

061205T4CYB

CYBER SECURITY LEVEL 5

SEC/OS/CS/CR/07/5/A

CONDUCT CYBER SECURITY ASSESSMENT AND TESTING

Nov. / Dec. 2023



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

WRITTEN ASSESSMENT

Time: 3 Hours

INSTRUCTIONS TO CANDIDATES

Maximum marks for each question are indicated in brackets ().

*This paper consists of **THREE** sections: A, B and C.*

Answer questions as per instructions in each section.

You are provided with a separate answer booklet.

Answer the questions in English

This paper consists of SEVEN (7) 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: (20 Marks)

Answer ALL the questions in this section.

1. Which of the following best describes the primary source for determining the types of information required in line with industry best practices?
 - A. Company's financial statements
 - B. Industry standards and regulations
 - C. Internal employee preferences
 - D. Social media trends
2. When establishing an organization's operation platform in line with industry best practices, which of the following is a key consideration?
 - A. The organization's preferred color scheme for branding.
 - B. Adherence to industry-specific standards and best practices.
 - C. The CEO's personal hobbies and interests.
 - D. The availability of the latest mobile devices for employees.
3. Which of the following protocols is commonly used in service and protocol enumeration to identify open ports and services?
 - A. TCP/IP
 - B. HTTP
 - C. SNMP
 - D. Nmap
4. Why is information gathering and reconnaissance an essential phase in cybersecurity assessments?
 - A. To directly exploit vulnerabilities.
 - B. To determine the scope of the assessment.
 - C. To install security patches.
 - D. To encrypt sensitive data.
5. What is the primary purpose of service enumeration in a cyber-security assessment?
 - A. To identify potential vulnerabilities and weaknesses in network services.
 - B. To map out the physical locations of devices on a network.
 - C. To determine the compliance of the network with industry standards.
 - D. To assess user satisfaction with network services.