

Variable	Range
Network topology may include but not limited to:	• Star • Ring • Mesh • Hybrid • Point to point
Network components may include but not limited to:	• Routers • Switches • Hub • RJ 45 connectors • Ports • Computers • Printers
Network types may include but not limited to:	• WAN • LAN • PAN • WLAN
Network protocols may include but not limited to:	• OSI • TCP/IP
Network Standards	• IEEE 802.3 • IEEE 802.11 • IEEE 802.15. • IEEE 802.16:
IP addressing scheme	• IPv4 • IPv6
designing a Local Area Network	• Logical topology • Physical topology
Types of Network Maintenance	• Preventive • Corrective • Adaptive
Monitoring tools may include but not limited to:	• Wireshark • PRTG

	• NetFlow • SNMP • Syslog
--	---

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Network Architecture
- Network programming languages
- Network Components and devices
- Network types
- Network security Measures
- Network Monitoring procedures
- Network testing techniques
- Network configuration techniques
- Network protocols
- Network security techniques and procedures
- Network testing procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:

- Communications (verbal and written);
- Proficient in digital literacy
- Problem solving
- Decision Making
- Leadership
- Self-training

EVIDENCE GUIDE

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

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Network design is developed according to the site survey 1.2 Network components are identified according to the site survey 1.3 Network type is identified as per the client's requirements 1.4 Identified of the transmission media is done according to network types 1.5 Network topologies are established based on the computer network needs. 1.6 Network connection is performed according to Network standards 1.7 IP addressing scheme configuration is performed 1.8 Basic Troubleshooting is done according to network issue 1.9 Types of Network Maintenance are identified 1.10 Network monitoring tools are identified as per the type of tests to be carried out 1.11 Network scalability survey is done 1.12 Key Components of a Network Report are established.
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 Observation 3.2 Oral questioning 3.3 Practical demonstration
4. Context of Assessment	Competency may be assessed individually in the actual workplace and simulated setting of the actual work place
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

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