Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 17 – 12- 2025 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** IST	
Course Code: IST2000	**Course Name:** Business Continuity and Risk Analysis	
Semester: V	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	24	24	26	26	-

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.	List people included in DR team	**2 Marks**	**L1**	**CO1**
2.	Explain the objectives of short-term recovery	**2 Marks**	**L2**	**CO1**
3.	List 5 key strategies to maintain business.	**2 Marks**	**L2**	**CO2**
4.	Explain business impact analysis	**2 Marks**	**L2**	**CO2**
5.	Differentiate Qualitative vs Quantitative assessment.	**2 Marks**	**L2**	**CO3**
6.	List four steps involved in structured process of risk management.	**2 Marks**	**L1**	**CO3**
7.	Explain in brief Penetration testing	**2 Marks**	**L2**	**CO3**
8.	List the necessity of information classification	**2 Marks**	**L1**	**CO4**
9.	Describe the role of security team in system acquisition process.	**2 Marks**	**L2**	**CO4**
10.	List different levels in information classification	**2 Marks**	**L1**	**CO4**

Part B

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

11.	a.	Explain significance of DR plan with roles and responsibilities of DR team.	10 Marks	L2	CO1
	b.	Explain in detail disaster recovery objectives with examples	10 Marks	L2	CO1
		Or			
12.	a.	Explain in detail types of disaster and their effects with examples	10 Marks	L2	CO1
	b.	With neat diagram, explain the operational cycle of disaster recovery	10 Marks	L2	CO1

13.	a.	Explain any two cloud service providers for business continuity	10 Marks	L2	CO2
	b.	Scenario: Customer email IDs and limited personal data were accessed by hackers. Press Release Points: • Acknowledge the breach promptly. • Clarify exactly what type of data was (and wasn't) exposed. • Share measures taken (password resets, identity protection services). • Reassure customers about system strengthening. Draft a press release to inform public and the media. Message should be transparent, timely and reassuring.	10 Marks	L3	CO2
		Or			
14.	a.	Explain the key elements of BCP	10 Marks	L2	CO2
	b.	Apply on the given case study how Netflix uses Cloud based solution for its operations. Challenge: As a global streaming service, Netflix needed a robust business continuity strategy to ensure uninterrupted service to millions of subscribers.	10 Marks	L3	CO2

15.	a.	Out of ten ways to reduce Cybersecurity Risk for your organization, Explain employee training and IDS in detail.	10 Marks	L2	CO3
	b.	Apply the concept of risk matrix on given case study and reason out for probability, impact and mitigation strategies with risk matrix. Banking Sector – Data Breach Problem Statement: A national bank experiences repeated cyberattacks targeting customer databases and online transactions. Key Risk Factors: Weak cybersecurity controls, phishing attacks, third-party system vulnerabilities. Impact: Severe financial loss, customer data theft, and regulatory penalties.	10 Marks	L3	CO3
		Or			
16.	a.	Explain role and responsibility of IT security professionals in risk assessment process.	10 Marks	L2	CO3

	b.	Case Study: Risk Assessment in a Financial Services Firm: Organization: FinTrust Bank Ltd. – A leading private sector bank offering retail and corporate financial services across India. Background: In 2024, FinTrust Bank faced increasing cyber threats, rising non-performing assets (NPAs), and operational disruptions due to third-party IT service failures. The Board of Directors directed senior management to perform a comprehensive enterprise-wide risk assessment to identify, evaluate, and mitigate potential threats to the bank's operations, data, and reputation. Apply procedures of risk assessment for given case and determine the objectives, roles and responsibilities and outcomes.	10 Marks	L3	CO3

17.	a.	Explain in detail 5 pillars of information assurance.	10 Marks	L2	CO4
	b.	Case Study: Data Classification in a Multi-Specialty Hospital (Healthcare Domain) Background: City Care Multi-Specialty Hospital is one of the largest healthcare institutions in the region. It maintains electronic health records (EHR), billing information, diagnostic reports, administrative documents, and research data. Over the years, the volume of data has grown rapidly, and the hospital now plans to implement a formal data classification policy to improve data handling, security, and compliance with health-information regulations. Scenario: During an internal audit, it was found that several departments were storing and sharing data without proper controls: 1. The laboratory team shares blood test results via email without encryption. 2. HR stores employee attendance records and leave forms in a shared network folder accessible to all interns. 3. The billing department keeps patient payment receipts and insurance details on personal computers. 4. The research wing maintains a large dataset of anonymized patient statistics for research collaboration with universities. 5. The Emergency Department keeps a printed log of patient names and diagnosis openly on the nurse station desk. 6. Marketing uses general hospital brochures and event photos for online promotion without any restrictions. The hospital's governance board requests the IT team to analyse all information assets and classify them under standard categories such as: • Public • Internal • Confidential • Highly Confidential / Sensitive Analyse the scenario and classify each type of information into the appropriate category. Identify the classification level, justify your choice, and recommend required controls for each dataset.	10 Marks	L4	CO4

		Or			
18.	a.	Describe with an example why identifying assets and defining objectives are important steps in development of Information assurance principles and practices.	10 Marks	L2	CO4
	b.	Analyse and categorise each incident as a *standard, emergency, or major change*. Describe the required actions (documentation, approvals, testing, and rollback, post-review). Background: • Medi Core Hospitals Network operates 12 multi-specialty hospitals with centralized Electronic Health Record (EHR) systems. • Continuous availability is critical because doctors access real-time patient data for surgeries, prescriptions, and ICU monitoring. Incident Description — Impact Summary 1. A routine antivirus signature update was pushed during OPD hours and caused temporary system lags on nursing stations. — Minor slowdowns, but no patient harm reported. 2. A critical vulnerability was detected in the EHR portal, leading the security team to immediately apply a vendor emergency patch. — High urgency; system was unavailable for 20 minutes but database integrity remained intact. 3. The biomedical IT team migrated the radiology image storage server (PACS) to a new cloud platform. — Two-hour delay in diagnostic report uploads; radiology department frustrated. 4. A planned feature enhancement proposed for the hospital mobile app to include telemedicine chat and video consultation. — Requires planning, testing, approval from clinical heads. 5. A switch upgrade in the ICU network rack altered VLAN configurations unexpectedly. — Momentary disconnection of patient monitoring systems; logs captured automatically. • The CTO now mandates that all changes must be approved.	10 Marks	L4	CO4