SOFTWARE APPLICATION SECURITY

UNIT CODE: SEC/CU/CU/CR/06/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Secure software application

Duration of Unit: 110 hours

Unit Description
This unit covers the competencies required to secure software application. It involves identifying software to be secured, establishing tools for application security assessment, perform application security assessment, hardening software application, monitoring application security performance, performing application security configuration and preparation of reports on software security.

Summary of Learning Outcomes

1. Identify software to be secured
2. Establish tools for application security assessment
3. Perform application security assessment
4. Harden software application
5. Monitor application security performance
6. Prepare a report on software security

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	Content	Suggested Assessment Methods
1. Identify software to be secured	• Meaning of Terms • Types of software • Classification of software and their application • Factors influencing software selection • Software operation platform	• Observation • Written tests • Oral questioning • Practical tests

2. Establish tools for application security assessment	• Meaning of terms
	• Types of tools used in software application security assessment
	  • Network communication in tools selection
	• Platform vulnerability
	• Factors to consider in selection security assessment tools
	  • Tool data size in tools selection
		• Observation
		• Written tests
		• Oral questioning
		• Practical tests

Learning Outcome	Content	Suggested Assessment Methods
	• Environment • Software and Hardware	
3. Perform application security assessment	• Meaning of terms • Types of known standards in application security assessment • Best practice standards in application security assessment	• Observation • Written tests • Oral questioning • Practical tests
• Harden software application	• Meaning of terms • Software configuration • Factors to consider in software hardening • Policies and regulations software hardening • Security measures in software application • Elements of security in software hardening • Licenses in software installation • Software monitoring process • Installation of patches, upgrades and updates in software hardening • Purposes of environment in software hardening	• Observation • Written tests • Oral questioning • Practical tests
5. Monitor application security performance	• Meaning of terms • Factors to consider in monitoring of application security performance • Implementation of monitoring solutions • Logs management and monitoring • Measurement of application security performance	• Observation • Written tests • Oral questioning • Practical tests
6. Prepare a report on software security	• Meaning Testing • Report preparation • Report dissemination • Report filing	• Observation • Written tests • Oral questioning • Practical tests

Suggested Methods of Instructions
- Demonstration by trainer
- Practice by the trainee
- Discussions

Recommended Resources

Equipment	Materials and supplies
• Computers • Printers • Cameras • Phones • Photocopiers	• Stationery •
Reference materials • Manufacturers' manuals • Relevant catalogues • Tables • National and international standards	