

061205T4CYB

CYBER SECURITY TECHNICIAN LEVEL 5

SEC/OS/CS/CR/05/5

Secure Databases

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)

Answer All Questions in This Section.

1. An organization relies on its database system for daily operations. Recent system downtime has caused service delays and limited access to critical information. State FOUR cybersecurity measures that can be implemented to ensure data availability. (4 marks)
2. Databases can be grouped according to how data is structured. Identify THREE classification of databases based on structure. (3 marks)
3. An organization uses a database system with minimal security controls, making it an easy target for cyberattacks. State FOUR characteristics of database vulnerabilities. (4 marks)
4. Risk assessment is part of database security management. Identify THREE factors considered when assessing database security risks. (3 marks)
5. Applying patches incorrectly can cause system failure. State THREE factor to consider before installing a database patch. (3 marks)
6. A middle level college stores student examination results in an Access database. Identify FOUR database threats associated with this system. (4 marks)
7. Before deploying a new database, the ICT officer checks data accuracy and security settings. State FOUR reason for checking the security settings. (4 marks)
8. A database keeps a record of user logins, updates, and deletions.
 - a) Identify the security feature used. (1 mark)
 - b) Identify THREE benefits of this feature. (3 marks)
9. Database access is recorded at night when the office is closed.
 - a) State the importance of investigating this activity. (1 mark)
 - b) Identify THREE possible causes of this breach. (3 marks)
10. Microsoft releases an update to fix a security flaw in Access databases. The ICT department must install the update to protect the system. State FOUR risks of delaying the update. (4 marks)
11. A hospital stores patient records in a database, including names, addresses, medical history, and treatment details. State THREE measures the hospital should implement to ensure the confidentiality of patient data. (3 marks)

SECTION B (60 MARKS)

Attempt ANY THREE Questions in This Section.

12. A company stores its customer database on a shared network drive. The database contains sensitive information such as customer names, phone numbers, national IDs, and transaction history. It is stored without encryption, and many staff members can access the shared folder.
- a) Explain FOUR risks of storing the database without encryption. (8 marks)
 - b) Describe THREE security threats that may result from this practice. (6 marks)
 - c) Explain THREE measures the company should implement to secure the database. (6 marks)
13. A college is developing a new student management system using MS Access. The database stores student details, and before deployment, the ICT department must carry out database testing.
- a) Explain the meaning of database testing. (2 marks)
 - b) Describe FIVE types of database tests that should be carried out. (10 marks)
 - c) Explain FOUR reasons for testing the database before deployment. (8 marks)
14. A bank uses a centralized database to store customer accounts, transaction history, and employee access logs. Recently, there have been several incidents of unauthorized access and data manipulation. The ICT security team has decided to implement log monitoring and auditing to detect suspicious activities.
- a) Describe FIVE types of events that should be recorded in the database audit logs. (10 marks)
 - b) Explain FIVE benefits of log monitoring in database security. (10 marks)
15. A government ministry is implementing a Database Security Management System (DSMS) to protect sensitive citizen data stored in multiple databases. The ICT team must select and configure the DSMS to ensure the database environment is secure, compliant, and reliable.
- a) Describe FIVE features of a DSMS. (10 marks)
 - b) Explain FIVE criteria considered when selecting a DSMS. (10 marks)