Total No. of Printed Pages : 6 Roll No.....

MIT (CS)-201/PGDCS-05

INFORMATION SECURITY ASSURANCE FRAMEWORK, STANDARDS AND INDUSTRY BEST PRACTICES

Master of Science (Cyber Security)/ P.G. Diploma in Cyber Security (MSCCS-18/PGDCS-17)

2nd Semester, Examination-2020

Time Allowed : 2 Hours Maximum Marks : 80

Note : This paper is of Eighty (80) marks divided into Two (02) sections A and B. Attempt the question 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) What is Business Impact Analysis? What is the purpose of Business Impact Analysis? 7

   (b) Write a short note on the Sarbanes-Oxley Act. 6

   (c) What are security controls? Explain the various categories of Security controls. 7

2. Write short notes on the following : 5×4=20

   (a) Payment Card Industry Data Security Standard (PCI DSS)

   (b) HIPAA

   (c) GLBA

   (d) FISMA

   (e) FIPS.

3. Answer the following :

   (a) What is the Target of Evaluation (TOE)? Explain how TOE verifies the target's security features? 7

(b) What is OWASP? Explain. 6

(c) What is significance of ISO/IEC 27000 standard. 7

4. Answer the following :

(a) What is Information Security Management System (ISMS)? What are the necessary conditions for ISMS to be effective? 7

(b) What is PDCA cycle? Explain. 6

(c) Compare NIST cyber security framework with ISO 27001. 7

5. Answer the following :

(a) Explain Auditing. Explain different types of auditing. 7

(b) Discuss principles of auditing. 6

(c) What is role of non-disclosure agreement in auditing. 7

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. What is Business Continuity plan (BCP)? Why it is important?

2. What are the various elements of Information Security Policy?

3. What are the best Practices for implementing PCI DSS into Business-as-Usual Processes?

4. Explain Risk assessment process and risk treatment plan.

5. Answer the following :

(a) Define the term "cyberspace" as per ISO/IEC 27032. 5

(b) Differentiate between ISO 27001 and ISO 27002. 5

6. Answer the following :

(a) Discuss some responsibilities of auditee during ISMS audit execution. 5

(b) Discuss responsibilities of auditors in ISMS audit engagement. 5

7. Answer the following :

(a) Describe different types of Disasters with appropriate example. 5

(d) What is disaster recovery plan (DRP)? Write down the components of controversies in DRP. 5

8. Answer the following :

(a) Describe the onion model of defense in depth. 3

(b) Why is Security Classification of information necessary? 3

(c) What is administrative control? How to achieve it? 4

****