


Seat No.: Enrolment No. **NATIONAL FORENSIC SCIENCES UNIVERSITY**

Semester End Examination (December – 2024)
M.Sc. Digital Forensic and Information Security
(Batch 2024-26)
Semester - I

Subject Code: CTMSDFIS 24 SI P2
Subject Name: Cyber Security Audit And Compliance
Time: 02:30PM TO 05:30PM

Date: 05/12/2024

Total Marks: 100

Instructions:

1. Write down each question on a separate page.
2. Attempt all questions.
3. Make suitable assumptions wherever necessary.
4. Figures to the right indicate full marks.

		Marks
Q.1	Attempt any three.	
(a)	What Does An Organisation Do To Be In Compliance?	08
(b)	What Are The Compliance Requirement For User Domain and LAN Domain?	08
(c)	Explain Business Continuity Planning Life Cycle	08
(d)	List And Explain The Principles Of GDPR On Data Protection	08
Q.2	Attempt any three.	
(a)	Describe Adjudication Process Under Indian IT Act.	08
(b)	Describe HIPPA With its Privacy and Security Rule?	08
(c)	What Are The Key Sections Of Indian IT Act 2008?	08
(d)	How COBIT Framework Benefits The IT Industry?	08
Q.3	Attempt any three.	
(a)	What Are The Key Areas Covered In ISO/IEC 27002 Standard?	08
(b)	What If an Organization Does Not Comply with Compliance Laws?	08
(c)	Explain Certification Process Of ISO/IEC 27001 Standard.	08
(d)	What Are The Key Objectives Of PCIDSS	08
Q.4	Attempt any two.	
(a)	List And Explain The IT Audit Process	07
(b)	List And Explain Different Types Of CAATs	07
(c)	How Will You achieve CIA In Remote Access Domain? <i>How</i>	07
	<i>diag</i>	
Q.5	Attempt any two.	
(a)	Imagine you are part of the Risk Management Team at BankSecure Inc., a global bank known for its advanced online banking services. Recently, the bank experienced a surge in cyber threats, including phishing attacks, malware attempts, and unauthorized access	07

		incidents. The board of directors has asked your team to develop a complete risk management strategy to ensure the platform's security and maintain customer trust. List And Explain The Risk Assessment Strategy	
	(b)	<p>A medium-sized e-commerce company, ShopEase, heavily relies on its website for processing sales, managing customer data, and handling inventory. The company's IT infrastructure includes:</p> <ul style="list-style-type: none"> • A primary data center in Mumbai, hosting all servers and databases. • A secondary offsite data center in Delhi for backups, used only during emergencies. • A cloud storage service for incremental backups of customer data. <p>One evening, a fire in the Mumbai data center causes a complete shutdown of their primary servers, leaving the website offline. Customers are unable to make purchases, and ongoing orders are stalled. Competitors are already targeting frustrated customers with aggressive discounts.</p> <p>Identify the disaster recovery strategies ShopEase should implement to minimize downtime and data loss in this situation And Business continuation with reputation.</p>	07
	(c)	<p>A hacker gains unauthorized access to SlipCart a popular e-commerce website and alters its homepage, changing the displayed products and prices, causing reputational damage to the business. Later, the same hacker spreads a virus through the website's contact form to infect visitors' devices. Afterward, they launch a denial-of-service (DoS) attack on the website, making it unavailable for users.</p> <p>Identify the sections under the Information Technology Act, 2000 with Amendments, under which the hacker's actions are classified. For each action (website defacement, spreading viruses, and launching a DoS attack), specify the relevant section and penalties.</p>	07

--- End of Paper---

NATIONAL FORENSIC SCIENCE UNIVERSITY

Branch: MSc Cyber Security/ MSc DFIS

Sem: I

Date: 14/10/2024

Subject name: Cyber security audit and compliance

Subject code: CTMSCS SI P2/CTMSDFIS SI P2

Time: 1.5 hours

Max Marks: 50

Instructions: 1) Answer all the questions. 2) Assume suitable data.

Q1.	Solve any Four	20 marks
	I) How do Security assessment & security audit differ from each other?	5 marks
	II) Why are governance & compliance important?	5 marks
	III) What does an organisation do to be in compliance?	5 marks
	IV) What if the organisation does not comply with compliance laws?	5 marks
	V) What are we actually auditing within the IT infrastructure?	5 marks
Q2	Attempt All	15 marks
	I) What are the key aspects of Cybersecurity Audit?	5 marks
	II) List examples of security controls in IT Audit.	5 marks
	III) Explain internal-audit vs external-audit	5 marks
Q3	Attempt a and b	15 marks
Q3 a.	Attempt any one	8 marks
	I) Why are security controls important in an IT audit?	
	OR	
	II) Explain Goal-based controls & Implementation based controls with examples.	
Q3 b.	Attempt any one	7 marks
	I) Explain seven domains of typical IT infrastructure	
	OR	
	II) Discuss the steps involved in planning & implementation of IT Audit for compliance	



National Forensics Sciences University, Goa
Campus
TA-1 Examination

Program Name – M.Sc Digital Forensic & Information Security		Sem – 1
Subject Name- Cyber Security Audit & Compliance		
Subject Code- CTMSDFIS SI P2		Date- 10/09/2024
Time- 45 minutes		Max. Marks- 25
Instructions - 1) Answer all questions. 2) Assume suitable data.		
	Answer any 5 questions (5x5 marks each)	25 marks
Q 1	Explain Types of IT audit in detail.	5 Marks
Q 2	Describe how to conduct IT Audit and process of IT security audit.	5 marks
Q 3	Compare Internal audit vs External Audit.	5 marks
Q 4	List Best Practices to Perform Cyber Security Audits.	5 marks
Q 5	What is compliance and describe the importance of compliances.	5 marks
Q 6	Why are assessments and audits important?	5 marks

BEST OF LUCK