

061206T4CYB

CYBER SECURITY TECHNICIAN LEVEL 6

SEC/OS/CS/CR/02/6

Demonstrate Understanding of Security Laws, Policies and Regulations

March/April 2026



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

WRITTEN ASSESSMENT

INSTRUCTIONS TO CANDIDATE

1. This paper consists of **TWO** sections: **A** and **B**.
2. Answer **ALL** questions in Section A, Question 12 in Section B, and **ANY TWO (2)** other 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 FIVE(5) printed pages
Candidates 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 government website lets people upload scanned copies of their ID cards and school certificates. State THREE security problems with this upload system that could put people's personal information at risk. (3 marks)
2. A supermarket chain's loyalty program app experiences a breach where customer purchase history and phone numbers are leaked. List FOUR potential violations of consumer protection and privacy laws stemming from this incident. (4 marks)
3. A consulting firm with remote employees across East Africa is implementing a 'Work From Anywhere' model. State FOUR specific policy controls it must enforce on employee-owned laptops to safeguard client confidential data. (4 marks)
4. A Kenyan agricultural export company uses a logistics platform hosted on servers in the European Union to track shipments. Name THREE regulatory considerations it must address regarding this international data flow. (3 marks)
5. A popular betting company in Kenya suffers repeated Distributed Denial of Service (DDoS) attacks during major sporting events. Outline THREE specific mandates or advisories from national regulatory bodies that could guide its cyber defense strategy. (3 marks)
6. The rapid growth of mobile money (M-Pesa) and digital banking in Kenya has revolutionized financial inclusion. Name THREE negative socio-economic consequences that could arise from a widespread, coordinated attack on these platforms. (3 marks)
7. The Communications Authority of Kenya (CA) is enhancing its national cybersecurity infrastructure. Outline FOUR critical technological components required to establish a functional Security Operations Centre (SOC) for national threat monitoring. (4 marks)
8. A Pan-African telecommunications operator headquartered in Nairobi must demonstrate compliance across multiple jurisdictions. State FOUR methods it could use to evaluate its alignment with Kenya's Computer Misuse and Cybercrimes Act and related Data Protection regulations. (4 marks)

9. A private university developing a cybersecurity policy for its new e-learning platform must consider external influences. List THREE external entities that would play a role in shaping the policy's adequacy. (3 marks)
10. An insurance company is undergoing a mandatory ICT governance audit. Identify THREE concrete evaluation measures an auditor would use to assess the company's compliance with the statutory requirement to report cybersecurity incidents. (3 marks)
11. The implementation of a new Data Loss Prevention (DLP) system is a complex, multi-phase project. State THREE reasons why adhering to a strict, phased rollout schedule is critical for the project's overall success and organizational adoption. (3 marks)
12. A manufacturing company introduces 24/7 security monitoring for its industrial control systems (ICS) and corporate network. Outline THREE ways this continuous monitoring will change the dynamics between the IT staff (people), incident response procedures, and the technology stack itself. (3 marks)

SECTION B: 60 MARKS

Attempt Question 12 and any other TWO from this section.

13. The Kenyan healthcare sector is rapidly adopting digital records and telemedicine, increasing exposure to cyber threats such as ransomware and data breaches. Hospitals must comply with the Data Protection Act and healthcare regulations.
- a) Explain FIVE operational and reputational risks a hospital faces if it fails to comply with data security laws. (10 marks)
 - b) Describe FIVE benefits of Cybersecurity compliance in protecting patients and maintaining essential medical services. (10 marks)
14. In today's connected business world, a cybersecurity policy is a key governance tool, not just an IT document. A weak or outdated policy can expose an organization to serious strategic, financial, and legal risks.
- a) Explain THREE cybersecurity policy components that help manage third-party risks. (6 marks)
 - b) Describe THREE organizational challenges that affect the successful implementation and enforcement of a cybersecurity policy. (6 marks)
 - c) Suggest FOUR practical ways to keep a cybersecurity policy up to date with new technologies and threats. (8 marks)
15. New technologies such as cloud computing, IoT, and AI are regularly adopted faster than security policies are updated, creating gaps in cybersecurity governance.
- a) Explain FIVE challenges faced when applying traditional, perimeter-based cybersecurity policies to modern, cloud-based and decentralized systems. (10 marks)
 - b) Describe FIVE strategic actions an organization can take to create flexible cybersecurity policies that support innovation while maintaining security. (10 marks)
16. Failure to comply with cybersecurity directives from the Central Bank of Kenya (CBK) can have serious consequences for financial institutions, including reputational damage, operational disruption, and regulatory sanctions.
- a) Explain THREE risk factors that can create gaps in an institution's compliance posture. (6 marks)
 - b) Describe THREE ways a known compliance problem can affect long-term strategic

planning within the organization.

(6 marks)

- c) Evaluate FOUR proactive measures organizations can adopt to reduce non-compliance. (8 marks)

THE END