MANAGEMENT OF SECURITY OPERATIONS

UNIT CODE: SEC/CU/CS/CR/11/6/A

Relationship to Occupational Standards
This unit addresses the unit of competency: Manage security operations

Duration of Unit: 110 hours

Unit Description
This unit covers the competencies required to manage security operations. It involves gathering information asset inventory, implementing a security management solution, establishing threats landscape, responding to established threats, monitoring events in the landscape and generating security operation report.

Summary of Learning Outcomes

1. Gather information asset inventory
2. Implement a security management solution
3. Establish threats landscape
4. Respond to established threats
5. Monitor events in the landscape
6. Generate security operations report

Learning Outcomes, Content and Suggested Assessment Methods

Learning Outcome	**Content**	**Suggested Assessment Methods**
1. Gather information about organization and its systems	• Meaning of terms • Information assets inventory • Determination of asset value • Classification of information assets	• Observation • Oral questioning • Practical tests • Written tests
2. Implement a security management solution	• Meaning of terms • Acquisition of security management system • Security management solution deployment • Security management configuration • Security management system hardening • Dashboard/Portal configuration	• Observation • Oral questioning • Practical tests • Written tests
3. Establish threats landscape	• Meaning of terms • Threats identification and modelling • Threat mitigation measures	• Observation • Oral questioning • Practical tests • Written tests

Learning Outcome	Content	Suggested Assessment Methods
4. Respond to identified threats	• Meaning of terms • Reporting procedure • Incidence handling and response • Business continuity plan	• Observation • Oral questioning • Practical tests • Written tests
5. Monitor security events in the landscape	• Meaning of team • SIEM implementation • Technical users awareness training • Updating, upgrading and patching of security management system • Simulation of threats and monitoring	• Observation • Oral questioning • Practical tests • Written tests
6. Generate security operations report	• Report preparation • Report dissemination • Report filing	• Observation • Oral questioning • Practical tests • Written tests

Suggested Methods of Instructions

- Demonstration by trainer
- Practice by the trainee
- Field trips
- Discussions

Recommended Resources

Equipments	**Materials and supplies**
• SOC • CERT • Computer • Mobile phone • Radio frequency receivers	• Stationery • Software and hardware • Cloud • Working platform
Reference materials • Internet • Manufacturers’ manuals • Installation manuals • NIST cyber security framework framework • KE-CERT	