A-0886

Total Pages : 6 **Roll No. ----------**

MCS-601/MIT (CS)-201

Information Security Assurance:

Framework, Standards & Industry Best

Practices

(MCA/MSCCS)

3rd /2nd Semester Examination 2024(Dec.)

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.

P.T.O.

Section-A (Long-Answer-Type Questions)

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.

[2x19=38]

Q.1. Answer the following:

a. What are the elements of an Information Security Policy? [5 marks]

b. Discuss ISO/IEC 27001: 2013 and its significance for Information Security Management Systems (ISMS). [7 marks]

c. How do network and data protection view points contribute to improving an organization's security posture? [7 marks]

Q.2. Answer the following:

a. Explain the Sarbanes-Oxley Act (SOX) and its significance in Information Security regulations. [5 marks]

b. Discuss the Payment Card Industry Data Security Standard (PCIDSS). What are its requirements and best practices? [7 marks]

c. How does HIPAA (Health Insurance Portability and Accountability Act) impact Information Security in healthcare organizations? [7 marks]

Q.3. Answer the following:

a. Discuss the concept of Risk Management in Information Security. [5 marks]

b. What is the role of NIST in Information Security? Explain the objectives of NIST SP800-50. [7 marks]

c. Describe the OWASP Top Ten Application Security Risks and their importance in securing web applications. [7 marks]

P.T.O.

Q.4. Answer the following:

a. What is an Information Security Management System (ISMS)? Discuss its planning and documentation process. [5 marks]

b. Explain the PDCA (Plan-Do-Check-Act) cycle for Information Security management. [7 marks]

c. Discuss the Statement of Applicability (SoA) and its role in ISMS. [7 marks]

Q.5. Answer the following:

a. Explain the concept of Security Audits in Information Security. [5 marks]

b. What are the various types of security audits? Discuss the audit activities and process involved in an ISMS audit. [7 marks]

c. How does the Sarbanes-Oxley Act Influence IT audits and the need for regulatory compliance? [7 marks]

Section-B (Short-Answer-Type Questions)

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. [4x8=32]

Q.1. Define Information Security. What are the key principles of Information Security?

Q.2. Discuss the importance of Disaster Recovery Planning and its role in Business Continuity.

Q.3. What are the benefits and limitations of ISO/IEC 27001 and 27002 in securing organizational information?

Q.4. Explain the concept of Data Encryption and the different types of encryption algorithms.

Q.5. What are the common pitfalls in implementing Information Security programs and how can they be mitigated?

P.T.O.

Q.6. Discuss the role of ITIL (Information Technology Infrastructure Library) in Information Security management.

Q.7. What is Business Continuity Planning (BCP) and how does it ensure the resilience of an organization during disruptions?

Q.8. Explain the concept of Defense in Depth in Information Security. How does it enhance security posture?

****