Graphic Era HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

Mid Term (Odd) Semester Examination November 2025

Roll no.....

Name of the Course and semester: B.Tech , Vth
Name of the Paper: Security Audit and Compliance
Paper Code: TCS-595
Time: 1.5 Hour Maximum Marks: 50

Note:
(i) All the questions are compulsory.
(ii) Answer any one question from a and b
(iii) Total marks for each question is 10 (twenty).
(iv) Each sub-question carries 10 marks.

Q1. (1X10=10 Marks)

a. Define the terms **Netizen, Security Hole, Security Patch**, Hackers, Hacker's Tools, and Online Reputation Attacks. Explain the difference between **white-hat, grey-hat, and black-hat hackers** with suitable Examples. (CO1)

OR

b. Based on the Scenario above, answer the following:

a) Identify and explain at least four types of malware involved in the attack (e.g., ransomware, trojan, rogue software, keylogger, botnet, etc.).
b) Explain how social engineering enabled this attack and which psychological principles were exploited.
c) Describe the spread mechanism inside the organization.
d) Recommend five preventive cybersecurity measures that could have stopped or minimized the attack. (CO1)

Q2. (1X10=10 Marks)

a. What is Social Engineering? Describe techniques such as **Phishing, Spear-phishing, Cyberstalking, Cyberbullying, Spoofing, and SPAM/SPIM**. Explain how attackers exploit human behaviour and how individuals can protect themselves. (CO1)

OR

b. What is a **Security Hole and a Security Patch**? Explain how unpatched systems are exploited by Attackers with real-world examples (e.g., **WannaCry attack**). (CO1)

Q3. (1X10=10 Marks)

a. Explain the Information **Security Standards including ISO 27001, NIST Framework, GDPR, HIPAA, and SOX**. Compare their objectives and importance in modern organizations. (CO2)

OR

b. Discuss the importance of **Intellectual Property Rights (IPR)** in Cybersecurity. Explain Copyright Law, Patent Law, and Software Licensing with examples, and describe how violations of IPR create cybersecurity risks. (CO2)

Q4. (1X10=10 Marks)

a. A Healthcare Technology company stores patient data such as medical history, identity details, and payment records. Recently, the company faced a massive data breach because:

- Sensitive data was not encrypted.
- A contractor was found downloading patient records to an external drive.
- The company had no data **classification policy**.
- No one was assigned the role of **Data Protection Officer (DPO).**
- Audit logs were turned off due to "**storage optimization.**"
- The company operates in India but also has customers in Europe and the USA.

(CO2)

OR

b. Based on the scenario above, answer the following:

a) Which **Cyber Laws and Compliance Regulations** are violated? Discuss at least 4 (e.g., **GDPR, HIPAA, IT Act 2000, ISO 27001**, etc.).
b) Explain the ethical violations involved in handling patient data.
c) Identify the missing security governance and enterprise roles that should have prevented this breach.
d) Recommend six policy and compliance measures the company must adopt to meet legal and ethical standards. (CO2)

Q5. (1X10=10 Marks)

a. Describe the **IT Act 2000** and its major provisions related to cybercrimes in India. Explain cyber offenses such as identity theft, unauthorized access, cyber fraud, publishing obscene content, and digital signature misuse. (CO2)

OR

b. A Mid-sized company notices unusual activity in its internal network. Employees report the following incidents:

- Their computers have become extremely slow.
- Several systems display a fake antivirus warning asking users to "**Pay to Clean Threats.**"
- Files are silently encrypting themselves, and a message pops up demanding Bitcoin Payment.
- One employee admits clicking on an email link titled "Salary Revision – **Click to View Document**".
- Multiple systems are generating abnormal outbound traffic, suggesting communication with an unknown external server.
- Passwords typed on some systems were later found misused by attackers

(CO1)