S-778

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

MCS-601

Information Security Assurance: Framework, Standards & Industry Best Practices

Master of Computer Application (MCA)

3rd Semester, Examination 2022(Dec.)

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.

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 x 19 = 38]

P.T.O.

Q.1. Write a short note on:

a. What is regulation? (2 marks)

b. What is policy? (2 marks)

c. What is Public-Key Cryptography? (3 marks)

d. What is compliance? (3 marks)

e. What is Target of Evaluation? (3 marks)

f. What is Evaluation Assurance Level? (3 marks)

g. What is Security Assurance Requirements? (3 marks)

Q.2. Answer the following:

a. What is SARBANES-OXLEY ACT (SOX). (4)

b. Why SOX was born? (5)

c. List Key requirement/provisions made in SOX. (5)

d. What should SOX implementers do in real-time? (5)

Q.3. Answer the following:

a. Explain the scope and objectives of NIST. (5)

b. What is SANS? Explain. (5)

c. What are Application Security Risks? (5)

d. List the Code of Ethics suggested by OWASP. (4)

Q.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)

Q.5. Answer the following:

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

b. Why information security is important? (3)

c. Explain IAS-octave. (6)

d. What is risk management? (3)

e. Explain why security classification for information is important? (4)

P.T.O.

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 x 8 = 32]

Q.1. Answer the following:

a. Explain ISO/IEC 27002:2013 model. (4)

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

Q.2. Answer the following:

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

b. Explain FISMA. (4)

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

Q.4. Answer the following:

a. How do the common Criteria work? (4)

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

Q.5. Answer the following:

a. What are the Critical factor of ISMS? (2)

b. Explain ISMS planning phase in details (3)

c. What is Risk Treatment plan? (3)

Q.6. Explain PDCA cycle in details. (8)

Q.7. Answer the following:

a. Differentiate between ISO 27001 and ISO 27002. (2)

b. Explain NIST CYBER SECURITY FRAMEWORK. (6)

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

****