

|   |                                                            |                                                                                                                                                                                                                                                                           |
|---|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2 | Resource<br>Implications for<br>competent<br>certification | <p>The following resources should be provided:</p> <p>2.1 Access to relevant workplace where assessment can take place</p> <p>2.2 Appropriately simulated environment where assessment can take place</p> <p>2.3 Materials relevant to the proposed activity or tasks</p> |
| 3 | Methods of<br>Assessment                                   | <p>Competency may be assessed through:</p> <p>3.1 Observation</p> <p>3.2 Oral questioning</p> <p>3.3 Practical test in conducting test</p> <p>3.4 Demonstration of interpretation of test results</p>                                                                     |
| 4 | Context of<br>Assessment                                   | <p>Competency may be assessed individually</p> <p>4.1 On job</p> <p>4.2 Out of job</p> <p>4.3 During Industrial attachment</p>                                                                                                                                            |
| 5 | Guidance<br>information for<br>assessment                  | <p>Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.</p>                                                                                                                                                       |

## SECURE SOFTWARE APPLICATION

**TVET CDACC UNIT CODE:** SEC/OS/CS/CR/06/5/MA

### UNIT DESCRIPTION

This unit covers the competencies required to secure software application. Competencies include Identifying software to be secured, establishing tools for application security assessment, perform application security assessment, hardening software application, monitoring application security performance and preparing of reports on software security.

### ELEMENTS AND PERFORMANCE CRITERIA

| <b>ELEMENT</b>                                                    | <b>PERFORMANCE CRITERIA</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br><i>(Bold and italicised terms are elaborated in the Range)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 1. Identify software to be secured                                | <ul style="list-style-type: none"><li>1.1 Organizational requirements and security policies are reviewed to determine software security needs.</li><li>1.2 Software applications (desktop, web, mobile, cloud-based) are identified for assessment.</li><li>1.3 Application functions, workflows, and user roles are analyzed to determine potential security risks.</li><li>1.4 Existing security controls and vulnerabilities in the software are documented.</li><li>1.5 Software components (databases, APIs, third-party libraries, integrations) are identified as part of the security scope.</li><li>1.6 Software to be secured is prioritized based on criticality, sensitivity of data handled, and business impact.</li></ul> |
| 2. Establish tools for application security assessment            | <ul style="list-style-type: none"><li>2.1 Security assessment requirements are identified in line with organizational policies and industry standards.</li><li>2.2 Appropriate security assessment tools (static analysis, dynamic analysis, penetration testing, vulnerability</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                            | <p>scanners, code review tools) are selected based on application type.</p> <p>2.3 Open-source and commercial tools are evaluated for effectiveness, compatibility, and cost-efficiency.</p> <p>2.4 Testing environments are set up to ensure safe execution of security assessment tools without disrupting production systems.</p> <p>2.5 Security benchmarks and baselines (e.g., OWASP, NIST, ISO/IEC 27001) are established for tool configuration.</p> <p>2.6 Selected tools are installed, configured, and validated to ensure accuracy of results.</p> <p>2.7 Documentation of assessment tools, usage procedures, and configurations is prepared for future reference.</p>                                                                                                                                                                                         |
| 3. Perform application security assessment | <p>3.1 Security assessment is planned in accordance with organizational policies and scope of the software application.</p> <p>3.2 Static application security testing (SAST) is conducted to identify vulnerabilities in source code.</p> <p>3.3 Dynamic application security testing (DAST) is performed to detect runtime vulnerabilities.</p> <p>3.4 Penetration testing is carried out to simulate real-world attack scenarios.</p> <p>3.5 Vulnerabilities related to authentication, authorization, input validation, and session management are identified and documented.</p> <p>3.6 Third-party libraries, APIs, and integrations are tested for security weaknesses.</p> <p>3.7 Assessment results are analyzed and prioritized based on severity, exploitability, and potential business impact.</p> <p>3.8 A detailed vulnerability report is generated and</p> |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             | submitted for corrective action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 4. Harden software application              | <p>4.1 Security vulnerabilities identified during assessment are prioritized and addressed according to severity.</p> <p>4.2 Secure coding practices are applied to mitigate common threats such as SQL injection, cross-site scripting (XSS), buffer overflows, and insecure APIs.</p> <p>4.3 Application configuration settings are reviewed and adjusted to enforce security best practices.</p> <p>4.4 Strong authentication and authorization mechanisms are implemented to control user access.</p> <p>4.5 Sensitive data is protected through encryption, hashing, and secure key management.</p> <p>4.6 Application dependencies, libraries, and frameworks are updated and patched to eliminate known vulnerabilities.</p> <p>4.7 Security hardening guidelines are applied to the application environment.</p> <p>4.8 Hardened application is tested to verify that vulnerabilities have been mitigated and functionality is not compromised.</p> |
| 5. Monitor application security performance | <p>5.1 Application security logs and audit trails are reviewed regularly to detect suspicious activities.</p> <p>5.2 Security monitoring tools (e.g., SIEM, IDS/IPS, application firewalls) are configured to track application behaviour.</p> <p>5.3 Key security metrics (failed login attempts, privilege escalations, abnormal traffic patterns) are analyzed to assess performance.</p> <p>5.4 Vulnerability scans and penetration tests are scheduled periodically to evaluate ongoing security posture.</p> <p>5.5 Alerts and notifications are generated to provide real-time response to potential threats.</p>                                                                                                                                                                                                                                                                                                                                    |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | <p>5.6 Incident response procedures are followed to address detected security breaches.</p> <p>5.7 Monitoring results are documented and reported in line with organizational and compliance requirements.</p> <p>5.8 Application security policies and controls are reviewed and updated based on monitoring outcomes.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 6. Prepare a report on software security | <p>6.1 Findings from security assessments, hardening activities, and monitoring are compiled into a comprehensive report.</p> <p>6.2 Report includes identified vulnerabilities, corrective actions taken, and residual risks.</p> <p>6.3 Security performance metrics and incident response outcomes are documented.</p> <p>6.4 Compliance with organizational policies, legal, and regulatory standards is verified and included in the report.</p> <p>6.5 Recommendations for continuous improvement and future security enhancements are outlined.</p> <p>6.6 Report is formatted according to organizational templates and presented to relevant stakeholders.</p> <p>6.7 Documentation is stored securely and updated regularly to reflect changes in the application's security posture.</p> |

## 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                                                                                                                                                                    |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software applications for assessment may include but not limited to: | <ul style="list-style-type: none"> <li>• Database applications</li> <li>• Web applications</li> <li>• Mobile applications</li> <li>• Cloud-based applications</li> </ul> |