C1000

Total Pages : 4 Roll No. ....

MIT (CS)-201/PGDCS-05

Information Security Assurance: Framework, Standards and Industry Best Practices

(MSCCS-18/PGDCS-17)

2nd Semester Examination, 2022 (June)

Time : 2 Hours] **Max. Marks : 80**

Note : This paper is of Eighty (80) 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 Twenty (20) marks each. Learners are required to answer any Two (02) questions only.

(2×20=40)

1. Answer the following :

(a) Define Auditing. (3)

(b) Explain different types of auditing. (6)

(c) Discuss phases of ISMS audit. (6)

(d) What is role of non-disclosure agreement in auditing. (3)

(e) What is follow-up audit ? (2)

2. Answer the following :

(a) What is Information Security? (4)

(b) What is administrative control? How to achieve it? (8)

(c) Define different types of Access controls. (8)

3. Answer the following :

(a) Explain some of the common pitfalls of Information Security Program. (7)

(b) What is HIPPA? (3)

(c) What is FISMA? (5)

(d) What is the purpose of FISMA? (5)

4. Answer the following :

(a) Explain COBIT framework. (6)

(b) Explain COBIT cube. (7)

(c) Explain COBIT Pentagon. (7)

5. Answer the following:

(a) Define NIST. (4)

(b) What is the scope/objectives of NIST? (5)

4. (c) Explain the lifecycle of Information security training and awareness program. (6)

(d) What are the various models used in managing a security training function? (5)

SECTION–B

(Short Answer Type Questions)

Note : Section 'B' contains Eight (08) short answer type questions of Ten (10) marks each. Learners are required to answer any Four (04) questions only. (4×10=40)

1. Answer the following :

(a) Compare NIST cyber security framework with ISO 27001. (5)

(b) Explain ISO 27001 certification process. (5)

2. Answer the following :

(a) How to make an effective Security Audit Reporting? (6)

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

3. Answer the following :

(a) What is disaster recovery plan (DRP)? Why DRP is important? Write its benefits. (5)

(b) Write the steps of planning methodology. (5)

4. Describe Business Impact Analysis. What is the purpose of Business impact analysis (BIA)?

5. Answer the following :

(a) What is OWASP project? (3)

(b) What is the code of ethics of OWASP? (3)

(c) What is OWASP Top Ten? (4)

6. Answer the following :

(a) Explain Information Security Management System. (3)

(b) Explain Risk assessment process and risk treatment plan. (4)

(c) What is SoA? (3)

7. Answer the following :

(a) Write note on ISO standards. (3)

(b) What is ISO 27001? (4)

(c) Define the term "cyberspace" as per ISO/IEC 27032. (3)

8. Explain the following terms : (2 marks each)

(a) Confidentiality.

(b) Availability.

(c) Integrity.

(d) Non-repudiation.

(e) Risk Management.