MANAGE SECURITY OPERATIONS

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

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.

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. Gather information asset inventory	1.1 Capacity of the organization is established as per the information required 1.2 Assets in the organization are established in line with industry best practice 1.3 Assets are classified according to organization ICT policy
2. Implement a security management solution	2.1 Security management solution is acquired according to the context of the information gathered 2.2 Security management solution is deployed as per manufacturers guides 2.3 Security management solution is set up and configured in line with the organization ICT policy 2.4 Configuration are verified and hardened as per the industry best practices 2.5 Workspaces and dashboards are set up in line with the manufacturers guide and industry best practices
3. Establish threats landscape	3.1 Common threats are established in line with the installed dashboards 3.2 Reasons for presence of the threats identified are analysed as per the workplace procedures 3.3 Mitigation measures of the threats identified are implemented as per the organization ICT policy and industry best practice.
4. Respond to identified threats	4.1 Share the established threats with CIRT/CERT as per the organization ICT policy 4.2 Quarantine or removal of the established threats is performed in line with workplace procedures 4.3 System is kept live as per the organization ICT

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)***
	policy 4.4 Participate in creation and implementation of business continuity plan in line with the organization policy
5. Monitor events in the landscape	5.1 Continuous monitoring of events is performed as per the implemented security management system 5.2 System user awareness is conducted in line with the organization policy 5.3 Security system, hardware and software are kept up to date as per the organization policy 5.4 Simulation of threats is performed on the system and response monitored as per the organization policy
6. Generate security operations report	6.1 Security operation reports are prepared in line with the organizations approved format 6.2 Security operation reports are shared with relevant parties as per the organization policy 6.3 Security operation reports are documented and filled according organization filing system 6.4 Security operation 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

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 • 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 Security management solutions were deployed as per manufacturers guides 1.2 Security management solutions were set up and configured in line with the organization ICT policy 1.3 Configuration were verified and hardened as per the industry best practices 1.4 Mitigation measures of the threats identified were implemented as per the organization ICT policy and industry best practice. 1.5 Established threats were shared with CIRT/CERT as per the

	organization ICT policy 1.6 Quarantine or removal of the established threats was performed in line with workplace procedures 1.7 Security system, hardware and software were kept up to date as per the organization policy 1.8 Simulation of threats was performed on the system and response monitored as per the organization policy 1.9 Security operation reports were shared with relevant parties as per the organization policy
2. Resource Implications for competence 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	4.1 Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	5.1 Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.