance of ISMS documentation, asset identification, and risk assessment. 10

   (b) Describe the PDCA (Plan-Do-Check-Act) cycle in the context of ISO/IEC 27001. How does it contribute to the continuous improvement of Information Security ? 9

4. Answer the following :

   (a) Provide an introduction to security audit, its process, and planning. Discuss the different types of audits and their purposes, with a focus on ISMS auditing.

(b) Explain the importance of disaster recovery planning. Discuss the development of disaster recovery plans, including the methodology and classification of disasters.

5. Answer the following :

(a) Explain specific tools used in network security in details. 8

(b) What is SANS ? Explain. 4

(c) What are Application Security Risks ? 4

(d) Write steps included in Incident response plans ? 3

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. Define the elements of an Information Security Policy. Discuss the significance of having a well-defined policy in an organization.

2. Explore the significance of OWASP (Open Web Application Security Project) in the context of application security.

3. Highlight the importance of information security. Define key concepts such as confidentiality, integrity, availability, and non-repudiation.

4. Explain Payment Card Industry Data Security Standard.

5. Discuss risk management, controls, and frameworks such as defense in depth. Explore different types of controls, including administrative, logical, and physical controls.

6. Define business continuity planning and its importance. Discuss the key components of creating a business continuity plan, including governance, business impact analysis, and continuity plans.

7. Explain the guidelines for auditors/auditing organizations and auditees in the context of Information Security Management.

8. Answer the following :

   (a) List some of the points to improve security posture of organization. 4

   (b) What is role of non-disclosure agreement in auditing ? 4

****