Seat No.: _____ Enrolment No. 2501030002004

NATIONAL FORENSIC SCIENCES UNIVERSITY

MSc. CS - Semester - I - Dec 2025

Subject Code: CTMSCS SI P1 **Date: 15/12/2025**

Subject Name: ECS CW Essentials of Cyber Security & Cyber Warfare.

Time: 02:00 to 05:00 PM **Total Marks: 100**

(80/85)

Instructions:

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

Q.1	**Attempt any three.**		**Marks**
	(a)	Your university's lab computers frequently get infected by USB-borne malware brought by students. As the security administrator, what steps will you take on Windows systems to reduce this risk?	**08** 7/8
	(b)	Explain the three classes of operating systems: with examples.	**08** 7
	(c)	What is a Service Pack, Hotfix and Security Patch? How do they improve Windows security?	**08**
	(d)	What is BitLocker Drive Encryption? Explain its purpose, how it protects data, and what happens if a laptop is stolen.	**08** 7/8
Q.2	**Attempt any three.**		
	(a)	You suspect a particular Windows machine in your lab is running crypto-mining malware explain in detail the scenario and how will you investigate using built-in tools?	**08**
	(b)	What is User Account Control (UAC)? How does it help in securing Windows?	**08** 6/7
	(c)	Explain the role of Process Hacker and task manager in Windows security.	**08** 7/8
	(d)	Scenario: You want to enforce a complex password policy. Describe the steps with relevant examples.	**08** 7/8
Q.3	**Attempt any three.**		
	(a)	What is Linux service hardening? Why is it important for security?	**08** 6.5/7
	(b)	Explain how syslog works. What are its components?	**08** 6
	(c)	What is a host-based firewall? Explain **iptable** in detail.	**08** 7
	(d)	What is Registry? Explain its types in detail.	**08**
Q.4	**Attempt any two.**		
	(a)	Define Cyber Warfare. How is it different from cybercrime?	**07** 6.5/7
	(b)	Explain types of Cyber Warfare operations.	**07**

P.T.O

	(c)	Your web server is running many unused services. How would you harden it to reduce attack surface?	07

Q.5 Attempt any two.

	(a)	What are Psychological Operations (PSYOPS)?	07
	(b)	Scenario: How can misinformation campaigns affect national stability? Suggest countermeasures.	07
	(c)	Explain the difference between Information Warfare and Cyber Warfare.	07

END OF PAPER

Seat No.: _____ Enrolment No. 250103002004

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Cyber Security - Semester - I - December-2025

Subject Code: CTMSCS SI P2 **Date: 16/12/2025**

Subject Name: Cyber Security Audit and Compliance

Time: 2.00 PM TO 5.00 PM

Total Marks: 100

Instructions:

1. **Write down each question on 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)	Differentiate between an IT Security Assessment and an IT Security Audit. Explain how each contributes to organizational security posture.	08
(b)	Explain the processes of risk analysis, risk identification, risk assessment, risk response, risk mitigation, and risk reporting in IT risk management.	08
(c)	Discuss the role of Computer-Assisted Audit Techniques (CAATs) in modern auditing.	08
(d)	A retail company wants to strengthen its IT security by implementing goal-based and implementation-based security controls. Provide a plan for formulating, developing, and implementing these controls, ensuring they align with the company's security architecture design.	08
Q.2	**Attempt any three.**	
(a)	Describe the importance of IT governance and compliance in an organization. Explain the consequences of noncompliance with regulatory laws and standards.	08
(b)	Evaluate compliance issues within the LAN-to-WAN and WAN domains. How do penetration testing and configuration validation support compliance?	08
(c)	Differentiate between preventive, detective, and corrective controls, providing practical examples of each.	08
(d)	Explain how to identify critical audit requirements. Outline the steps in assessing IT security and obtaining necessary audit information, documentation, and resources.	08
Q.3	**Attempt any three.**	
(a)	Discuss Business Continuity Planning (BCP) and Disaster Recovery (DR) planning comprehensively.	08

(b) Discuss compliance requirements and business drivers within the User Domain and Workstation Domain. How can organizations maximize confidentiality, integrity, and availability (CIA) in these domains? 08

(c) Explain the importance of identifying and testing monitoring requirements. How do monitoring controls strengthen compliance? 08

(d) An e-commerce organization is concerned about determining its acceptable risk levels. As an IT auditor, guide the organization in defining appropriate security baseline definitions for three critical areas: (a) the online platform, (b) the payment gateway, and (c) the customer database. Explain how these baselines help in managing compliance and risk. 08

Q.4 **Attempt any two.**

(a) Define the scope of an IT compliance audit. What factors influence scope definition, and why is scope critical for audit success? 07

(b) What is a multitiered governance and control framework? Describe its typical layers or tiers. 07

(c) Compare and contrast ISO/IEC 27001/27002 with COBIT. Discuss their objectives, scope, and how each framework supports IT governance and compliance in organizations. 07

Q.5 **Attempt any two.**

(a) Discuss compliance and security concerns within the Remote Access Domain and the Application Domain. Explain application server vulnerability management and patch management. 07

(b) Describe the steps involved in writing a comprehensive IT infrastructure audit report. What are the key components and recommended structure? 07

(c) A multinational healthcare provider operates in both the United States and Europe. As the compliance officer, compare HIPAA and GDPR in terms of how they address data protection, privacy requirements, and compliance obligations. 07

END OF PAPER

Seat No.: _____ Enrolment No._____

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (December - 2025)
M.Sc. Cyber Security - Semester - I

Subject Code: CTMSCS SI P3 **Date: 17/12/2025**
Subject Name: Web Application Security
Time: 2.00 PM TO 5.00 PM **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 is Virtual Hosting? Describe different ways to implement virtual Hosting with its Advantages and Disadvantages.	08
(b)	What are HTTP Cookies? Describe how to manage a session using cookies. Also, explain the Security Considerations associated with cookies.	08
(c)	Describe the OSI Model. Give detailed information on the protocols that are used at the Transport Layer and the Application Layer.	08
(d)	What is Fingerprinting of the Web Server? What different Information can you retrieve in this activity, and how will it be helpful in VAPT? Also explained the various tools used for the same purpose.	08
Q.2	**Attempt any three.**	
(a)	Describe the Attack Lifecycle. Describe the different approaches to perform the VAPT.	08
(b)	How is Threat Modelling applied in the Secure Development Life Cycle of the Software? Describe the STRIDE threat modelling in detail.	08
(c)	Explain CWE (Common Weakness Enumeration) in detail. How does it help in VAPT?	08
(d)	Describe CVE and CVSS in detail.	08
Q.3	**Attempt any three.**	
(a)	What is the difference between Cross-Site Request Forgery and Server-Side Request Forgery? Explain in detail.	08
(b)	What is the difference between File Inclusion and File Upload vulnerabilities? What are all the possible impacts on the web application for these vulnerabilities?	08

(c) Describe the different Types of SQL Injection. What are all the different ways to identify whether SQL Injection will work or not? What is the possible mitigation to avoid SQL Injection attacks? 08

(d) What is Username harvesting and password guessing? How can you perform a brute-force attack to bypass the authentication using any proxy server? Describe in detail. 08

Q.4 **Attempt any two.**

(a) What is serialization and deserialization? Describe Insecure deserialization vulnerabilities in detail. 07

(b) What are command injection vulnerabilities? If it is found, describe possible impacts; it may create on the web application and server. 07

(c) Explain Logging and Security Misconfiguration in Detail. 07

Q.5 **Attempt any two.**

(a) What are all the different types of API used in Web applications? What all are possible attack surfaces for the API? 07

(b) Explain CMS and Docker in detail. 07

(c) What is Insecure Direct Object Reference (IDOR)? How this vulnerabilities impact on any web application. 07

END OF PAPER

Seat No.: _____ Enrolment No. 2501030002004

NATIONAL FORENSIC SCIENCES UNIVERSITY

M. Sc. Cyber Security - Semester - I – December - 2025

Subject Code: CTMSCS SI P4 **Date: 19.12.2025**

Subject Name: ARTIFICIAL INTELLIGENCE

Time: 2.00 PM TO 5.00 PM

Total Marks: 100

Instructions:

1. **Write down each question on 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)	Write a Python program to generate the Fibonacci series using both recursion and iterative (loop-based) methods.	08
(b)	Consider the following series: 5,7,9,9,10,12,15 for calculating mean, median, mode and standard deviation.	08
(c)	Discuss the different types of Regression algorithms with appropriate examples.	08
(d)	Explain the role of Machine Learning (ML) in cybersecurity and discuss any two of its applications with suitable examples.	08
Q.2	**Attempt any three.**	
(a)	Explain the different types of learning in artificial intelligence with examples	08
(b)	Write a python program to find all the prime numbers which are less than 25.	08
(c)	Explain Object Detection and Image Segmentation in Computer Vision. Provide examples and use cases for both.	08
(d)	Using the below dataset, demonstrate how the K-Nearest Neighbors (KNN) algorithm predicts a new class label X(3,2) with K value = 3. Explain each step of the calculation in detail.	08

Point	x	y	Class
A	1	1	Blue
B	2	2	Blue
C	3	1	Red
D	6	5	Red
E	7	7	Red

Q.3 **Attempt any three.**

(a) Explain the Support Vector Machine (SVM) algorithm in detail and discuss the key terminologies such as hyperplane, margin, and support vectors. **08**

(b) Calculate the precision, recall and accuracy using the given confusion matrix **08**

	Predicted Positive (PP)	Predicted Negative (PN)
Actual Positive (AP)	45	15
Actual Negative (AN)	10	30

(c) List various Social Engineering threats relevant to Cyber Security and explain each with examples. **08**

(d) Explain Natural Language Processing (NLP) in detail and describe the different phases involved in NLP. **08**

Q.4 **Attempt any two.**

(a) Explain the differences among Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) in detail. **07**

(b) Explain the various performance metrics used for evaluating Machine Learning models. **07**

(c) Explain the working principle of a Perceptron along with its architecture. Illustrate the concept with an example. **07**

Q.5 **Attempt any two.**

(a) List and explain different types of Activation Functions used in Neural Networks with illustrative diagrams. **07**

(b) Explain ML-based Anomaly Detection in Cyber Security with suitable examples. **07**

(c) Explain the concepts of underfitting and overfitting in machine learning. How do they affect model performance? Illustrate your answer with suitable examples. **07**

END OF PAPER

Seat No.: _____ Enrolment No. 25 0103002004

NATIONAL FORENSIC SCIENCES UNIVERSITY

M. Sc. Cyber Security - Semester - I – December -2025

Subject Code: CTMSCS SI P5 **Date: 22.12.2025**

Subject Name: Introduction to Forensic Science and Laws

Time: 2.00 PM TO 5.00 PM

Total Marks: 100

Instructions:

1. **Write down each question on 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)	Define the seven basic principles of forensic science and provide one example for each principle demonstrating its application in crime investigation.	08
(b)	Design a comprehensive forensic report writing template that incorporates best practices for a more effective report.	08
(c)	Discuss the role of CCTNS in modernizing police investigations in India, including its features and impact on criminal justice.	08
(d)	In a rape investigation case, describe the complete procedure for medical examination of the victim under Section 184 of BNSS, including documentation requirements and forensic importance.	08
Q.2	**Attempt any three.**	
(a)	Analyze the differences between electronic signatures and digital signatures in terms of technology, security, legal validity, and authentication mechanisms. Why is digital signature preferred in legal proceedings?	08
(b)	Compare cognizable vs. non-cognizable offences and bailable vs. non-bailable offences. Explain the implications for police investigation and accused's rights in each category.	08
(c)	Examine the provisions of the Digital Personal Data Protection Act 2023, evaluating its effectiveness in protecting individual privacy while balancing organizational data processing needs.	08
(d)	Design a comprehensive forensic science laboratory protocol for digital crime scene investigation, incorporating chain of custody procedures, evidence preservation, and report writing standards.	08

Q.3 **Attempt any three.**

(a) Distinguish between murder, culpable homicide, and negligent death under BNS, including punishment provisions for each. 08

(b) Enumerate the essential elements of cyber ethics and explain how each principle guides ethical conduct of cybersecurity professionals. 08

(c) Explain the hierarchy of Indian courts and describe the jurisdiction and powers of each level. 08

(d) Discuss the functions and organizational structure of the Directorate of Forensic Science Services (DFSS) and its role in criminal justice delivery. 08

Q.4 **Attempt any two.**

(a) A First Information Report (FIR) is registered in a theft case. Explain the procedure for FIR registration under BNSS and discuss the forensic importance of timely and accurate FIR filing. 07

(b) Apply the procedures for Section 176 (Procedure for Investigation) and Section 329 (Reports of Government Scientific Experts) BNSS in a hypothetical criminal case involving scientific evidence. 07

(c) Analyze the concept of mens rea and actus reus in criminal law. How do these two elements work together to establish criminal liability? Provide examples for different criminal offences. 07

Q.5 **Attempt any two.**

(a) Differentiate between examination-in-chief, cross-examination, and re-examination of witnesses under the Bharatiya Sakshya Adhiniyam 2023, including their purposes and procedural rules. 07

(b) Evaluate the effectiveness of INTERPOL notices in international crime prevention and investigation. Critically examine the advantages and potential misuse of RED notices in particular. 07

(c) Analyze the classification of cyber crimes under the Information Technology Act 2000, examining specific sections (66-72) and their applicability to emerging cyber threats. 07

END OF PAPER