MANAGE CYBER SECURITY RISKS

UNIT CODE: SEC/OS/CS/CR/09/6/A

UNIT DESCRIPTION

This unit covers the competencies required to manage cyber security risks. It involves establishing risk context, identify risk factors, implementing contingency plans, monitoring and updating risk profiles and reporting of risk profiles.

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. Establish Risk context	1.1 ***Infrastructure*** is identified as per the organizations network scope 1.2 Types of assets used in the organization are established in line with the size of the organization 1.3 Organization’s security awareness is established in line with its staff 1.4 Risk context is established as per the organizations cyber security policies
2. Identify Risk factors	2.1 Risk factors are identified as per the organization cyber security policy 2.2 Risk factors are assessed in line with the manufacturer’s manuals 2.3 Risk factors are identified as per the organizations ICT policy and cyber security related equipment 2.4 Risk factors are classified as per their impact 2.5 Information access is assessed as per the organization policy 2.6 Risk factors are identified according to National and international standards
3. Implement contingency plans	3.1 ***Contingency plans*** are implemented as per the systems operation manuals 3.2 Back up measures are implemented as per the organization policy 3.3 Data loss prevention measures are implemented according to organization policy and rules and regulation 3.4 Communication contingency plans are adhered to in sharing of the information within and outside the

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)***
	organization 3.5 Intrusion detection and prevention measures are implemented according to organization best practices. 3.6 Contingency plans are simulated in adherence to the expected efficiency
4. Monitor and update risk profile	4.1 Risk calculation is performed as per the standard operating procedures 4.2 Automated security operation centres and monitor the risk factors as per the standard operating procedures 4.3 System users are continuously trained on trends in cyber security issues in line with the organizations policy 4.4 Risk profile is updated in line with simulated risk factors 4.5 Risk monitoring and updates are performed according to systems manufacturer's security updates
5. Report risk profile	5.1 Risk reports are prepared in line with the organizations approved format 5.2 Risk reports are shared with relevant parties as per the organization policy 5.3 Risk reports are documented and filled according organization filing system 5.4 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. infrastructure may	• People • Data

Variable	Range
include but not limited to:	• Procedures • Information
2. Contingency plans may include but not limited to:	• Incidence response • Cyber threats intelligence • Business continuity plans • Disaster recovery plans • Back up stratey

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
- Government ICT policies and regulations
- Government policies and regulation
- Applicable laws and regulations

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; • Creativity • Self-driven

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 Risk assets established as per the organizations cyber security policy 1.2 Organization security awareness established as per its staff 1.3 Risk assets assessed in line with manufacturers manual 1.4 Information access is assessed as per the organization policy 1.5 Contingency plans implemented as per system operating manual 1.6 Implemented back up measures as per the organization policy 1.7 Implemented data loss prevention measures according to organization policy and rules and regulation 1.8 Performed risk calculations as per the standard operating procedures 1.9 Updated risk profile in line with simulated risk factors 1.10 Risk reports are documented risk reports and filled according to organization filing system
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	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.