

061206T4CYB

CYBER SECURITY LEVEL 6

SEC/OS/CS/CR/04/6

BUILD SECURE NETWORK

March/April 2026



**TVET CURRICULUM DEVELOPMENT, ASSESSMENT AND CERTIFICATION
COUNCIL (TVET CDACC)**

WRITTEN ASSESSMENT

Time: 2 HOURS

INSTRUCTIONS TO CANDIDATE

1. This paper consists of **TWO** sections: **A** and **B**.
2. Answer **ALL** questions in section A and **ANY THREE** (3) questions in section B
3. Marks for each question are indicated in the brackets.
4. Candidates are provided with a separate answer booklet
5. Do not write on the question paper.

*This paper consists of **THREE** (3) printed pages
Candidate should check the question paper to ascertain that all pages
are printed as indicated and that no questions are missing.*

SECTION A (40 MARKS)

Attempt ALL the questions in this section.

1. A county data centre supports multiple online public services that experience congestion during peak access hours. Outline FOUR network design considerations that improve availability and bandwidth efficiency. (4 marks)
2. A manufacturing company interconnects its head office and factory sites over untrusted networks. State FOUR ways encrypted tunnel-based connections protect data in transit. (4 marks)
3. Network perimeters are deployed to control traffic flow between trusted and untrusted zones. Identify FOUR functions of a network security perimeter. (4 marks)
4. Organizations must understand the risks facing their networks before implementing security solutions. List THREE network threats organizations are likely to face. (3 marks)
5. After a security audit, an organization reviews its existing controls. Outline THREE factors that should be considered when reviewing network security issues. (3 marks)
6. Selecting appropriate protection mechanisms is critical for effective network defense. List FOUR security control measures used to safeguard network infrastructure. (4 marks)
7. Industry standards guide the secure exchange of information across networks.
 - a) Identify THREE network security protocols commonly used to secure data transmission. (3 marks)
 - b) Highlight THREE purposes of using standardized network security protocols in ensuring secure, interoperable, and compliant data transmission. (3 marks)
8. Before deploying a defense solution, organizations must evaluate several factors. Outline FOUR factors to consider when acquiring Unified Threat Management (UTM) devices. (4 marks)
9. Internal network devices must be properly configured to support organizational security objectives. Identify FOUR types of internal network devices commonly found in enterprise networks. (4 marks)
10. Monitoring and documentation are essential parts of network security management. Outline FOUR ways in which security monitoring reports contribute to the effectiveness of an organization's security posture. (4 marks)

SECTION B (60 MARKS)

Answer Any THREE Questions in This Section

11. Security monitoring systems face challenges as attackers design techniques to avoid detection, reducing the effectiveness of traditional monitoring tools.
- a) Describe THREE techniques attackers use to avoid detection by network monitoring systems. (6 marks)
 - b) Analyze THREE factors that may cause monitoring systems to generate incorrect alerts. (6 marks)
 - c) Evaluate FOUR methods organizations can adopt to strengthen detection accuracy and resilience of monitoring systems. (8 marks)
12. Organizations increasingly rely on centralized security platforms to manage large volumes of security data generated across the network.
- a) Describe FOUR advantages of aggregating and correlating security logs from multiple sources. (8 marks)
 - b) Explain THREE benefits of continuous security monitoring for maintaining a strong security posture. (6 marks)
 - c) Explain THREE ways structured security reporting improves incident response and decision-making. (6 marks)
13. Ensuring dependable data transfer is a critical requirement in enterprise and wide-area networks.
- a) Explain THREE techniques used by transport-layer protocols to ensure accurate and ordered data delivery. (6 marks)
 - b) Describe THREE network-related conditions that can negatively impact reliable data transmission. (6 marks)
 - c) Analyze FOUR strengths of congestion control mechanisms in modern high-speed networks. (8 marks)
14. A financial institution has deployed cloud-based banking and customer management systems and plans to enforce stronger user authentication controls.
- a) Explain FIVE ways enhanced authentication mechanisms improve the protection of cloud-hosted financial data. (10 marks)
 - b) Describe FIVE organizational benefits gained from implementing access control and identity management. (10 marks)

THE END