SECURE SOFTWARE APPLICATION

UNIT CODE: SEC/OS/CS/CR/04/6/A

UNIT DESCRIPTION

This unit covers the competencies required to secure software application. Competencies includes: 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

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. ***(Bold and italicised terms are elaborated in the Range)***
1. Identify software to be secured	1.1 Software is identified in line with manufacturers 1.2 Software use is established as per its applications 1.3 Software platform diversity is established according to manufactures user guides
2. Establish tools for application security assessment	2.1 Types of tools are identified according to the platform of use 2.2 Network communication is adhered to in tools identification 2.3 Tools are identified as per their availability and cost 2.4 Tools are identified as per the data size 2.5 Tools are identified according to the environment of use. 2.6 Tools identification is performed as per the nature of the software 2.7 Tools are established as per the type of hardware and software 2.8 Tools are selected as per the expected outcome of the application security assessment.
3. Perform application security assessment	3.1 Application assessment is performed in line with national and international standards 3.2 Application assessment is conducted as per the ISO 27001 3.3 Assessment is performed in line with NIST
4. Harden software application	4.1 Configuration is performed as per the manufacturers guide, ICT regulations and industries best practice

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. ***(Bold and italicised terms are elaborated in the Range)***
	4.2 ***Security measures*** are put around the software according ICT policy 4.3 Access control measures are set up in line organizations ICT policy 4.4 Valid licenses are installed in software as per the manufacturer's guides 4.5 Software is monitored continuously as per its operations 4.6 Security updates and patches are installed in line with manufacturers guidelines 4.7 Environment of software use is secured as per the organization policy
5. Monitor application security performance	5.1 Monitoring solution is implemented in line with organization policy 5.2 Logs are monitored as per the organization ICT policy 5.3 Continuous security assessment is conducted as per the industries best practice 5.4 Application security performance is measured in line with its uptime period
6. Prepare a report on software security	6.1 Software security reports are prepared in line with the organizations approved format 6.2 Software security reports are shared with relevant parties as per the organization policy 6.3 Software security reports are documented and filled according organization filing system 6.4 Software security risk mitigation recommendations are prepared and shared with the relevant parties

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 components and infrastructure may include but not limited to:	• Software • Hardware • People • Data • Procedures • Information

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • 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 Software was identified in line with manufacturers 1.2 Software use was established as per its applications 1.3 Tools identification was performed as per the nature of the software 1.4 Application assessment was performed in line with OWASP 1.5 Configuration was performed as per the manufactures guide, ICT regulations and industries best practice 1.6 Valid licenses were installed in software as per the manufacturer's guides 1.7 Security updates and patches were installed in line with manufacturers guidelines 1.8 SIEM solution was implemented in line with organization policy 1.9 Software security reports were shared with relevant parties as per the organization policy 1.10 Environment of software use is secured as per the organization policy
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.