DEMONSTRATE UNDERSTANDING OF CYBER SECURITY LAWS, POLICIES AND REGULATIONS

UNIT CODE: SEC/OS/CS/CR/02/6/A

UNIT DESCRIPTION

This unit covers the competencies required in applying Cyber security laws, policies and regulations. It involves demonstrating the understanding of different cyber security policies and regulations, developing cyber security policy, implementing Cyber security policies and regulations, evaluating Cyber security policies, evaluating compliance in Cyber security policies and regulations and monitoring effectiveness of Cyber security policy in an organization.

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. Demonstrate understanding of cyber security laws, polices and regulation	1.1 Different cyber security laws are identified based on the available world's legal systems. 1.2 Various types of cyber-crimes are identified based on the existing and emerging treaths 1.3 Cyber crime laws are identified based on the country's legal framework. 1.4 Cyber security laws are applied as per the country's legal system 1.5 Cyber security laws are complied with as per the organizations or country's legal framework. 1.6 Impacts of cyber crimes are identified according to country's social economic factors 1.7 Application of different cyber security policies are determined as per the industry best practice 1.8 Policies and regulation stakeholders are identified
2. Develop Cyber Security policy	2.1 ***Infrastructure and components*** for cyber security policy are identified and classified 2.2 Nature and operations of the business aligned to the policy is established 2.3 Draft cyber security policy is developed in line with the known industrial standards and the laws of the land 2.4 Review drafted cyber security policy in line with the industry best practice
3. Implement Cyber Security	3.1 Cyber security policy is adopted for implementation as per the organization requirements

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 and regulations	3.2 Cyber security policy implementation team is constituted in line with the organization requirements 3.3 Implementation schedule is prepared as per the organization requirement 3.4 Initiation of the cyber security policy implementation schedule is performed in line with organization policies 3.5 Cyber security policy implementation process is monitored in line with the established schedule 3.6 Cyber security policy and regulation implementation is verified as per the substantive law and organization policies
4. Evaluate Cyber security policy	4.1 Continuous review and updates of cyber security policy is performed in line with organization requirements 4.2 Cyber security policy is evaluated in line with the cyber security emerging trends
5. Evaluate compliance in Cyber security policy and regulations	5.1 ***Infrastructure landscape*** is audited in line with the organization Cyber security policy and regulations 5.2 Risk factors for non-compliance are calculate as per the industry best standards 5.3 Recommendation is reported on the compliance level as per the policy and regulations
6. Monitor effectiveness of Cyber security policy in an organization	6.1 Adoption levels are determined in line with organization requirements 6.2 Cyber security policy impact on technologies, process and people within the organization is monitored as per the organization policy. 6.3 Effectiveness of the Cyber security policy implemented is monitored in line with organization requirement

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
1. Components and infrastructure may include but not limited to:	• Software • Hardware • People • Data • Procedures • Information
2. Organization landscape may includes but not limited to:	• People • Process • Technology

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- Cyber security infrastructure auditing procedures
- Cyber security safety and precautious measures
- Cyber security prevention measures
- Performance monitoring techniques
- Cyber security policy
- Causes of hardware and software failure
- Components of cyber security 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 • 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 Identified different types of cyber security policies and regulations 1.2 Determined application of different cyber security policies as per the industry best practice 1.3 Developed a draft of cyber security policy in line with the known industrial standards and the laws of the land 1.4 Prepared implementation schedule as per the organization requirement 1.5 Evaluated cyber security policy line with the cyber security trends 1.6 Calculated risk factors for non-compliance as per the industry best standards

	1.7 Reported recommendations on the compliance level as per the policy and regulations 1.8 Monitored Cyber security policy impact on technologies, process and people within the organization as per the organization policy 1.9 Monitored effectiveness of the Cyber security policy implementation in line with the organization requirement 1.10 Performed audit on existing cyber security components and infrastructure 1.11 Verified drafted cyber security policy in line with the standard operating procedure
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 Written tests 3.3 Practical demonstration 3.4 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.