

Software components may include but not limited to:	• Databases • APIs • Third-party libraries • System integrations
Security assessment requirements may be based on but not limited to:	• Organizational policies • Security standards • Compliance regulations
Assessment tools may include but not limited to:	• Open-source tools • Commercial tools • Automated scanners • Manual testing utilities
Security benchmarks and baselines may include but not limited to:	• OWASP • NIST • ISO/IEC 27001 • Industry-specific standards
Assessment activities may include but not limited to:	• Development of assessment plan • Vulnerability scanning • Penetration testing • Risk documentation
Security monitoring tools may include but not limited to:	• SIEM • IDS/IPS • Firewalls • Log management systems
Monitoring activities may include but not limited to:	• Scheduled vulnerability scans • Continuous penetration testing • Tracking application behaviour
Compliance verification may include but not limited to:	• Organizational policies • Legal standards • Regulatory requirements • Industry-specific compliance frameworks

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Recognizing and classifying different types of applications (desktop, web, mobile, cloud).
- Analyzing application functions, workflows, and user roles to assess risks.
- Identifying security assessment requirements aligned with policies and industry standards.
- Installing, configuring, and validating tools for accurate results.
- Performing penetration testing to simulate real-world attacks.
- Producing a detailed vulnerability report for corrective action.
- Applying secure coding practices to mitigate common threats (SQLi, XSS, buffer overflow, insecure APIs).
- Reviewing logs and audit trails for suspicious activities.
- Documenting vulnerabilities, corrective actions, and residual risks.

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in Digital Literacy;
- 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 List of software applications (desktop, web, mobile, cloud-based) was identified for security assessment. 1.2 Application functions, workflows, and user roles were analyzed and documented to highlight potential risks. 1.3 Software components such as databases, APIs, third-party
-----------------------------------	--

	libraries, and integrations were identified as part of the security scope. 1.4 Security assessment requirements were identified and documented in line with organizational policies and standards. 1.5 Evaluation of open-source and commercial tools was documented with considerations of effectiveness, compatibility, and cost-efficiency. 1.6 Security benchmarks and baselines (OWASP, NIST, ISO/IEC 27001) were established and documented for tool configuration. 1.7 Security assessment plan was developed and documented in line with organizational policies and defined scope. 1.8 Penetration testing findings were documented to demonstrate simulated attack scenarios. 1.9 Prioritized list of vulnerabilities was addressed and documented according to severity levels. 1.10 Secure coding practices were applied and documented to mitigate common threats such as SQL injection, XSS, and buffer overflows. 1.11 Security hardening guidelines were applied to the application environment and documented. 1.12 Security monitoring tools (SIEM, IDS/IPS, firewalls) were configured and documented to track application behavior. 1.13 Scheduled vulnerability scans and penetration tests were performed and documented to maintain security posture. 1.14 Monitoring results were documented and reported according to organizational and compliance requirements. 1.15 Findings from assessments, hardening, and monitoring were compiled and documented into a comprehensive report. 1.16 Security performance metrics and incident response outcomes were recorded and documented. 1.17 Compliance with organizational policies, legal, and regulatory standards was verified and included in the report.
--	---

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 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.

PERFORM WEBSITE DESIGN AND DEVELOPMENT

TVET CDACC UNIT CODE: SEC/OS/CS/CR/07/5/MA

Unit Description

This unit specifies competencies required Perform Website Design and Development. It involves gathering data required, determining website design tool, developing functional website, host website developed and perform website routine maintenance.

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. Gather data required for website development	1.1 All client requirements, including target audience, site objectives, and functionality needs, are documented in a project brief that is at least 95% complete according to the client's feedback. 1.2 Market and competitor research findings are compiled into a clear, organized report with a minimum of three competitor analysis entries. 1.3 All multimedia assets (text, images, videos, branding elements) are collected, named consistently, and stored in an accessible folder structure with no missing files before development starts.
2. Determine Website design tool	2.1 At least two suitable design tools are compared in a short report based on criteria such as compatibility, cost, features, and ease of use. 2.2 The selected tool is approved by the project supervisor/client and documented in the project plan with a clear justification. 2.3 The chosen tool is successfully installed/configured on the developer's workstation within one business day of approval.

3. Develop functional website	3.1 The website meets the documented functional requirements such as navigation, forms submit correctly, and media loads properly during testing. 3.2 All page's load within a reasonable amount of amount of time such as three seconds under normal internet speeds (5–10 Mbps) when tested. 3.3 The design is fully responsive, passing a mobile-friendly test on at least three different devices/screen sizes without layout breakage.
4. Host Website developed	4.1 The website is uploaded to the hosting server with no missing files or broken links as verified by a post-deployment test. 4.2 The domain is correctly linked to the hosting server and resolves without errors within 24 hours of deployment. 4.3 SSL/TLS certificate is installed, and the site passes a basic security scan with no high-severity issues.
5. Perform Website Routine Maintenance	5.1 All CMS, plugins, and security updates are applied within 48 hours of release. 5.2 A full site backup (files + database) is created and verified at least once per week. 5.3 Site performance is monitored, with load times kept under three seconds and zero downtime exceeding two consecutive hours in any given month.

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
1. Website application design tools may include but are not limited to:	• Vscode • WordPress/Joomla/Drupal • Xampp/Nginx
2. Website application design approaches may include but are not limited to:	• Static • Dynamic • Adaptive

	• Mobile first • Progressive • Single page application
3. Website application visual hierarchy may include but are not limited to:	• Graphical user interface • Site Map • Typography • Color • Layout
4. Website application testing techniques may include but are not limited to:	• Functional testing • Usability testing • Interface testing • Compatibility testing • Performance testing • Security testing.

REQUIRED KNOWLEDGE AND SKILLS

This section describes the knowledge and skills required for this unit of competency.

REQUIRED KNOWLEDGE

The individual needs to demonstrate knowledge of:

- Documentation processes
- Technology trends in development of website design.
- Coding skills in HTML, CSS and JavaScript.
- Bug fixing.
- Types of maintenance techniques

Required skills

The individual needs to demonstrate the following skills:

- Report Writing
- Data collection
- Analytical skills
- Problem solving skills
- Communication skills
- Time management

- Critical thinking

EVIDENCE GUIDE

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

1. Critical aspects of competency	1.1 Documented website user requirements specifications process as per the user needs. 1.2 Developed <i>website application visual hierarchy</i> as per the user needs. 1.3 Created website application site map as per the user needs. 1.4 Created front end web pages per website application design. 1.5 Created front end web pages per website application design. 1.6 Created back-end web pages as per website application design. 1.7 Integrated website application to the backend as per workplace procedure. 1.8 Uploaded website application files as per host requirements. 1.9 Configured website server as per host requirements. 1.10 Installed SSL/TLS certificate and performed basic scan as per the security standards. 1.11 Fixed website application bugs as per monitoring report. 1.12 Updated website application as per the workplace procedures.
2. Resource implications	The following resources should be provided: 2.1 Appropriately simulated environment where assessment can take place. 2.2 Access to relevant work environment. 2.3 Resources relevant to the proposed activities or

	tasks.
3. Methods of assessment	Competency may be assessed through: 3.1 Practical 3.2 Projects 3.3 Third Party Reports 3.4 Portfolio of evidence 3.5 Written tests
4. Context of assessment	Competency may be assessed in a workplace or in a simulated workplace.
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace job role is recommended.

CONDUCT SECURITY ASSESSMENT AND TESTING

TVET CDACC UNIT CODE: SEC/OS/CS/CR/08/5/MA

UNIT DESCRIPTION

This unit covers the competencies required to conduct cyber security assessment and testing. It involves gathering information about organization and its systems, scan and mapping of network, enumerating network resources, exploiting known vulnerabilities, performing social engineering and preparing security assessment and testing report.

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. Gather information about organization and its systems	1.1 Organizational policies, procedures, and compliance requirements are reviewed to understand the security context. 1.2 Business processes, critical assets, and data flows are identified to determine assessment scope. 1.3 Hardware, software, and network infrastructure components are documented for security evaluation. 1.4 User roles, access privileges, and authentication mechanisms are reviewed to assess potential risks. 1.5 Existing security controls and previous assessment reports are collected for reference. 1.6 Threat landscape relevant to the organization's industry and environment is analyzed. 1.7 Information gathering methods (interviews, questionnaires, document reviews, system scans) are applied to ensure comprehensive data collection.
2. Scan and map the network	2.1 Network scanning objectives and scope are defined in line with organizational policies and assessment requirements. 2.2 Approved scanning tools (e.g., Nmap, Nessus, OpenVAS, Wireshark) are selected based on assessment needs. 2.3 Network discovery scans are conducted to identify active

	hosts, IP addresses, and connected devices. 2.4 Port scanning is performed to detect open, closed, and filtered ports on network devices. 2.5 Services and applications running on detected hosts are enumerated and documented. 2.6 Network topology is mapped to illustrate connections, pathways, and data flows. 2.7 Scanning results are validated to minimize false positives and ensure accuracy. 2.8 Findings are documented securely and shared with authorized stakeholders.
3. Enumerate target resources	3.1 Enumeration scope is defined to identify systems, services, and resources within the target environment. 3.2 Enumeration tools (e.g. Netcat, Nmap scripts, SMB enumeration, SNMPwalk, LDAP queries) are selected based on target systems. 3.3 User accounts, groups, and roles are enumerated to assess access privileges. 3.4 Network shares, directories, and services are identified and documented. 3.5 System banners, software versions, and configurations are collected for vulnerability analysis. 3.6 Third-party services, APIs, and applications connected to the target system are identified. 3.7 Enumeration findings are analyzed to reveal potential attack vectors. 3.8 Results are validated, documented, and shared with authorized stakeholders for further testing.
4. Exploit known vulnerabilities	4.1 Identified vulnerabilities are reviewed and prioritized based on severity, exploitability, and potential business impact. 4.2 Exploitation activities are planned in line with organizational policies, rules of engagement, and legal requirements. 4.3 Approved penetration testing tools and frameworks (e.g.,

	Metasploit, Burp Suite, SQLmap) are selected for exploitation. 4.4 Exploits are executed in a controlled manner to validate the existence of vulnerabilities without disrupting business operations. 4.5 Exploitation attempts are monitored and documented, including successful access, privilege escalation, or data exposure. 4.6 Evidence of exploitation (screenshots, logs, payload outcomes) is collected securely for reporting. 4.7 Exploitation results are analyzed to determine potential risks and system weaknesses. 4.8 Findings are reported to stakeholders with recommendations for remediation.
5. Perform social engineering	5.1 Social engineering scope and objectives are defined in line with organizational policies, legal, and ethical guidelines. 5.2 Human-based attack vectors (e.g., phishing, pretexting, baiting, impersonation) are identified for testing. 5.3 Social engineering tools and techniques (e.g., phishing simulators, phone-based pretexting, onsite physical tests) are selected and approved. 5.4 Controlled social engineering exercises are carried out to assess employee awareness and adherence to security policies. 5.5 User responses to social engineering attempts are monitored, recorded, and analyzed. 5.6 Findings are documented, including vulnerabilities in human behaviour, processes, or training gaps. 5.7 5.7. Recommendations for security awareness training and procedural improvements are provided to mitigate identified risks. 5.8 5.8. Results are communicated to stakeholders in a confidential and constructive manner.

6. Conduct System hacking	6.1 System hacking activities are planned and approved in line with organizational policies, scope, and legal requirements. 6.2 Attack vectors (password cracking, privilege escalation, session hijacking, malware injection) are identified based on assessment objectives. 6.3 Approved ethical hacking tools and techniques (e.g., Metasploit, Hydra, John the Ripper, keyloggers in controlled environments) are utilized. 6.4 System vulnerabilities are exploited in a controlled manner to gain unauthorized access and escalate privileges. 6.5 System defenses (antivirus, intrusion detection, access controls) are tested to evaluate their effectiveness. 6.6 Evidence of successful exploitation, privilege escalation, or data compromise is documented securely. 6.7 Risks and impacts of system hacking activities are analyzed and reported to stakeholders. 6.8 Recommendations for hardening systems against hacking attempts are provided.
7. Prepare security assessment and testing report	7.1 Social engineering scope and objectives are defined in line with organizational policies, legal, and ethical guidelines. 7.2 Human-based attack vectors (e.g., phishing, pretexting, baiting, impersonation) are identified for testing. 7.3 Social engineering tools and techniques (e.g., phishing simulators, phone-based pretexting, onsite physical tests) are selected and approved. 7.4 Controlled social engineering exercises are carried out to assess employee awareness and adherence to security policies. 7.5 User responses to social engineering attempts are monitored, recorded, and analyzed. 7.6 Findings are documented, including vulnerabilities in human behavior, processes, or training gaps. 7.7 Recommendations for security awareness training and procedural improvements are provided to mitigate identified

	risks. 7.8 Results are communicated to stakeholders in a confidential and constructive manner.
--	---

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
1. ICT infrastructure components may include but not limited to:	• Hardware • Software • Network infrastructure
2. Threat landscape may cover but not limited to:	• Industry-specific risks • Environmental risks • Emerging threats • Known vulnerabilities
3. Scanning tools may include but not limited to:	• Nmap • Nessus • OpenVAS • Wireshark
4. Enumeration scope may include but not limited to:	• Systems • Services • Resources • Network shares and directories
5. Penetration testing tools may include but not limited to:	• Metasploit • Burp Suite • SQLmap
6. Exploitation activities may include but not limited to:	• Access attempts • Privilege escalation • Data exposure evidence

Variable	Range
7. Social engineering tools and techniques may include but limited to:	• Phishing simulators • Phone pretexting tools • Onsite testing
8. Report compliance may include but not limited to:	• Organizational policies • Contractual requirements • Legal standards • Regulatory obligations

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Knowledge of hardware, software, and network infrastructure components and their role in organizational security.
- Understanding of industry-specific risks, environmental risks, emerging threats, and known vulnerabilities that may impact systems and data.
- Skills in using tools such as Nmap, Nessus, OpenVAS, and Wireshark to identify vulnerabilities and analyze network/system security.
- Ability to enumerate systems, services, resources, and network shares/directories to gather technical intelligence for security assessment.
- Practical competence in the use of tools such as Metasploit, Burp Suite, and SQLmap to simulate real-world attacks.
- Knowledge of exploitation techniques including system access attempts, privilege escalation, and identifying evidence of data exposure.
- Understanding of social engineering tools and techniques such as phishing simulators, phone pretexting, and onsite testing to assess human-related vulnerabilities.
- Knowledge of organizational policies, contractual requirements, legal standards, and regulatory obligations to prepare compliant security assessment reports.

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	Assessment requires evidence that the candidate: 1.1 Organizational policies, procedures, and compliance requirements were reviewed and documented to determine the security context. 1.2 Hardware, software, and network infrastructure components were documented for evaluation. 1.3 Threat landscape relevant to the organization's industry and environment was analyzed and documented. 1.4 Approved scanning tools (Nmap, Nessus, OpenVAS, Wireshark) were selected and documented. 1.5 Network discovery scans were conducted and documented to identify active hosts, IP addresses, and connected devices. 1.6 Port scanning results were documented to show open, closed, and filtered ports. 1.7 Network topology was mapped and documented to illustrate connections, pathways, and data flows. 1.8 Scope of enumeration was defined and documented to identify systems, services, and resources. 1.9 Network shares, directories, and services were identified and documented. 1.10 Results were validated, documented, and shared with authorized stakeholders.
--	--

	1.11 Enumeration findings were analyzed, documented, and mapped to potential attack vectors. 1.12 Approved penetration testing tools and frameworks (Metasploit, Burp Suite, SQLmap) were selected and documented. 1.13 Exploitation attempts were monitored and documented, including evidence of access, privilege escalation, or data exposure. 1.14 Scope and objectives of social engineering activities were defined and documented in line with policies, legal, and ethical guidelines. 1.15 Human-based attack vectors (phishing, pretexting, baiting, impersonation) were identified and documented for testing. 1.16 Approved tools and techniques (phishing simulators, phone pretexting, onsite tests) were selected and documented. 1.17 Findings were documented, highlighting vulnerabilities in human behavior, processes, or training gaps. 1.18 Results from information gathering, scanning, enumeration, exploitation, and social engineering were compiled and documented into a structured report. 1.19 Recommendations for remediation, mitigation, and security improvements were documented. 1.20 Report was reviewed and documented to ensure compliance with organizational policies, contracts, and legal requirements. 1.21 Final report was documented, stored securely, and archived in line with organizational and regulatory standards.
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 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.