Name:

Enrolment No:

UPES

End Semester Examination, December 2023

Course: Information Security Audit and Monitoring **Semester: XI**
Program: B. Com. LL.B (Hons.) **Time : 03 hrs.**
Course Code: CLCB6003 **Max. Marks: 100**

Instructions:

SECTION A
(5Qx2M=10Marks)

S. No.		Marks	CO
Q 1	Define GRC (Governance, Risk, and Compliance) in the context of cybersecurity.	**02**	**CO1**
Q 2	What is the primary objective of ISO 27001 implementation?	**02**	**CO2**
Q 3	Briefly explain the significance of PCI DSS in the payment card industry.	**02**	**CO3**
Q 4	Why is it essential to implement security regulatory requirements in organizations?	**02**	**CO2**
Q 5	What is the purpose of security assurance in the context of information security?	**02**	**CO4**

SECTION B
(4Qx5M= 20 Marks)

Q 6	Discuss the key components of a typical Governance, Risk, and Compliance (GRC) framework and explain how they contribute to overall cybersecurity management.	**05**	**CO2**
Q 7	Describe the steps involved in the implementation of the ISO 27001 standard for information security. Highlight the benefits of ISO 27001 certification.	**05**	**CO1**
Q 8	Explain the core principles of PCI DSS (Payment Card Industry Data Security Standard) and the key requirements that organizations must meet for compliance.	**05**	**CO3**
Q 9	What are the challenges organizations may face when implementing security regulatory requirements, and how can they address these challenges effectively?	**05**	**CO4**

SECTION-C
(2Qx10M=20 Marks)

Q 10	Outline the key stages of a security assurance and audit process in an organization. Explain how this process ensures the security and compliance of an organization's information systems.	**10**	**CO4**

Q 11	In the context of ISO 27001 implementation, discuss the role of risk assessment and risk management. Provide examples of potential risks that organizations should address.	**10**	**CO3**
SECTION-D **(2Qx25M=50 Marks)**			
Q 12	You are a cybersecurity consultant hired by a medium-sized e-commerce company looking to implement the PCI DSS standard. a) Develop a comprehensive implementation plan, including key steps, responsibilities, and a timeline. [15] b) Discuss the potential challenges the company may face and how to address them. [10]	**25**	**CO1**
Q 13	Imagine you are an internal auditor for a multinational corporation with a complex IT infrastructure. The company is preparing for an ISO 27001 certification audit. a) Create a detailed audit plan, including the audit scope, objectives, and the specific areas you will assess. [15] b) Explain how your audit plan aligns with ISO 27001 requirements and provides assurance of compliance. [10]	**25**	**CO2**