

PGDM, 2021-2023
Cyber Security, Ethics & Privacy
DM-481

Trimester – IV End-Term Examination: September 2022

Time allowed: 2 Hrs
Max Marks: 40

Roll No: _____

Instruction: Students are required to write Roll No on every page of the question paper, writing anything except the Roll No will be treated as Unfair Means. All other instructions on the reverse of Admit Card should be followed meticulously.

Sections	No. of Questions to attempt	Marks	Total Marks
A	Answer 4 question with internal choice with CO (Course Intended Learning Outcome) covered.	4*5	20
B	Case Study Compulsory	(6+6+8)	20
			40

Section A

Answer any 4 questions from the below

4 X 5 = 20

(Word Limit for each answer: 200 words)

Q1a. What is CIA triad in cyber security? Explain CIA triad with relevant examples. **(CO 1)**

OR

Q1b. List any 4 domains of cyber security and give a brief description of each of them. **(CO 1)**

Q2a. Explain Enterprise Risk Management (ERM) with the help of a diagram detailing the steps for conducting a risk assessment. **(CO 2)**

OR

Q2b. List any 2 ways in which insider threats can be ascertained and briefly describe the process. **(CO 2)**

Q3a. Discuss any 2 social engineering attack techniques with examples. When hackers use hackers will use deceptive emails, websites, and text messages to steal sensitive personal or organizational information from unsuspecting victims, what is it called? **(CO 4)**

OR

Q3b. It is said that Organizations should engage cyber hygiene in advance, not in response? What is cyber hygiene? Explain its importance to maintain optimal cyber security. **(CO 4)**

Q4a. What is a cyber kill chain? Why it is required in the organization Explain it with a diagram.
(CO 3)

OR

Q4b. Explain the concept of three Lines of Defence in Cyber Security in the context of governance Risk & Compliance (GRC) . Explain it with a diagram. Suppose we do not use this model what will be the impact to the organization? **(CO 3)**

Section B

Read the case and answer all questions of the case studies 6+6+8 = 20 (CO 4)

Questions

5. InstaServe Pvt Ltd offers IT outsourcing services in BFSI sector with HQ in Mumbai, India. The company has a full fledged Information Security department to handle client audits and due diligence. Of late, they have been flooded with requests for audits by their (prospective) clients (most of them are Top 50 banks in India) and the team is overwhelmed with multiple audits and as a service provider they are obligated to fulfill.

Being the head of the Information Security function, what is one key compliance they need to fulfill that would cater to these multitude of audit requests and save your company's time, effort and resources? Explain the salient features of this compliance program you have proposed. (Marks 6)

6. TalkTime Ltd is a big telecom company with headquarters in France and operations spread across Europe. As part of providing new mobile phone connections to customer, they collect personal data. Now one customer wants to withdraw consent but don't know how to go about it.

As the head of the privacy function, how would you put in place a process to enable customers to withdraw consent? Give brief description of the steps involved. (Marks 6)

7. Honest Bank Ltd is a large commercial bank based in Mumbai, India. The bank has recently decided to outsource its payroll function to GreatPay IT Services Pvt Ltd but are worried about the security controls and program they have.

As the Head of Information Security function, what key parameters (only external validation) would you look for in your due diligence of security program of outsourced vendors? List the key security posture indicators (from external compliance perspective) you would evaluate before conducting a detailed security assessment. Explain briefly what each of these assure from compliance perspective. (Marks 8)