824

Total pages : 05 Roll No. .....

MIT (CS)-201/PGDCS-05

Information Security Assurance: Framework, standards and Industry best practices

(MSCCS-18/PGDCS-17)

Examination 2021 (Winter)

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 x 20=40)

Q.1 Answer the following :

a. Define key concepts of Information Security. (4 marks)

b. Describe Risk Management process. (6 marks)

P.T.O.

c. Describe the onion model of defense in depth. (5 marks)

d. Write steps included in Incident response plan. (5 marks)

Q.2 Answer the following :

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

b. What is disaster recovery plan (DRP)? (5 marks)

c. Why DRP is important? Write its benefits. (7 marks)

Q.3 Answer the following :

a. What is Sarbanes-Oxley Act? (4 marks)

b. Why SOX was born? (4 marks)

c. Key requirements/provisions of SOX? (8 marks)

d. What should SOX implementers do in real-time? (4 marks)

Q.4 Explain the following terms: (4 marks each)

a. Protection Profile

b. Security Target

c. Security Functional Requirements

d. Security Assurance Requirements

e. Evaluation Assurance Level

Q.5 Answer the following :

a. What is ISMS? (6 marks)

b. What are the critical factors of ISMS? (7 marks)

c. What are the necessary requirements for the ISMS to be effective? (7 marks)

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 x 10=40)

Q.1 Answer the following :

a. Write short note on relationship of ISO/IEC 27001 and 27002 standards. (5 marks)

b. Explain benefits of ISO 27001 certification. (5 marks)

Q.2 Answer the following :

a. What do you understand by ISMS internal audit? (2 marks)

b. Discuss phases of ISMS audit. (5 marks)

P.T.O.

c. Discuss some responsibilities of auditors and auditee during ISMS audit execution. (3 marks)

Q.3 What is business continuity planning (BCP)? Why is BCP important? Write different steps to create a business continuity plan.

Q.4 Answer the following :

a. What are the objectives of an IT security policy? (4 marks)

b. Explain Hierarchical policy scheme. (6 marks)

Q.5 Explain PDCA cycle in detatils.

Q.6 Answer the following :

a. Write short note on importance of international standards. (3 marks)

b. Explain benefits by international standards to the Governments. (3 marks)

c. Differentiate between ISO 27001 and ISO 27002. (4 marks)

Q.7 Answer the following :

a. Explain ISO 27001 certification process. (4 marks)

b. Compare NIST cyber security framework with ISO 27001. (6 marks)

Q.8 Answer the following :

a. Explain FISCAM (Federal Information Systems Control Audit Manual. (5 marks)

b. How to make an effective Security Audit Reporting? (5 marks)

****