



## Term Evaluation Theory (Even) Semester Regular Examination February 2026

Roll no.....

Name of the Course: BTech

Semester: VI

Name of the Paper: *Security Audit & Compliance- II*

Paper Code: TCS - 695

**Time: 1.5 hour**

**Maximum Marks: 50**

**Note:**

- (i) Answer all the questions by choosing any one of the sub-questions
- (ii) Each question carries 10 marks.

**Q1.**

**(10 Marks)**

a. Explain the Zero Trust Security Model in detail. How does it differ from the traditional perimeter-based security architecture? Illustrate your answer with a real-world enterprise implementation example, and draw a diagram showing how Zero Trust enforces continuous authentication and authorization.  
[CO1]

**OR**

b. Describe the Public Key Infrastructure (PKI). Explain its use in SSL/TLS communication, Digital Signature, and Digital Certificate, and discuss how they ensure authenticity.  
[CO1]

**Q2.**

**(10 Marks)**

a. Differentiate between the OSI Model and the TCP/IP Model with the help of a neat comparison table. Also, explain the concept of logical addressing at the Network Layer.  
[CO1]

**OR**

b. Discuss the major web security threats, including SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and session hijacking. Explain the security measures and best practices that can be implemented to secure web applications.  
[CO1]

**Q3.**

**(10 Marks)**

a. Explain the ITU Security Architecture and its key components. Discuss how ITU standards, such as X.800 and X.805, assist in designing secure communication networks.  
[CO1]

**OR**

b. Evaluate the role of Next Generation Firewalls (NGFWs) in defending against modern threats such as encrypted malware traffic and lateral movement attacks.  
[CO2]



**Term Evaluation Theory (Even) Semester Regular Examination February 2026**

Q4.

(10 Marks)

a. Consider a scenario where an organization is under a DDoS attack.

Explain how IDS/IPS, Firewall rules, and Rate-Limiting VPN gateways work together to mitigate the attack.  
[CO2]

OR

b. Define a firewall, explain its primary purpose in network security, and compare a Packet Filtering Firewall with an Application Layer Firewall by listing any three differences.

[CO2]

Q5.

(10 Marks)

a. Explain the concept of a VPN and its importance in secure communication. Discuss the types of VPNs, including Remote Access and Site-to-Site, with practical examples.

[CO2]

OR

b. Explain the working of IPSec and its two modes (Tunnel and Transport). Discuss SSL/TLS VPN and compare it with IPSec VPN.  
[CO2]