

Name: Enrolment No:			
UPES End Semester Examination, December 2024 Semester: XI Time : 03 hrs. Max. Marks: 100 Course: Information Security Audit and Monitoring Program: BT-CSE-LLB-SPZ-CL IPR Course Code: CLCB6003 Instructions:			
SECTION A (5Qx2M=10Marks)			
S. No.		Marks	CO
Q 1	Define monitoring.	2	CO1
Q2	Differentiate between authentication and authorization in terms of security.	2	CO2
Q3	State the pillars of accountability.	2	CO3
Q4	Identify how often security audits should be performed.	2	CO4
Q5	Describe the audit trail in information security audit	2	CO1
SECTION B (4Qx5M= 20 Marks)			
Q 6	List down some factors that can cause security vulnerabilities.	5	CO3
Q7	Analyze why data protection is important with strong passwords.	5	CO5
Q8	Discuss various challenges in record retention.	5	CO2
Q9	Justify why network traffic analysis is important.	5	CO4
SECTION-C (2Qx10M=20 Marks)			
Q 10	Explain in detail various techniques of audit.	10	CO2
Q11	State the working of warning banners.	10	CO3
SECTION-D (2Qx25M=50 Marks)			
Q12	ABC suspects that one of its employees, James whose Sudo name is Smith, is a secret agent working for their competitor. James has access to the company’s prize asset, the secret code. Security staff are worried that	25	CO4

	James may try to leak the company's secret code. As a cyber security expert A) Suggest a method to investigate and control the intrusion. B) Enumerate the role of the external auditor.		
Q 13	A) Describe the auditor's roles and responsibilities in identifying information security following record retention. B) Outline the life cycle of auditing with a neat diagram.	25	CO5