UNIT CODE: SEC/OS/CS/CR/06/6/A

UNIT DESCRIPTION

This unit covers the competencies required to administer cyber security system. It involves identifying and analysing information to be protected, establishing systems to be administered, assessing system compatibility, monitoring system performance, documenting system administration report and establishing a cyber-security backup and restoration plan.

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 and analyze information to be protected	1.1 Platform of the information location is established as per the organization policy 1.2 Information attributes of the organization is determined in line with the organization policy 1.3 Technology used in information storage is established as per the organization policy 1.4 Information access control is established in line with organization policy 1.5 Information or data to be protected is analyzed in line with the ***Cyber security policy*** and regulations
2. Establish systems to be administered	2.1 System is established as per the scope of the information to be protected 2.2 Existing ***threats*** and trends are considered in establishing the security system to be installed as per the industry best practice 2.3 Hardware and software requirements are established in line with the system to be installed
3. Asses system's compatibility	3.1 ***Cyber security system*** is assessed for compatibility with the cyber security devices and equipment 3.2 Components specification are checked in line with the entire cyber security system 3.3 System is assessed in line with the manufacturers manual and organizations objectives
4. Monitor system performance	4.1 System effectiveness is monitored periodically in line with the operation manual and cyber security policy 4.2 Simulations are performed during system

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)***
	monitoring period as per the organization policy 4.3 Logs are continuously analysed and reported as per the organization cyber security policy 4.4 System security updates and patches are installed according to manufacturer’s manuals and organization cyber security policy
5. Document system administration report	5.1 Installation and operation report are prepared and shared with the relevant parties 5.2 Prepared report is filled as per the organizations cyber security policy
6. Establish a cyber security back up and restoration plan	6.1 Location for the backup is identified as per the organization policy and industry best practice 6.2 Information to be backed up is established as per the organization cyber security policy 6.3 Back up platform is established in line with the organization policy 6.4 Performance validation of the backups is performed as per the organization cyber security policy 6.5 Measures on creating backup schedules are developed in line with the industry best practice

RANGE

This section provides work environment and conditions to which the performance criteria apply. It allows for different work environment and situations that will affect performance.

Variable	**Range**
Security threats includes but not limited to:	• Malicious hackers • Industrial espionage • Employee sabotage • Fraud and theft • Loss of physical and infrastructure support • Errors and Omissions
Cyber Security system	• Knowledge management system

Variable	Range
includes but not limited to:	- Firewalls instruction detection system

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Cyber Security risk management techniques and procedures
- Types of security threats and their control measures
- Cyber security audit procedures
- Cyber security policy
- Strategies for Mitigating risks
- Categories of Security threats
- Penetration testing skills

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:	
• Communications (verbal and written); • Time management; • Penetration Skills • 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 Considered existing threats and trends in establishing the security system to be installed 1.2 System to be installed was established with self-defensive mechanism 1.3 Components specification were checked in line with the entire cyber security system 1.4 System was installed and configured as per the manufacturers manual 1.5 Established testing types as per the standard operating procedure 1.6 Performed simulations during system monitoring period as per the organization policy

	1.7 Continuously analysed logs and reported as per the organization cyber security policy 1.8 Establish back up platforms in line with the organization policy 1.9 Performed validation of the backups as per the organization ICT policy 1.10 Developed back up schedule as per the organization cyber security policy 1.11 Training manual was prepared and shared with the system users
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 Observation 3.2 Oral questioning 3.3 Practical test in conducting test 3.4 Demonstration of interpretation of test results
4 Context of Assessment	Competency may be assessed individually 4.1 In the actual workplace 4.2 Simulated environment of the work place
5 Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.