



# **DELHI SCHOOL OF BUSINESS**

By Vivekananda Institute of Professional Studies - TC

**PGDM / PGDM (FINTECH) Program**

**TRIMESTER - VI (Batch: 2023-25)**

**END-TERM EXAMINATION, APRIL 2025**

<b>Course Name</b>	<b>Cyber Security Techniques &amp; Laws</b>	<b>Course Code</b>	
<b>Duration</b>	<b>Three Hours</b>	<b>Max. Marks</b>	<b>60</b>

## **Instructions:**

1. Read each question carefully and answer concisely.
2. For scenario-based questions, provide logical explanations and real-world examples where applicable.
3. Ensure clarity in responses, especially for regulatory and compliance-related questions.
4. Marks are indicated alongside each question.

### **Q1. Explain all the following. (3x2 = 6 marks)**

- I. What is the significance of cybersecurity in the financial sector?
- II. Define phishing and explain how it impacts financial institutions.
- III. What are FinTech-specific attack vectors?  
Provide an example

### **Q2. Explain all the following. (3x2 = 6 marks)**

1. Define GDPR and its importance in financial cybersecurity.
2. What is the role of HIP PA?
3. Explain one compliance requirement for FinTech companies.

### **Q3. Explain all the following (3x4 = 12 marks)**

1. What are the key cyber threats faced by FinTech companies?

2. Explain the process of incident response and recovery planning.
3. How can security controls be effectively applied in financial institutions?

Q4. Explain how compliance with cybersecurity laws helps in risk management for financial institutions. (6 marks)

Q5. Answer all parts (2x4 = 8 marks)

1. What is encryption, and why is it crucial in financial transactions?
2. Explain authentication and access control methods used in FinTech cybersecurity.

Q6. Answer all parts (2x4 = 8 marks)

1. What is SIEM, and how does it help in financial cybersecurity?
2. Why are cybersecurity training and awareness programs essential for financial employees?

Q7. Your financial organization has detected a ransomware attack that threatens to encrypt all customer transaction data. As a cybersecurity expert, explain the immediate and long-term actions you would take to contain and mitigate the attack. (7 marks)

Q8. Attempt any **ONE** of the following (7 marks)

Your FinTech company is expanding globally. How would you ensure compliance with different cybersecurity regulations (GDPR, PCI DSS) while maintaining security best practices?

**OR**

A customer's banking credentials were compromised due to weak authentication. As a security manager, what measures would you implement to strengthen authentication and prevent future breaches?