

061206T4CYB

CYBERSECURITY TECHNICIAN LEVEL 6

SEC/OS/CS/CR/06/6

Secure Software Application

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 this question paper.

*This paper consists of **THREE** (3) printed pages.*

*Candidates should check the question paper to ascertain that all the pages
are printed as indicated and that no questions are missing*

SECTION A (40 Marks)

Attempt ALL questions in this section.

1. Different software systems require specialized tools for effective operation and management. Identify FOUR tools commonly used in managing software systems. (4 marks)
2. A learning institution requires different software to support administration and teaching activities. List FOUR software applications. (4 marks)
3. Organizations monitor ICT logs to detect unusual or unauthorized activities. Differentiate between system logs and security logs. (4 marks)
4. Software security assessments normally follow national and international standards.
 - a) State TWO reasons why adhering to international standards is important in assessing software security (2 marks)
 - b) List TWO widely recognized international standards used in software security assessments. (2 marks)
5. John, a SOC Analyst, completed a software security test and shared the report with stakeholders. Explain TWO reasons timely report sharing is important in organizational security. (4 marks)
6. A technician ensures that software installations are properly licensed and configured. Highlight FOUR benefits of maintaining proper licensing and configuration compliance. (4 marks)
7. An organization is assessing its information systems using the NIST Cybersecurity Framework. List FOUR sequential steps in applying the framework. (4 marks)
8. Organizations must install security updates and patches in line with manufacturer guidelines.
 - a) State TWO reasons for performing regular updates and patches. (2 marks)
 - b) List TWO potential risks an organization faces if updates and patches are neglected. (2 marks)
9. Organizations implement monitoring systems to protect data and IT infrastructure. State FOUR types of monitoring systems used in Security Operation Centre. (4 marks)
10. Organizations use various software, some of which may be authorized while others are unauthorized. Distinguish between authorized software and unauthorized software. (4 marks)

SECTION B (60 marks)

Attempt THREE Questions in this Section.

11. A software development company must evaluate applications for vulnerabilities, compliance and performance.
- a) Describe FOUR categories of tools that can be used to assess software security. (8 marks)
 - b) Analyze THREE benefits of evaluating software for security compliance and performance. (6 marks)
 - c) Explain THREE reasons why vulnerability assessments are critical in maintaining software security. (6 marks)
12. An organization manages sensitive data using various software applications. Network security administrator must harden these applications to minimize risks.
- a) Describe FIVE practical techniques for hardening software applications to enhance security. (10 marks)
 - b) Explain FIVE benefits of applying software hardening measures. (10 marks)
13. Organizations require comprehensive reports to monitor and improve software security.
- a) Describe FOUR elements that must be included in a software security report. (8 marks)
 - b) Explain THREE types of software security reports used in organizations. (6 marks)
 - c) Analyze THREE ways reports help management strengthen software security policies. (6 marks)
14. Continuous monitoring of software applications is essential for threat detection and prevention.
- a) Describe FOUR methods for monitoring and reviewing system activities in a secure software environment. (8 marks)
 - b) Explain THREE types of security threats that can be identified through system monitoring (6 marks)
 - c) Evaluate THREE ways in which logs contribute to detecting security threats (6 marks)

THE END