Total No. of pages : 06 Roll No. .....

PGDCS-05

Information Security Assurance : Framework, Standards and Industry best practices

PG Diploma in Cyber Security (BCA-11/16/17)

2nd Semester

Examination, 2019

Time : **3** *Hours* *[Maximum 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 Fifteen (15) marks each. Learners are required to answer any three (03) questions only. **(3×15=45)**

1. Answer the following : (5 marks each)

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

   (b) List key requirements/provisions made in SOX.

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

2. Answer the following : (5 marks each)

   (a) Explain the scope and objectives of NIST.

   (b) What is SANS? Explain.

   (c) What are Application Security Risks?

3. Answer the following :

   (a) What is the concept of Auditing ? (3 marks)

   (b) What are the different types of audits ? (4 marks)

   (c) What is the purpose of auditing ? (3 marks)

   (d) Explain the four phases of ISMS audit program. (5 marks)

4. Answer the following :

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

(b) Why information security is important ? (3 marks)

(c) Explain IAS-octave. (6 marks)

(d) Explain why security classification for Information is important? (3 marks)

5. Answer the following : (5 marks each)

(a) What is Business continuity planning (BCP)? Why it is important?

(b) What is the purpose of Business Impact Analysis ?

(c) Write the different steps to create Business continuity plan.

Section–B

(Short-Answer-Type Questions)

Note : Section 'B' contains Eight (08) short-answer-type questions of Seven (07) marks each. Learners are required to answer any Five (05) questions only. **(5×7=35)**

1. Answer the following :

(a) Explain ISO/IEC 27002 : 2013 model. (3 marks)

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

2. Answer the following :

(a) List some of the common pitfalls of information security program. (3 marks)

(b) Explain FISMA. (4 marks)

3. Explain payment Card Industry Data Security Standard.

4. Answer the following :

(a) How do the Critical factors of ISMS? (3 marks)

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

5. Answer the following :

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

(b) Explain ISMS planning phase in details. (2 marks)

(c) What is Risk Treatment Plan? (3 marks)

6. Explain PDCA cycle in details.

7. Answer the following :

(a) Differentiate between ISO 27001 and ISO 27002. (3 marks)

(b) Explain NIST CYBER SECURITY FRAMEWORK. (4 marks)

8. Explain specific tools used in network security in details.