

SECURE DATABASES

TVET CDACC UNIT CODE: SEC/OS/CS/CR/04/5/MA

UNIT DESCRIPTION

This unit covers the competencies required to secure databases. Competencies include identifying database management system, designing a database, creating a database, implementing database security measures and monitor database security.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Identify database management system	1.1 Organizational requirements for data storage, access, and security are reviewed to determine database needs. 1.2 Types of database management systems (relational, object-oriented, NoSQL, distributed, hierarchical, etc.) are identified and described. 1.3 Features of different DBMSs (scalability, concurrency control, backup, recovery, security mechanisms) are compared. 1.4 DBMS options (e.g., MySQL, Oracle, SQL Server, PostgreSQL, MongoDB) are evaluated according to organizational and security requirements. 1.5 The most suitable DBMS is selected to meet functional, technical, and security specifications.
2. Design a database	2.1 User and organizational requirements are gathered and analyzed to define database objectives. 2.2 Entities, attributes, and relationships are identified and documented using Entity-Relationship Diagrams (ERDs). 2.3 Appropriate data types and structures are selected in line with system requirements and security considerations. 2.4 Database schema is designed to ensure normalization, integrity, and efficiency. 2.5 Security requirements (access controls, encryption, auditing needs) are incorporated into the database design. 2.6 Data dictionary is developed to document fields, data

	types, and constraints. 2.7 Database design is validated and reviewed against user needs, organizational policies, and security standards.
3. Create a database	3.1 Database is created using the selected DBMS according to approved design specifications. 3.2 Tables, fields, and relationships are defined based on the database schema. 3.3 Primary keys, foreign keys, and constraints are applied to ensure data integrity. 3.4 Security controls (user accounts, roles, and privileges) are established during database creation. 3.5 Stored procedures, triggers, and views are implemented where required to support functionality and security. 3.6 Sample data is inserted to test table structures, relationships, and security rules. 3.7 Database creation is documented according to organizational standards and security policies.
4. Implement database security measures	4.1 User authentication mechanisms (password policies, multi-factor authentication) are configured according to organizational requirements. 4.2 User roles and access privileges are assigned based on the principle of least privilege. 4.3 Data encryption (at rest and in transit) is implemented using appropriate tools and standards. 4.4 Database auditing and logging features are enabled to track user activities and system events. 4.5 Security patches and updates are applied to the DBMS in line with vendor and organizational policies. 4.6 Intrusion detection and prevention measures are configured to protect against unauthorized access. 4.7 Backup and recovery procedures are established to safeguard data integrity and availability. 4.8 Security configurations are tested and validated to ensure compliance with organizational and regulatory standards.
5. Monitor database security	5.1 Database activity is continuously monitored using auditing tools and security dashboards. 5.2 User access logs and transaction records are reviewed to detect unauthorized activities. 5.3 Intrusion attempts, anomalies, and suspicious

	behaviors are identified through monitoring tools. 5.4 Alerts and notifications are configured to respond to security incidents in real time. 5.5 Security performance metrics (failed login attempts, privilege escalations, access trends) are analyzed regularly. 5.6 Incident response procedures are followed to mitigate identified threats and vulnerabilities. 5.7 Monitoring reports are generated and documented in line with organizational and regulatory compliance requirements.
6. Manage database backups	6.1 Backup requirements (frequency, type, retention period) are determined according to organizational and regulatory policies. 6.2 Appropriate backup methods (full, incremental, differential, snapshot) are selected based on database size and criticality. 6.3 Automated backup schedules are configured using DBMS tools or third-party software. 6.4 Backup files are secured through encryption and access controls to prevent unauthorized access. 6.5 Backup storage locations (onsite, offsite, cloud) are managed to ensure data availability and disaster recovery readiness. 6.6 Test restorations are performed periodically to validate the integrity and reliability of backup data. 6.7 Backup and recovery procedures are documented and updated in accordance with organizational standards.

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

Variable	Range
Database management system may include but not limited to:	• MySQL workbench CE, MS SQL server, • MySQL Database
Database Monitoring tools may include but not limited to:	• Nagios • Solar winds Database Performance analyzer • Amason cloud watch • Azure Monitor

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Analytical skills
- Requirements analysis
- Data modeling
- Database Schema implementation
- SQL Programming skills
- Security configuration
- System administration
- Disaster recovery
- Monitoring and auditing
- Incident response

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in digital literacy
- Time management;
- Analytical
- Faults troubleshooting
- Problem solving;
- Planning;
- Decision making;
- Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	1.1 Document for database needs was outlined as per organizational requirements for data storage, access, and security. 1.2 Evaluation matrix of DBMS options such as MySQL, Oracle
-----------------------------------	--

	was mapped against organizational/security needs. 1.3 Requirements document from user interviews, surveys, or organizational was established as per policy analysis. 1.4 ERDs are outlined according to identifying entities, attributes, and relationships. 1.5 SQL scripts or schema files outlined based on definition of tables, fields, and relationships. 1.6 SQL code showing primary keys, foreign keys, and constraints outlined as per organizational/security needs. 1.7 Document for authentication configuration were outlined in line with organizational requirements (password policies, MFA). 1.8 Roles and access privileges were assigned and documented according to the principle of least privilege. 1.9 Security patches and updates were applied and recorded in accordance with vendor and organizational policies. 1.10 Backup files were secured with encryption and access controls, and the measures were documented. 1.11 Backup storage management (onsite, offsite, cloud) was outlined to ensure disaster recovery readiness.
2. Resource Implications for competent certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Projects 3.4 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

assessment	
------------	--