P-882

Total Pages : 4 Roll No. ....

MCS-601

Information Security Assurance: Framework, Standards & Industry Best Practices

Master of Computer Application (MCA)

3rd Semester Examination, 2023 (June)

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 therein. Candidates should limit their answer to the questions on the given answer sheet. No additional (B) answer sheet will be issued.

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.

(2×19=38)

1. Write a short note on :

(a) How to mitigate threats and risks? (4)

(b) Describe Business Impact Analysis ? (4)

(c) What is the purpose of Business impact analysis BIA ? (3)

(d) Write down the components of controversies in DRP. (4)

(e) What is the relationship between BCP and DRP? (4)

2. Answer the following :

(a) Explain PDCA cycle in details. (8)

(b) What is administrative control? How to achieve it? (5)

(c) Describe the onion model of defense in depth. (6)

3. 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)

4. 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)

5. Write a short note on the following :

(a) Cryptography. (3)

(b) IAS-octave. (3)

(c) OWASP. (3)

(d) Change management . (4)

(e) How to make an effective Security Audit Reporting? (3)

(f) Risk Management? (3)

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. (4×8=32)

1. Answer the following:

(a) List the objectives of the auditor. (4)

(b) What is follow-up audit? (4)

2. Answer the following:

(a) List some of the common pitfalls of information security program. (4)

(b) Compare NIST cyber security framework with ISO 27001. (4)

3. Explain Payment Card Industry Data Security Standard. (8)

4. Answer the following :

(a) How do the Common Criteria work? (4)

(b) What is COBIT? Explain COBIT pentagon. (4)

5. Answer the following :

(a) What are the Critical factors of ISMS? (2)

(b) Explain ISMS planning phase in details. (3)

(c) What should SOX implementers do in real-time ? (3)

6. Describe different types of Disasters with appropriate example. (8)

7. Answer the following :

(a) Define the term "cyberspace" as per ISO/IEC 27032. (2)

(b) Explain NIST CYBER SECURITY FRAMEWORK. (6)

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)