PRESIDENCY UNIVERSITY

BENGALURU

Make Up Examinations – December 2025

Date: 26 – 12- 2025   **Time:** 1.00pm to 04.00pm

School: SOCSE	Program: B.Tech	
Course Code: CSE2060	Course Name: Information Security and Management	
Semester: MK	Max Marks: 100	Weightage: 50%

CO - Levels	CO1	CO2	CO3	CO4
Marks	26	26	24	24

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks.   **10Q x 2M=20M**

1.	Name two components of an Information System.	2 Marks	L1	CO1
2.	Define the role of a Data Custodian in information security.	2 Marks	L1	CO1
3.	List out one advantage of the top-down security approach.	2 Marks	L1	CO1
4.	State the primary mission of an information security program.	2 Marks	L1	CO2
5.	Name two functions of information security for an organization.	2 Marks	L1	CO2
6.	Define threat agent. Give one example.	2 Marks	L1	CO2
7.	State significance of continuous improvement in risk management.	2 Marks	L1	CO3
8.	State the advantage of establishing context in the RM process.	2 Marks	L1	CO3
9.	Name two biometric characteristics considered truly unique for authentication.	2 Marks	L1	CO4
10.	Define the function of a packet-filtering firewall.	2 Marks	L1	CO4

Part B

Answer the Questions.   **Total Marks 80M**

11.	a.	Describe the Security Trinity components (Prevention, Detection, Response), explain why prevention is prioritized, and provide a real-world organizational example for each component.	**10 Marks**	**L2**	**CO1**
	b.	Compare SDLC and SecSDLC by outlining their phases, highlighting two unique security activities in SecSDLC's "Analysis" and "Design" phases, and explaining why SecSDLC is more proactive.	**10 Marks**	**L4**	**CO1**
		Or			
12.	a.	Analyze two of these scenarios: a) Employee copies secured customer data; b) Hacker alters financial emails; c) Ransomware encrypts health records—for each, identify violated CIA principle(s), justify why, and propose a countermeasure.	**10 Marks**	**L4**	**CO1**
	b.	Describe NIST Approach to Secure the SDLC.	**10 Marks**	**L2**	**CO1**

13.	a.	Explain why protecting an organization's ability to function is considered the first and most important function of information security.	**10 Marks**	**L2**	**CO2**
	b.	Contrast Active Attacks (like Modification or Denial-of-Service) with Passive Attacks (like Eavesdropping or Traffic Analysis) in terms of their primary target within the CIA triad (Confidentiality, Integrity, Availability).	**10 Marks**	**L2**	**CO2**
		Or			
14.	a.	Explain why Human Error or Failure is consistently cited as one of the greatest threats to information security assets, referencing specific examples of employee mistakes.	**10 Marks**	**L2**	**CO2**
	b.	Explain how the security principle of Diversity strengthens a layered defense strategy.	**10 Marks**	**L2**	**CO2**

15.	a.	Explain how the Risk Management Plan guides the implementation of both the risk management framework and risk management process.	**10 Marks**	**L**	**CO3**
	b.	Explain the importance of classifying and categorizing information assets in the risk management program, including the use of a data classification scheme.	**10 Marks**	**L2**	**CO3**
		Or			
16.	a.	Describe the threat assessment process and how it helps in prioritizing risks to organizational information assets.	**10 Marks**	**L2**	**CO3**
	b.	Explain the qualitative and quantitative risk analysis methods, highlighting their approaches, advantages, and limitations.	**10 Marks**	**L2**	**CO3**

17.	a.	Describe the different types of firewall processing modes and their specific roles in network security.	**10 Marks**	**L2**	**CO4**
	b.	Explain the screened subnet architecture (with DMZ) and its advantages in protecting organizational networks.	**10 Marks**	**L2**	**CO4**
Or					
18.	a.	Explain the factors to consider when selecting a firewall for an organization, including cost, features, and scalability.	**10 Marks**	**L2**	**CO4**
	b.	Describe the best practices for configuring and managing firewalls to balance security and business performance.	**10 Marks**	**L2**	**CO4**