Total Page No. : 4] **[Roll No. ....**

MCS–601/MIT(CS)–201

(MCA/MSCCS) IIIrd/IInd Semester Examination Dec., 2023

INFORMATION SECURITY ASSURANCE : FRAMEWORK, STANDARDS AND INDUSTRY BEST PRACTICES

Time : 2 Hours] [**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 there in. ***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.

   (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 ?

4. Answer the following :

   (a) Introduce business continuity planning and discuss its importance. Explain the components of business continuity planning, including BCP governance, business impact analysis, and recovery plans.

(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) What is the concept of Auditing ? (3)

(b) What are the different types of audits ? (4)

(c) What is the purpose of auditing ? (3)

(d) Explain the four phases of ISMS audit program. (5)

(e) Explain the three phases of an internal audit. (4)

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. Explain the purpose of cryptography and the types of cryptographic algorithms, including secret key cryptography, public-key cryptography and has functions.

2. Explain 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. Provide an overview of the Payment Card Industry Data Security Standard (PCI DSS) and its requirements.

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 planing 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. Compare the NIST Cyber Security Framework with ISO 27001. Discuss their respective applications in ensuring information security.

****