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

Course Name	**Cyber Security in Fintech**	**Course Code**	
Duration	**Three Hours**	**Max. Marks**	**60**

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.**

Section A (CO: 01-03)

Q1. Explain the importance of the CIA Triad in cybersecurity. How does it apply to FinTech companies? **(2 marks)**

Q2. Define phishing and explain why financial institutions are common targets of phishing attacks. **(2 marks)**

Q3. Identify the key compliance requirements under GDPR that FinTech companies must follow? **(2 marks)**

Q4. Risk assessment is crucial in cybersecurity. Elaborate the statement. List any two methods used for risk assessment. **(2 marks)**

Q5. Explain the role of encryption in securing financial transactions. **(2 marks)**

Q6. Interpret the SIEM system. How does it help financial institutions in cybersecurity? **(2 marks)**

Q7. Define multi-factor authentication (MFA) and explain its role in preventing unauthorized access. **(2 marks)**

Q8. Is ransomware a cyberattack? How can financial institutions protect themselves against it? Explain. **(2 marks)**

Q9. Describe the importance of cybersecurity policies in financial organizations. **(2 marks)** Q10. Explain the significance of incident response planning for financial institutions. **(2 marks)**

Section B (CO: 04)

Q11. Apprise the common security controls implemented in FinTech companies? **(3 marks)**

Q12. What is social engineering in cybersecurity, and why is it a major concern for FinTech companies? **(3 marks)**

Q13. A bank experiences a sudden increase in fraudulent transactions. Explain how cybersecurity risk management could help mitigate such incidents. **(3 marks)**

Q14. Explain the role of data protection and privacy laws in safeguarding customer information in FinTech. **(3 marks)**

Q15. A startup is planning to expand IN Europe. What cybersecurity regulations should they consider, and why? **(3 marks)**

Q16. “Continuous monitoring can improve the security posture of a financial organization”. Explain with suitable examples. **(4 marks)**

Q17. Explain the differences between proactive and reactive cybersecurity approaches with relevant FinTech examples. **(4 marks)**

Section C (CO: 05)

Q18. Discuss the importance of employee training and awareness programs in preventing cyber threats. **(5 marks)**

Q19. Case Study: As the Chief Information Security Officer (CISO) of SecurePay Bank, you discover that a sophisticated phishing attack has compromised customer login credentials. Multiple customers report unauthorized transactions, and the bank's reputation is at risk.
Cybercriminals used fake emails posing as bank representatives to deceive customers into revealing sensitive information. **(4x3= 12 marks)**

- What are the first three actions you would take as the CISO to contain the phishing attack and limit further damage?

- How would you communicate with affected customers to ensure transparency while preventing panic?
- What security measures would you implement to protect compromised accounts and prevent attackers from exploiting stolen credentials?
- What long-term strategies and security policies should be enforced to reduce the risk of future phishing attacks on the bank and its customers?