

BUILD SECURE NETWORK

TVET CDACC UNIT CODE: SEC/OS/CS/CR/01/6/A

UNIT DESCRIPTION

This unit covers the competencies required in building secure network. It involves reviewing security issues, analyzing network security protocols and features, designing and perimeters, installing and configuring perimeter solutions, configuring internal network devices, testing and verifying design performance and training network users.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	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. Review security issues	1.1 Organizational security policies, standards, and compliance requirements are reviewed to establish network security needs. 1.2 Existing network infrastructure is analyzed to identify current security controls and weaknesses. 1.3 Threats and vulnerabilities relevant to the organization's network environment are identified (e.g., unauthorized access, malware, denial-of-service, insider threats). 1.4 Security risks are assessed based on likelihood, impact, and potential business disruption. 1.5 Findings from past security audits, penetration tests, and incident reports are reviewed to guide planning. 1.6 Security objectives and priorities are documented in consultation with stakeholders.
2. Analyse network security protocols and features	2.1 Common network security protocols (SSL/TLS, IPSec, SSH, HTTPS, WPA2/3, RADIUS, Kerberos) are identified and described according to

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	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>
	their functions. 2.2 Features of security protocols (encryption, authentication, integrity, non-repudiation) are analyzed in relation to organizational requirements. 2.3 Secure communication mechanisms for data in transit are evaluated for effectiveness. 2.4 Strengths and limitations of different security protocols are compared based on use cases. 2.5 Network devices (firewalls, IDS/IPS, VPNs, access points) are reviewed for their security features and capabilities. 2.6 Protocols and security features are matched to organizational needs to support confidentiality, integrity, and availability. 2.7 Recommendations are documented for selecting appropriate security protocols and features.
3. Install and configure perimeter solutions	3.1 Perimeter security requirements are identified based on organizational risk assessment and network design. 3.2 Perimeter devices (firewalls, routers, IDS/IPS, VPN gateways, web application firewalls) are selected in line with security needs. 3.3 Devices are installed and configured according to vendor guidelines and organizational security policies. 3.4 Access control lists (ACLs), firewall rules, and traffic filtering policies are implemented to restrict unauthorized access. 3.5 Intrusion detection and prevention systems are

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	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>
	configured to monitor and block malicious activities. 3.6 Secure remote access solutions (VPNs, multi-factor authentication) are deployed and tested. 3.7 Perimeter devices are integrated into the overall network architecture to ensure seamless operation. 3.8 Configuration settings are documented, tested, and validated for effectiveness.
4. Test and verify design performance	4.1 Test plan is developed to evaluate security controls, functionality, and network performance against design specifications. 4.2 Security features (firewalls, IDS/IPS, VPNs, ACLs) are tested to confirm correct configuration and effectiveness. 4.3 Network performance metrics (throughput, latency, availability, reliability) are measured and compared with baseline requirements. 4.4 Penetration tests and vulnerability scans are conducted to validate resilience against potential threats. 4.5 Failover and redundancy mechanisms are tested to ensure business continuity during disruptions. 4.6 Test results are analyzed to identify gaps, weaknesses, or misconfigurations. 4.7 Findings are documented and reported to stakeholders for corrective actions. 4.8 Verified design is approved for deployment in the production environment.
5. Train network users	5.1 Training needs are identified based on

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	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>
	organizational security policies, user roles, and risk assessment. 5.2 User training materials (guides, tutorials, awareness programs) are developed in line with best security practices. 5.3 Training covers key areas such as password management, safe browsing, email security, and proper use of network resources. 5.4 Security awareness sessions are conducted to educate users on recognizing phishing, social engineering, and other cyber threats. 5.5 Hands-on demonstrations and simulations are used to reinforce secure network usage practices. 5.6 User understanding and compliance are evaluated through assessments, feedback, or testing. 5.7 Training effectiveness is reviewed regularly and updated to address emerging threats and technologies. 5.8 Records of training sessions and user participation are maintained for accountability and compliance.

RANGE

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

Variable	Range
Network infrastructure analysis may include but not limited to:	• Existing architecture • Current security controls • Identified weaknesses

Audit and testing references may include but not limited to:	• Past audit findings • Penetration test results • Incident reports
Network security devices may include but not limited to:	• Firewalls • IDS/IPS • VPNs • Access points
Perimeter security devices may include but not limited to:	• Firewalls • Routers • IDS/IPS • VPN gateways • Web Application Firewalls (WAFs)
Access control mechanisms may include but not limited to:	• Access Control Lists (ACLs) • Firewall rules • Filtering policies
Network performance metrics may include but not limited to:	• Throughput • Latency • Availability • Reliability
Training needs analysis may include but not limited to:	• Role-based requirements • Policy-driven needs • Risk-based needs
User compliance validation may include but not limited to:	• Assessments • Feedback mechanisms • Policy adherence checks

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Existing network architecture, current security controls, and the ability to identify weaknesses within the infrastructure.
- Past audit findings, penetration test results, and incident reports to inform ongoing security assessments.

- Firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and access points, including their configuration and role in network defense.
- Perimeter defense mechanisms such as firewalls, routers, IDS/IPS, VPN gateways, and web application firewalls (WAFs) to ensure secure boundary protection.
- Access control lists (ACLs), firewall rules, and filtering policies, and how they are applied to enforce security requirements.
- Key performance indicators such as throughput, latency, availability, and reliability in evaluating network effectiveness and resilience.
- Role-based, policy-driven, and risk-based training requirements to strengthen security awareness and capability.

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in Digital skills;
- Time management;
- Analytical
- 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	Assessment requires evidence that the candidate: 1.1 Organizational security policies, standards, and compliance requirements were reviewed and documented to define network security needs. 1.2 Existing network infrastructure was analyzed and documented to identify current security controls and weaknesses. 1.3 Security risks were assessed, prioritized, and documented based on likelihood, impact, and business disruption.
-----------------------------------	--

	1.4 Findings from past audits, penetration tests, and incident reports were reviewed and documented to guide planning. 1.5 Secure communication mechanisms for protecting data in transit were evaluated and documented for effectiveness. 1.6 Strengths and limitations of different protocols were compared and documented based on organizational use cases. 1.7 Network devices (firewalls, IDS/IPS, VPNs, access points) were reviewed and documented for their security features. 1.8 Appropriate perimeter devices (firewalls, routers, IDS/IPS, VPN gateways, WAFs) were selected and documented according to security needs. 1.9 Devices were installed, configured, and documented following vendor guidelines and organizational policies. 1.10 Access control lists (ACLs), firewall rules, and filtering policies were implemented and documented to restrict unauthorized access. 1.11 Secure remote access solutions (VPNs, MFA) were deployed, tested, and documented. 1.12 A test plan was developed and documented to evaluate security controls, functionality, and performance. 1.13 Security features (firewalls, IDS/IPS, VPNs, ACLs) were tested, validated, and documented for effectiveness. 1.14 Network performance metrics (throughput, latency, availability, reliability) were measured and documented against baselines. 1.15 Penetration testing and vulnerability scanning were conducted and documented to validate resilience against threats. 1.16 Training needs were identified and documented based on policies, roles, and risk assessments. 1.17 User training materials (guides, tutorials, awareness programs) were developed and documented in line with best practices.
--	--

	1.18 User understanding and compliance were evaluated, documented, and validated through assessments or feedback.
2. Resource Implications for competence 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 assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.