COMPETENCY STANDARDS

CYBER THREAT MONITORING LEVEL I

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECTOR

TECHNICAL EDUCATION AND SKILLS DEVELOPMENT AUTHORITY
East Service Road, South Luzon Expressway (SLEX), Taguig City, Metro Manila

Technical Education and Skills Development Act of 1994
(Republic Act No. 7796)

Section 22, “Establishment and Administration of the National Trade Skills Standards” of the RA 7796 known as the TESDA Act mandates TESDA to establish national occupational skills standards. The Authority shall develop and implement a certification and accreditation program in which private industry group and trade associations are accredited to conduct approved trade tests, and the local government units to promote such trade testing activities in their respective areas in accordance with the guidelines to be set by the Authority.

The Competency Standards (CS) serve as basis for the:

1 Competency assessment and certification;
2 Registration and delivery of training programs; and
3 Development of curriculum and assessment instruments.

Each CS has two sections:

Section 1 **Definition of Qualification** – describes the qualification and defines the competencies that comprise the qualification.

Section 2 The **Competency Standards** format was revised to include the Required Knowledge and Required Skills per element. These fields explicitly state the required knowledge and skills for competent performance of a unit of competency in an informed and effective manner. These also emphasize the application of knowledge and skills to situations where understanding is converted into a workplace outcome.

TABLE OF CONTENTS
ICT SECTOR

CYBER THREAT MONITORING LEVEL I

COMPETENCY STANDARDS FOR
CYBER THREAT MONITORING LEVEL I

Section 1 DEFINITION OF QUALIFICATION

The Cyber Threat Monitoring Level I qualification consists of competencies that a person must achieve to monitor and report cyber threats and to conduct vulnerability scanning of assets.

The units of competency comprising this qualification include the following:

UNIT CODE	BASIC COMPETENCIES
400311101	Receive and respond to workplace communication
400311102	Work with others
400311103	Solve/address routine problems
400311104	Enhance self-management skills
400311105	Support innovation
400311106	Access and maintain information
400311107	Follow occupational safety and health policies and procedures
400311108	Apply environmental work standards
400311109	Adopt entrepreneurial mindset in the workplace

UNIT CODE	COMMON COMPETENCIES
ICT315202	Apply quality standards
ICT311203	Perform Computer Operations

UNIT CODE	CORE COMPETENCIES
CS-ICT251101	Monitor and report cyber threats
CS-ICT251102	Conduct vulnerability scanning of assets

A person who has achieved this Qualification is competent to be:

- Cybersecurity analyst (L1)
- Cybersecurity support staff
- Cybersecurity help desk staff

SECTION 2 COMPETENCY STANDARDS

This section gives the details of the contents of the basic, common and core units of competency required in **Cyber Threat Monitoring Level I.**

BASIC COMPETENCIES

UNIT OF COMPETENCY: RECEIVE AND RESPOND TO WORKPLACE COMMUNICATION
UNIT CODE : 400311101
UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to receive, respond and act on verbal and written communication.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Follow routine spoken messages	1.1 Required information is gathered by listening attentively and correctly interpreting or understanding information/ instructions 1.2 Instructions/ information are recorded in accordance with workplace requirements 1.3 Instructions are acted upon immediately in accordance with information received 1.4 Clarification is sought from workplace supervisor on all occasions when any instruction/ information is not clear	1.1. Organizational policies/guidelines in regard to processing internal/external information 1.2. Ethical work practices in handling communications 1.3. Overview of the Communication process 1.4. Effective note-taking and questioning techniques	1.1. Conciseness in receiving and clarifying messages/ information/ communication 1.2. Accuracy in recording messages/ information 1.3. Basic communication skills 1.4. Active-listening Skills 1.5. Note-taking skills 1.6. Clarifying and probing questions (questioning skills)
2. Perform workplace duties following written notices	2.1 ***Written notices and instructions*** are read and interpreted correctly in accordance with **organizational guidelines** 2.2 Routine written instructions are followed in sequence 2.3 Feedback is given to workplace supervisor based on the instructions/ information received	2.1 Organizational guidelines in regard to processing internal/ external information 2.2 Ethical work practices in handling communications 2.3 Overview of the Communication process 2.4 Effective questioning techniques (clarifying and probing)	2.1 Conciseness in receiving and clarifying messages/ information/ communication 2.2 Accuracy in recording messages/ information 2.3 Clarifying and probing questions (Questioning Skills) 2.4 Skills in reading and recording and labeling data 2.5 Skills in locating information

RANGE OF VARIABLES

VARIABLE	RANGE
1. Written notices and instructions	May include: 1.1. Written work instructions 1.2. Internal memos/memorandum 1.3. Business letters 1.4. External communications 1.5. Electronic mail 1.6. Briefing notes 1.7. General correspondence 1.8. Marketing materials 1.9. Guidelines/Circulars
2. Organizational guidelines	May include: 2.1. Information documentation procedures 2.2. Company guidelines and procedures 2.3. Standard Operating Procedure (SOPs) 2.4. Organization manuals 2.5. Departmental Policies and Procedures Manual 2.6. Service manual

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Demonstrated knowledge and understanding of organizational procedures in handling verbal and written communications 1.2. Received and acted on verbal messages and instructions correctly and efficiently 1.3. Demonstrated ability in recording instructions/information 1.4. Utilized effective clarifying and probing techniques where necessary
2. Resource Implications	The following resources should be provided: 2.1. Pens 2.2. Note pads 2.3. Computer (if applicable)
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Demonstration on communication skills (e. g., role-playing) 3.2. Oral questioning/Interview 3.3. Written Test
4. Context for Assessment	4.1. Competency may be assessed individually in the actual workplace or in a simulated environment in TESDA-accredited institutions

UNIT OF COMPETENCY : WORK WITH OTHERS
UNIT CODE : 400311102
UNIT DESCRIPTOR : This unit covers the skills, knowledge and attitudes required in working as member of a team, interacting with co-members and performing one's role in the team.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Develop effective workplace relationships	1.1. ***Duties and responsibilities*** are done in a positive manner to promote cooperation and good relationship 1.2. Assistance is sought from ***workgroup*** when difficulties arise and addressed through discussions 1.3. ***Feedback*** provided by others in the team is encouraged, acknowledged and acted upon 1.4. Differences in personal values and beliefs are respected and acknowledged during interaction	1.1. One's role, duties and responsibilities in the workplace 1.2. Acknowledging/ receiving and giving feedback 1.3. Valuing respect and empathy in the workplace 1.4. Workplace communication protocols 1.5. Teamwork 1.6. Collaboration and teambuilding within the enterprise	1.1. Communication skills – oral and written (e. g., requesting advice, receiving feedback) 1.2. Ability to relate to/interact with people from a range of social and cultural backgrounds
2. Contribute to work group activities	2.1. ***Support is provided to team members*** to ensure workgroup goals are met 2.2. Constructive contributions to workgroup goals and tasks are made according to ***organizational requirements*** 2.3. Information relevant to work is shared with team members to ensure designated goals are met	2.1. Importance of creative collaboration, social perceptiveness and problem sensitivity in the workplace 2.2. Organizational Requirements 2.3. Importance of initiative and dedication in group process 2.4. Office and workplace technologies and automation (hardware, software systems)	2.1. Communication skills – oral and written (e. g., requesting advice, receiving feedback) 2.2. Organizing work priorities and arrangements 2.3. Team player skills 2.4. Technology skills including the ability to select and use technology appropriate to a task

RANGE OF VARIABLES

VARIABLE	RANGE
1. Duties and responsibilities	May include: 1.1 Job description and employment arrangements 1.2 Organization's policy relevant to work role 1.3 Organizational structures 1.4 Supervision and accountability requirements including OHS 1.5 Enterprise code of conduct
2. Work group	May include: 2.1 Supervisor or manager 2.2 Peers/work colleagues and clients 2.3 Other members of the organization
3. Feedback	May include: 3.1 Formal/Informal performance appraisal 3.2 Obtaining feedback from supervisors and colleagues and clients 3.3 Personal, reflective behavior strategies 3.4 Routine organizational methods for monitoring service delivery
4. Providing support to team members	May include: 4.1 Explaining/clarifying 4.2 Helping colleagues 4.3 Providing encouragement 4.4 Providing feedback to another team member 4.5 Undertaking extra tasks if necessary
5. Organizational requirements	May include: 5.1 Goals, objectives, plans, system and processes 5.2 Legal and organization policy/guidelines 5.3 OHS policies, procedures and programs 5.4 Ethical standards 5.5 Defined resources parameters 5.6 Quality and continuous improvement processes and standards

EVIDENCE GUIDE

1. Critical aspects of competency	**Assessment requires evidence that the candidate:** 1.1. Provided support to team members to ensure goals are met 1.2. Acted on feedback from clients and colleagues 1.3. Demonstrated quality/active participation in team meetings and activities
2. Resource Implications	**The following resources should be provided:** 2.1. Access to relevant workplace or appropriately simulated environment where assessment can take place 2.2. Materials relevant to the proposed activity or task
3. Methods of Assessment	**Competency in this unit may be assessed through:** 3.1 Written Test 3.2 Role play 3.3 Interview/Oral questioning 3.4 Structured and unstructured activity
4. Context for Assessment	4.1. Competency assessment may occur in workplace or any appropriately simulated environment 4.2. Assessment shall be observed while task are being undertaken whether individually or in group

UNIT OF COMPETENCY : SOLVE/ADDRESS ROUTINE PROBLEMS
UNIT CODE : 400311103
UNIT DESCRIPTOR : This unit of covers the knowledge, skills and attitudes required to solve problems in the workplace including the application of problem solving techniques and to determine and resolve the root cause of routine problems.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify the problem	1.1. Desired operating/output parameters and expected quality of products/services are identified. 1.2. The nature of the problem by observation on routines are defined. 1.3. ***Problems*** are stated and specified clearly.	1.1. Competence includes mastery of knowledge and understanding of the process, normal operating parameters, and product quality to recognize non-standard situations 1.2. Competence to include the ability to apply and explain fundamental causes of problems routine problems and to determine the corrective actions. 1.3. Relevant equipment and operational processes 1.4. Enterprise goals, targets and measures 1.5. Enterprise quality OHS and environmental requirement 1.6. Enterprise information systems and data collation 1.7. Industry codes and standards	1.1. Using range of formal problem-solving techniques (e.g., planning, attention, simultaneous and successive processing of information). 1.2. Identifying and clarifying the nature of the problem.
2. Assess fundamental causes of the problem	2.1. Problem-solving tool appropriate to the problem and the context is selected 2.2. Possible causes based on experience and the use of problem-solving tools/***basic analytical techniques*** are identified 2.3. Possible fundamental causes of problems are specified.	2.1 Competence includes a thorough knowledge and understanding of the process, normal operating parameters, and product quality to recognize non-standard situations 2.2 Competence to include the ability to apply and explain fundamental causes of problems routine problems and to determine the corrective actions. 2.3 Relevant equipment and operational processes 2.4 Enterprise goals, targets and measures	2.1 Using range of formal problem-solving techniques (e.g., planning, attention, simultaneous and successive processing of information). 2.2 Identifying extent and causes of procedural problems.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
		2.5 Enterprise quality OHS and environmental requirement 2.6 Enterprise information systems and data collation 2.7 Industry codes and standards	
3. Determine corrective action	3.1. All possible options are considered for resolution of the routine problem. 3.2. Corrective actions are determined to resolve the problem and possible future causes 3.3. ***Action plans*** are developed identifying measurable objectives, resource needs and timelines in accordance with safety and operating procedures	3.1. Competence includes a thorough knowledge and understanding of the process, normal operating parameters, and product quality to recognize non-standard situations 3.2. Competence to include the ability to apply and explain, sufficient for the identification of fundamental cause, determining the corrective action and provision of recommendations 3.3. Relevant equipment and operational processes 3.4. Enterprise goals, targets and measures 3.5. Enterprise quality OHS and environmental requirement 3.6. Principles of decision making strategies and techniques 3.7. Enterprise information systems and data collation 3.8. Industry codes and standards	3.1. Using range of formal problem-solving techniques. 3.2. Identifying and clarifying the nature of the problem. 3.3. Devising and applying the best possible solution to a problem. 3.4. Evaluating the solution
4. Communicate action plans and recommendations to routine problems	4.1. Report on recommendations are prepared 4.2. Recommendations are presented to ***appropriate person***. 4.3. Recommendations are followed-up, if required	4.1. Competence includes a thorough knowledge and understanding of the process, normal operating parameters, and product quality to recognize non-standard situations 4.2. Competence to include the ability to apply and explain, sufficient for the identification of fundamental cause, determining the corrective action and provision of recommendations	4.1. Using range of formal problem solving techniques 4.2. Identifying and clarifying the nature of the problem 4.3. Devising the best possible solution to a routine problem 4.4. Evaluating the solution 4.5. Developing action plans to

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
		4.3. Relevant equipment and operational processes 4.4. Enterprise goals, targets and measures 4.5. Enterprise quality, OHS and environmental requirement 4.6. Principles of decision-making strategies and techniques 4.7. Enterprise information systems and data collation 4.8. Industry codes and standards	resolving and managing routine problems.

RANGE OF VARIABLES

VARIABLES	RANGE
1. Problem	May include: 1.1. Routine/non – routine processes and quality problems 1.2. Equipment selection, availability and failure 1.3. Teamwork and work allocation problem 1.4. Safety and emergency situations and incidents
2. Basic analytical techniques	May include: 2.1. Brainstorming 2.2. Case Analysis 2.3. Cause and effect diagrams 2.4. Pareto analysis 2.5. SWOT analysis 2.6. Gant chart, Pert CPM and graphs 2.7. Scattergrams
3. Action plans	May include: 3.1. Priority requirements 3.2. Measurable objectives 3.3. Resource requirements 3.4. Timelines 3.5. Co-ordination and feedback requirements 3.6. Safety requirements 3.7. Risk assessment 3.8. Environmental requirements
4. Appropriate person	May include: 4.1 Supervisor or manager 4.2 Peers/work colleagues 4.3 Other members of the organization

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Identified the problem. 1.2. Determined the fundamental causes of the problem. 1.3. Determined the correct / preventive action. 1.4. Developed action plans in managing routine problems. These aspects may be best assessed using project-based learning mode of assessment and case formulation.
2. Resource Implications	Assessment will require access to a workplace over an extended period, or a suitable method of gathering evidence of operating ability over a range of situations.
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Case Formulation 3.2. Life Narrative Inquiry (Interview) 3.3. Standardized test The unit will be assessed in a holistic manner as is practical and may be integrated with the assessment of other relevant units of competency. Assessment will occur over a range of situations, which will include disruptions to normal, smooth operation. Simulation may be required to allow for timely assessment of parts of this unit of competency. Simulation should be based on the actual workplace and will include walk through of the relevant competency components. These assessment activities should include a range of problems, including new, unusual and improbable situations that may have happened.
4. Context for Assessment	4.1 Competency may be assessed individually in the actual workplace or simulation environment in TESDA accredited institutions

UNIT OF COMPETENCY : ENHANCE SELF-MANAGEMENT SKILLS
UNIT CODE : 400311104
UNIT DESCRIPTOR : This unit covers the knowledge, skills, and attitudes in applying the ability to regulate actions, make good decisions, and show appropriate behavior based on self-awareness.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Set personal and career goals	1.1. The difference between ***personal*** and ***career goals*** are described 1.2. Clear and concise personal and career goals are developed 1.3. Characteristics of motivational goals according to Locke &Latham are identified	1.1. Definition of personal goals and career goals 1.2. SMART Model for goal setting 1.3. Five principle of goal setting according to Locke & Latham (Clarity, Challenge, Commitment, Feedback, and Task complexity)	1.1. Setting of personal and career goals 1.2. Defining, creating, and mapping personal and career goals using SMART Model for goal setting 1.3. Applying goal setting principles to personal and career goals
2. Recognize emotions	2.1. Influence that people, situations and events have on ***emotions*** are described 2.2. Importance of responding with appropriate emotions are explained 2.3. Influences on and consequences of emotional responses in a ***social and work-related contexts*** are examined	2.1. Common positive and negative emotions manifested in the workplace 2.2. Professional and non-professional behaviors in the workplace 2.3. Triggers and implications of positive and negative emotions in the workplace	2.1. Identifying sensitively the positive and negative emotions in the workplace 2.2. Responding with appropriate emotions in the workplace 2.3. Identifying possible consequences of inappropriate emotional responses in a social and work-related context
3. Describe oneself as a learner	3.1. Factors and strategies that assist learning are identified and described 3.2. Preferred **learning styles** according to VAK Learning Style Model and Kolb's Theory of Learning Styles are identified 3.3. Range of **learning strategies** appropriate to specific tasks and describe work practices that assist their learning are identified and chosen	3.1. Kolb's Theory of Learning Styles (Converger, Diverger, Assimilator, Accommodator) 3.2. VAK Learning Style Model (Visual, Auditory, Kinesthetic) 3.3. Range of learning strategies appropriate to specific tasks and describe work practices that assist their learning	3.1. Identifying factors and strategies that assist learning 3.2. Applying learning styles to positively influence school/work performance 3.3. Using appropriate learning strategies to improve study habits and learning

RANGE OF VARIABLES

VARIABLE	RANGE
1. Personal goals	May include: 1.1. Graduate from Tech-Voc training 1.2. Buy a car 1.3. Travel around the world
2. Career goals	May include but not limited to: 2.1. Graduate from Tech-Voc training 2.2. Graduate from college 2.3. Buy a car 2.4. Retire at 50 years old
3. Emotions	Positive emotions may include: 3.1. Joy 3.2. Gratitude 3.3. Hope 3.4. Serenity Negative emotions may include: 3.5. Anger 3.6. Fear 3.7. Disgust 3.8. Sadness
4. Social and work-related contexts	May include professional behavior such as: 4.1. Committed to developing and improving their skills 4.2. Professionals get the job done 4.3. They keep their word and deliver what they promise. May include non-professional behavior such as– 4.4. They engage in office politics 4.5. Bluffing and misrepresenting their skills 4.6. Blaming a colleague
5. Learning styles	May include: 5.1. Visual 5.2. Auditory 5.3. Kinesthetic 5.4. Converger 5.5. Diverger 5.6. Assimilator 5.7. Accommodator
6. Learning strategies	May include: 6.1. Explain and describe ideas with many details 6.2. Switch between ideas while studying 6.3. Use specific examples to understand abstract ideas

EVIDENCE GUIDE

1. Critical aspects of Competency	**Assessment requires evidence that the candidate:** 1.1. Developed SMART personal and career goals 1.2. Applied goal setting principles 1.3. Identified sensitively the positive and negative emotions in the workplace 1.4. Responded with appropriate emotions in the workplace 1.5. Identified possible consequences of inappropriate emotional responses in a social and work-related context 1.6. Applied learning styles to positively influence school/work performance 1.7. Developed reflective practice through realization of limitations, likes/ dislikes; through showing of self-confidence
2. Resource Implications	The following resources for should be provided: 2.1. Access to workplace and resources
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Demonstration or simulation with oral questioning (ex. how to recognize emotions) 3.2. Case problems involving workplace diversity issues 3.3. Third-party report
4. Context for Assessment	4.1. Competency assessment may occur in workplace or any appropriately simulated environment

UNIT OF COMPETENCY : SUPPORT INNOVATION
UNIT CODE : 400311105
UNIT DESCRIPTOR : This unit of covers the knowledge, skills and attitudes required to identify, recognize and support innovation.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify the need for innovation in one's area of work	1.1. The value of **innovative practices** in the workplace is recognized 1.2. Creativity in **innovation** in one's scope of work is applied 1.3. The need for innovation in own scope of work is recognized	1.1. Clear-cut definition of innovation 1.2. Current practice in own scope of work 1.3. Workplace procedures	1.1. Contributing in brainstorming session 1.2. Examining current practice in one's scope of work 1.3. Identifying issues and concerns of one's scope of work
2. Recognize innovative and creative ideas	2.1. Opportunities within the team are identified to develop innovation 2.2. Creative ideas of coworkers pertaining to work practices are analyzed 2.3. Environment conducive for learning and innovating is maintained	2.1. Support required to generate creative ideas 2.2. Difference between innovation and creativity 2.3. Innovative climate in one's scope of work	2.1. Identifying resources required for creativity and innovation 2.2. Examining potential obstacles to and opportunities for creativity and innovation 2.3. Communicating creative ideas of co-workers
3. Support individuals' access to flexible and innovative ways of working	3.1. Individuals and key people are reinforced to identify innovative ideas to achieve outcomes 3.2. Sharing of best practices using flexible and innovative ways of working is accomplished 3.3. Obstacles to progress in implementing flexible and innovative ways of working are recognized	3.1. The role of employees/workers in the improvement of practices in the organization 3.2. Best practices using flexible and innovative ways of working 3.3. Obstacles in implementing innovation in one's scope of work	3.1. Encouraging co-workers to generate and develop ideas 3.2. Evaluating potential obstacles to and opportunities for creativity and innovation 3.3. Sharing of best practices related to innovation and creativity

RANGE OF VARIABLES

VARIABLE	RANGE
1. Innovative practices	May include: 1.1 Self-directed support 1.2 Community based services 1.3 Working within a collaborative arrangement 1.4 Making scope of work more efficient
2. Innovation	May include: 2.1 New ideas 2.2 Original ideas 2.3 Different ideas 2.4 Methods or tools

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Identified need for innovation in the area of work 1.2. Recognized innovative and creative ideas 1.3. Pursed agreement for flexible and innovative ways of working 1.4. Supported individuals and people to access flexible and innovative ways of working
2. Resource Implications	Specific resources for assessment 2.1. Evidence of competent performance should be obtained by observing an individual in an information management role within the workplace or operational or simulated environment.
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Written Test 3.2. Interview The unit will be assessed in a holistic manner as is practical and may be integrated with the assessment of other relevant units of competency. Assessment will occur over a range of situations, which will include disruptions to normal, smooth operation. Simulation may be required to allow for timely assessment of parts of this unit of competency. Simulation should be based on the actual workplace and will include walk through of the relevant competency components.
4. Context for Assessment	4.1. Competency may be assessed individually in the actual workplace or simulation environment in TESDA accredited institutions

UNIT OF COMPETENCY : ACCESS AND MAINTAIN INFORMATION
UNIT CODE : 400311106
UNIT DESCRIPTOR : This unit of covers the knowledge, skills and attitudes required to identify, gather, interpret and maintain information.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify and gather needed information	1.1. Required ***information*** is identified based on requirements. 1.2. Sources to produce required information are identified and accessed 1.3. Report information is collected, organized and recorded 1.4. Organize information is collected in a way that enables easy access and retrieval by other staff	1.1. Policies, procedures and guidelines relating to information handling in the public and private sector, including confidentiality, privacy, security, freedom of information 1.2. Data collection and management procedures 1.3. Cultural aspects of information and meaning 1.4. Sources of public sector work-related information 1.5. Public/private sector standards	1.1. Handling policies, procedures and guidelines relating to information handling in the public sector, including confidentiality, privacy, security, freedom of information 1.2. Collecting data and managing procedures 1.3. Practicing cultural aspects of information and meaning 1.4. Using public/private sector standards
2. Search for information on the internet or an intranet	2.1. Engine is search to find and select appropriate information 2.2. Suitable techniques is use to make it easier to find useful information and to pass it on to others 2.3. Records are use where useful information came from 2.4. Results are used for searches of useful information 2.5. ***Search engine*** is chosen appropriate for the information that is needed 2.6. Searches are carry out as per requirements	2.1. Find and select appropriate information 2.2. Techniques in finding useful information Records are use where useful information came from 2.3. Search engines for information	2.1. Finding and selecting search engine to find and select appropriate information 2.2. Using suitable techniques to find useful information easier 2.3. Using records 2.4. Carrying out Searches

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Examine information	2.5. Information and its ***sources*** are evaluated for relevance and validity to business and/or client requirements. 2.6. Information is examined as required to identify key issues. 2.7. Detailed evaluation of information is carried out as required using relevant techniques including mathematical calculations.	3.1. Data evaluation procedures 3.2. Cultural aspects of information and meaning 3.3. Sources of public sector work-related information 3.4. Public sector standards	3.1. Evaluating data 3.2. Practicing cultural aspects of information and meaning 3.3. Using public sector standards
4. Secure information	4.1. Basic file-handling techniques are used for the software 4.2. Techniques is used to handle, organize and secure information	4.1. Policies, procedures and guidelines relating to information handling in the public sector, including confidentiality, privacy, security, freedom of information 4.2. Basic file-handling techniques 4.3. Techniques in handling, organizing and saving files 4.4. Electronic and manual filing systems	4.1. Handling policies, procedures and guidelines relating to information handling in the public sector, including confidentiality, privacy, security, freedom of information 4.2. Using basic file-handling techniques is used for the software 4.3. Using different techniques in handling, organizing and saving files 4.4. Using electronic and manual filing systems
5. Manage information	5.1. Information and records are maintained to ensure data and system integrity using a range of standard and complex information systems and operations. 5.2. Routine data and records are reconciled as required. 5.3. Inadequacies in system/s relating to information retrieval are identified and corrected or reported to relevant staff as required.	5.1. Policies, procedures and guidelines relating to information handling in the public sector, including confidentiality, privacy, security, freedom of information 5.2. Data collection and management procedures 5.3. Organizational information handling and storage procedures 5.4. Cultural aspects of information and meaning	5.1. Handling policies, procedures and guidelines relating to information handling in the public sector, including confidentiality, privacy, security, freedom of information 5.2. Collecting data and managing procedures 5.3. Handling organizational information and storage procedures

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
		5.5. Sources of public sector work-related information 5.6. Public sector standards 5.7. Databases and data storage systems	5.4. Practicing cultural aspects of information and meaning 5.5. Using public sector standards 5.6. Managing databases and data storage systems

RANGE OF VARIABLES

VARIABLE	RANGE
1. Information	May include: 1.1. Property 1.2. Organizational 1.3. Technical reference
2. Search engine	May include: 2.1. Crawler-based search engine 2.1.1. Google 2.1.2. AlltheWeb 2.1.3. AltaVista 2.2. Human-powered directories 2.2.1. Yahoo directory 2.2.2. Open directory 2.2.3. Looksmart
3. Sources	May include: 3.1. Other IT systems 3.2. Manually created 3.3. Within own organization 3.4. Outside own organization 3.5. Geographically remote

EVIDENCE GUIDE

1. Critical aspects of Competency	**Assessment requires evidence that the candidate:** 1.1 Identified and gathered needed information 1.2 Searched for information on the internet or an intranet 1.3 Studied and interpreted information 1.4 Handled files 1.5 Maintained information
2. Resource Implications	**Specific resources for assessment** 2.1. Evidence of competent performance should be obtained by observing an individual in an information management role within the workplace or operational or simulated environment.
3. Methods of Assessment	**Competency in this unit may be assessed through:** 3.1. Written Test 3.2. Interview 3.3. Portfolio The unit will be assessed in a holistic manner as is practical and may be integrated with the assessment of other relevant units of competency. Assessment will occur over a range of situations, which will include disruptions to normal, smooth operation. Simulation may be required to allow for timely assessment of parts of this unit of competency. Simulation should be based on the actual workplace and will include walk through of the relevant competency components.
4. Context for Assessment	4.1. In all workplace, it may be appropriate to assess this unit concurrently with relevant teamwork or operation units.

UNIT OF COMPETENCY : FOLLOW OCCUPATIONAL SAFETY AND HEALTH POLICIES AND PROCEDURES

UNIT CODE : 400311107

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes to identify relevant occupational safety and health policies and procedures, perform relevant occupational safety and health procedures, and comply with relevant occupational safety and health policies and standards

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify relevant occupational safety and health policies and procedures	1.1 Related ***occupational safety and health risks and hazards*** are recognized based on ***OSH work standards*** 1.2 ***OSH requirements/ regulations*** towards work are determined in accordance to workplace policies and procedures 1.3 ***Incident/ Emergency procedures*** relevant to workplace are identified based on relevant OSH work standards	1.1. Occupational safety and health risks and hazards 1.2. OSH work standards 1.3. Government approved Occupational Safety and Health Policies and regulations 1.4. Terms related to occupational safety and health 1.5. Workplace process and procedures 1.6. Standard emergency plan and procedures	1.1 Observation skills 1.2 Critical thinking skills 1.3 Communication skills
2. Perform relevant occupational safety and health procedures	2.1 Safety devices are checked in accordance with workplace OSH work standards 2.2 ***OSH Work instructions*** are followed in accordance with workplace policies and procedures* 2.3 ***Personal protective equipment*****,** materials, tools, machinery, and equipment are utilized according to OSH work standards	2.1 OSH Work instructions Personal protective equipment 2.2 Safe handling procedures of tools, equipment and materials 2.3 Standard emergency plan and procedures 2.4 Different OSH control measures 2.5 Standard accident and illness reporting procedures	2.1 Communication skills 2.2 Knowledge management 2.3 Organizing skills 2.4 Observation skills
3. Comply with relevant occupational safety and health policies and standards	3.1 ***Preventive Control Measures*** are identified in accordance with OSH work standards 3.2 OSH requirements are obeyed in accordance with workplace policies and procedures 3.3 Incident/ Emergency procedures are executed based on OSH Procedures	3.1 OSH Preventive Control Measures 3.2 Principles of 5S 3.3 Environmental requirements relative to industrial wastes disposal 3.4 OSH requirements relative to safe handling and disposal of materials 3.5 Personal hygiene practices	3.1 Communication skills 3.2 Knowledge management 3.3 Organizing skills 3.4 Critical thinking skills 3.5 Observation skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Occupational Safety and Health Risks and Hazards	May include: 1.1 Physical hazards – impact, illumination, pressure, noise, vibration, extreme temperature, radiation 1.2 Biological hazards- bacteria, viruses, plants, parasites, mites, molds, fungi, insects 1.3 Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors 1.4 Ergonomics 1.5 Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, varying metabolic cycles 1.6 Physiological factors – monotony, personal relationship, work out cycle 1.7 Safety hazards (unsafe workplace condition) – confined space, excavations, falling objects, gas leaks, electrical, poor storage of materials and waste, spillage, waste and debris 1.8 Unsafe workers' act (Smoking in off-limited areas, Substance and alcohol abuse at work)
2. OSH Work Standards	May include: 2.1 OSHS Rule 1090 Hazardous Materials 2.2 OSHS Rule Gas & Electric Welding and Cutting Operations 2.3 OSHS Rule 1120 Hazardous Work Processes 2.4 OSHS Rule 1150 Materials Handling & Storage 2.5 OSHS Rule 1180 Internal Combustion Engine 2.6 OSHS Rule 1210 Electrical Safety 2.7 OSHS Rule 1420 Logging 2.8 OSHS Rule 1410 Construction Safety 2.9 OSHS Rule 1950 Pesticides & Fertilizers
3. OSH Requirements/ Regulations	May include: 3.1 Clean Air Act 3.2 Building code 3.3 National Electrical and Fire Safety Codes 3.4 Waste management statutes and rules 3.5 Permit to Operate 3.6 Philippine Occupational Safety and Health Standards 3.7 Department Order No. 13 (Construction Safety and Health) 3.8 ECC regulations 3.9 Republic Act No. 11058 – An Strengthening Compliance with Occupational Safety and Health
4. Incident and Emergency Procedures	May include: 4.1 Chemical spills 4.2 Equipment/vehicle accidents 4.3 Explosion

VARIABLE	RANGE
	4.4 Fire Drill 4.5 Gas leak 4.6 Injury to personnel 4.7 Structural collapse 4.8 Earthquake drill 4.9 Toxic and/or flammable vapors emission 4.10 Evacuation 4.11 Isolation 4.12 Basic life support/CPR 4.13 Decontamination 4.14 Calling designed emergency personnel
5. OSH Work Instructions	May include: 5.1 Worker's Participation Policies 5.2 Company Environment Safety and Health Policies 5.3 Continual OSH Improvement Instructions 5.4 Education and Training 5.5 Safety and Health Policy Statements 5.6 Mission and Vision Statements 5.7 Operating Instructions and Policies
6. Personal Protective Equipment	May include: 6.1 Arm/Hand guard, gloves 6.2 Eye protection (goggles, shield) 6.3 Hearing protection (ear muffs, ear plugs) 6.4 Hair Net/cap/bonnet 6.5 Hard hat 6.6 Face protection (mask, shield) 6.7 Apron/Gown/coverall/jump suit 6.8 Anti-static suits 6.9 High-visibility reflective vest
7. Preventive Control Measures	May include: 7.1 Eliminate the hazard (i.e., get rid of the dangerous machine 7.2 Isolate the hazard (i.e. keep the machine in a closed room and operate it remotely; barricade an unsafe area off) 7.3 Substitute the hazard with a safer alternative (i.e., replace the machine with a safer one) 7.4 Use administrative controls to reduce the risk (i.e. give trainings on how to use equipment safely; OSH-related topics, issue warning signages, rotation/shifting work schedule) 7.5 Use engineering controls to reduce the risk (i.e. use safety guards to machine) 7.6 Use personal protective equipment 7.7 Safety, Health and Work Environment Evaluation 7.8 Periodic and/or special medical examinations of workers

EVIDENCE GUIDE

1. Critical aspects of Competency	**Assessment requires evidence that the candidate:** 1.1. Recognize related occupational safety and health risks and hazards based on OSH work standards 1.2. Identify incident/emergency procedures relevant to workplace based on relevant OSH work standards 1.3. Follow the OSH work instructions in accordance with workplace policies and procedures 1.4. Utilize personal protective equipment, materials, tools, machinery, and equipment according to OSH work standards 1.5. Obey OSH requirements in accordance with workplace policies and procedures 1.6. Executed incident/ emergency procedures based on OSH Procedures
2. Resource Implications	**The following resources should be provided:** 2.1 Facilities, materials tools and equipment necessary for the activity
3. Methods of Assessment	**Competency in this unit may be assessed through:** 3.1 Observation/Demonstration with oral questioning 3.2 Third party report
4. Context for Assessment	4.1 Competency may be assessed in the work place or in a simulated work place setting

UNIT OF COMPETENCY : APPLY ENVIRONMENTAL WORK STANDARDS
UNIT CODE : 400311108

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitude to identify environmental work hazards, follow environment work procedures and comply with environmental requirements.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify environmental work hazards	1.1. Related ***environmental hazards*** are recognized based on ***environmental work standards*** 1.2. Environmental work standards are interpreted in accordance to relevant policies 1.3. ***Required resources*** to minimize effect of environmental hazards are prepared based on relevant environmental work standards	1.1. Environmental Hazards 1.2. Environmental Work Standards 1.3. Required Resources 1.4. OSH Standards 1.5. Fight against poverty rights 1.6. Environmental Protection 1.7. Respect of Human Rights	1.1. Critical thinking 1.2. Problem solving 1.3. Observation Skills
2. Follow environmental work procedures	2.1. ***Environmental protection*** pre-cautionary activities are practiced based on environmental work procedures *2.2.* Work activities are executed in accordance with ***Environmental work Procedures*** 2.3. Environmental Protection Post-Activities are accomplished based on environmental work procedures*	2.1. Environmental Protection 2.2. Environmental Work Procedures 2.3. Renewable Energies	2.1. Critical thinking 2.2. Problem solving 2.3. Observation Skills
3. Comply with environmental work requirements	3.1. Required resources are utilized in accordance with workplace environmental policies 3.2. ***Environmental hazardous and non-hazardous*** *materials* are stored in accordance with ***environmental regulations*** 3.3. Hazardous and Non-hazardous Wastes disposed according to environmental regulations	3.1. Environmental Work Procedures 3.2. Environmental Laws 3.3. Environmental Hazardous and Non-Hazardous Materials	3.1. Critical thinking 3.2. Problem solving 3.3. Observation Skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Environmental Hazards	May include: 1.1 Tobacco Smoke 1.2 Asbestos 1.3 Lead 1.4 Combustion Gases 1.5 Chemicals 1.6 Pesticides 1.7 Pollutants 1.8 Contaminated Drinking Water 1.9 Noise 1.10 Dust
2. Environmental Work Standards	May include: 2.1 Air Quality Standards 2.2 Emission Standards 2.3 ISO 14001: Environmental Management System 2.4 Environmental Statements 2.5 Environmental Quality Standards 2.6 Work Environment Measurement Standard
3. Required Resources	May include: 3.1 Electric 3.2 Water 3.3 Fuel 3.4 Telecommunications 3.5 Supplies and Materials 3.6 Trash Cans 3.7 Relevant Data Sheets 3.8 Barriers or Barricades
4. Environmental Protection	May include protection against 4.1 Overconsumption of Resources 4.2 Destruction of Ecosystems 4.3 Habitat Destructions 4.4 Extinction of Wildlife 4.5 Pollutions 4.6 Water Degradation
5. Environmental Work Procedures	May include: 5.1 Environmental pollution control measures 5.2 Oil and Fuel use 5.3 Disposal and Reuse 5.4 Herbicide applications 5.5 Breed Bird Mitigation 5.6 Tree Removal Works 5.7 Erosion Protection 5.8 Scrub Clearance 5.9 Bankside sediment clearance

VARIABLE	RANGE
6. Environmental Hazardous and Non-Hazardous Materials	May include but not limited: 6.1 Acids 6.2 Adhesives 6.3 Aerosols 6.4 Asbestos 6.5 Batteries 6.6 Chemicals 6.7 Compact fluorescent lamps 6.8 Drugs 6.9 Dyes 6.10 E-Waste 6.11 Gasoline 6.12 Grease 6.13 Lead 6.14 Motor Oil 6.15 Solvents 6.16 Weed Killers
7. Environmental Regulations	May include: 7.1 Clean Air Act 7.2 Clean Water Act 7.3 Endangered Species Act 7.4 Resource Conservation and Recovery Act 7.5 Cave Resources and Management Act 7.6 Fisheries Code 7.7 Forestry Code 7.8 Mining Act

EVIDENCE GUIDE

1. Critical aspects of Competency	**Assessment requires evidence that the candidate:** 1.1. Interpreted the Environmental Work Standards in accordance to relevant policies 1.2. Prepared required resources to minimize effects of environmental hazards based on relevant environmental work standards 1.3. Practiced environmental protection pre-cautionary activities based on environmental work procedures 1.4. Executed work activities in accordance with environmental work procedures 1.5. Accomplished environmental protection post-activities based on environmental work procedures 1.6. Stored environmental hazardous and non-hazardous materials in accordance with environmental regulations 1.7. Disposed hazardous and non-hazardous wastes according to environmental regulations
2. Resource Implications	**The following resources should be provided:** 2.1. Workplace with storage facilities 2.2. Tools, materials and equipment relevant to the tasks (ex. Cleaning tools, cleaning materials, trash bags, etc.) 2.3. PPE 2.4. Manuals and references
3. Methods of Assessment	**Competency in this unit may be assessed through:** 3.1. Demonstration 3.2. Oral questioning 3.3. Written examination
4. Context for Assessment	4.1. Competency assessment may occur in workplace or any appropriately simulated environment 4.2. Assessment shall be observed while task are being undertaken whether individually or in-group

UNIT OF COMPETENCY : ADOPT ENTREPRENEURIAL MINDSET IN THE WORKPLACE

UNIT CODE : 400311109

UNIT DESCRIPTOR : This unit covers the outcomes required to support and internalize an entrepreneurial mindset and observe basic entrepreneurial practices in the workplace.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Determine entrepreneurial mindset	1.1. ***Entrepreneurial mindset*** in the workplace is determined from enterprise practices and policies. 1.2. ***Entrepreneurial mindset*** in the workplace is studied and ***affirmed*** based on current enterprise practices 1.3. Clarification from reliable ***sources*** is sought regarding entrepreneurial ***mindset*** and corporate culture.	1.1. Workplace policies and practices relating to entrepreneurship 1.2. Elements of corporate culture 1.3. Entrepreneurial mindset 1.4. Entrepreneurial practices in the workplace 1.5. Desirable attitudes: ● Patience ● Willingness to learn ● Attention to details	1.1. Identifying entrepreneurial mindset 1.2. Studying and affirming entrepreneurial mindset 1.3. Selecting and emulating desirable entrepreneurial practices 1.4. Communication skills
2. Identify entrepreneurial practices	2.1. Entrepreneurial practices are determined based on enterprise requirements 2.2. Entrepreneurial practices are performed following workplace and client requirements. 2.3. Cost-effective measures are complied with reference to workplace best practices	2.1. Quality assurance practices 2.2. Workplace and client requirements 2.3. Types of cost-effective measures 2.4. Workplace quality policy 2.5. Attitude: ● Patience ● Attention to details	2.1. Performing quality assurance practices 2.2. Complying quality assurance requirements 2.3. Complying to cost-effective measures 2.4. Communication skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Entrepreneurial mindset	May include workplace thinking relating to: 1.1. Economy in the use of resources 1.2. Waste management 1.3. Quality-consciousness 1.4. Cost-consciousness 1.5. Safety- and health- consciousness
2. Quality assurance practices	May include: 2.1. Use of quality procedures manual 2.2. Quality policy 2.3. Best/Good practices 2.4. Continuous improvement program
3. Reliable sources	May include: 3.1. Supervisors 3.2. Colleagues 3.3. Clients/Partners

EVIDENCE GUIDE

1. Critical aspects of competency	**Assessment requires evidence that the candidate:** 1.1 Demonstrated affirmation of entrepreneurial mindset 1.2 Observed entrepreneurial practices 1.3 Complied with cost effective measures
2. Resource Implications	**The following resources should be provided:** 2.1 Simulated or actual workplace 2.2 Tools, materials and supplies needed to demonstrate the required tasks 2.3 References and manuals
3. Methods of Assessment	**Competency in this unit may be assessed through :** 3.1 Written examination 3.2 Demonstration/observation with oral questioning 3.3 Third-party report
4. Context of Assessment	4.1 Competency may be assessed in workplace or in a simulated workplace setting 4.2 Assessment shall be observed while tasks are being undertaken whether individually or in-group

COMMON COMPETENCIES

UNIT TITLE : APPLY QUALITY STANDARDS

UNIT CODE : ICT315202

UNIT DESCRIPTOR : This unit covers the knowledge, skills, attitudes and values needed to apply quality standards in the workplace. The unit also includes the application of relevant safety procedures and regulations, organization procedures and customer requirements.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Assess quality of received materials	1.1. Work instruction is obtained and work is carried out in accordance with standard operating procedures. 1.2. Received ***materials*** are checked against workplace standards and specifications. 1.3. Faulty materials related to work are identified and isolated. 1.4. ***Faults*** and any identified causes are recorded and/or reported to the supervisor concerned in accordance with workplace procedures. 1.5. Faulty materials are replaced in accordance with workplace procedures.	1.1. Relevant production processes, materials and products 1.2. Characteristics of materials, software and hardware used in production processes 1.3. Quality checking procedures 1.4. Quality Workplace procedures 1.5. Identification of faulty materials related to work	1.1. Reading skills required to interpret work instruction 1.2. Critical thinking 1.3. Interpreting work instructions
2. Assess own work	2.1 ***Documentation*** relative to quality within the company is identified and used. 2.2 Completed work is checked against workplace standards relevant to the task undertaken. 2.3 ***Errors*** are identified and isolated. 2.4 Information on the quality and other indicators of production performance are recorded in accordance with workplace procedures. 2.5 In cases of deviations from specific ***quality standards***, causes are documented and reported in accordance with the workplace' s standards operating procedures.	2.1. Safety and environmental aspects of production processes 2.2. Fault identification and reporting 2.3. Workplace procedure in documenting completed work 2.4. Workplace Quality Indicators	2.1. Carry out work in accordance with OHS policies and procedures

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Engage in quality improvement	3.1 Process improvement procedures are participated in relative to workplace assignment. 3.2 Work is carried out in accordance with process improvement procedures. 3.3 Performance of operation or quality of product of service to ensure ***customer*** satisfaction is monitored.	3.1. Quality improvement processes 3.2. Company customers defined	3.1. Solution providing and decision-making 3.2. Practice company process improvement procedure

RANGE OF VARIABLES

VARIABLE	RANGE
1 Materials	1.1 Materials may include but not limited to: 1.1.1. Manuals 1.1.2. Job orders 1.1.3. Instructional videos
2 Faults	2.1 Faults may include but not limited to: 2.1.1. Materials not to specification 2.1.2. Materials contain incorrect/outdated information 2.1.3. Hardware defects 2.1.4. Materials that do not conform with any regulatory agencies
3 Documentation	3.1 Organization work procedures 3.2 Manufacturer's instruction manual 3.3 Customer requirements 3.4 Forms
4 Errors	4.1 Errors may be related but not limited to the following: 4.1.1. Deviation from the requirements of the Client 4.1.2. Deviation from the requirement of the organization
5 Quality standards	5.1 Quality standards may be related but not limited to the following: 5.1.1. Materials 5.1.2. Hardware 5.1.3. Final product 5.1.4. Production processes 5.1.5. Customer service
6 Customer	6.1 Co-worker 6.2 Supplier/Vendor 6.3 Client 6.4 Organization receiving the product or service

EVIDENCE GUIDE

1 Critical aspect of competency	Assessment requires evidence that candidate: 1.1 Carried out work in accordance with the company's standard operating procedures 1.2 Performed task according to specifications 1.3 Reported defects detected in accordance with standard operating procedures 1.4 Carried out work in accordance with the process improvement procedures
2 Method of assessment	The assessor may select two (2) of the following assessment methods to objectively assess the candidate: 2.1 Observation 2.2 Questioning 2.3 Practical demonstration
3 Resource implication	3.1 Materials, software and hardware to be used in a real or simulated situation
4 Context of Assessment	4.1 Assessment may be conducted in the workplace or in a simulated environment

UNIT TITLE : PERFORM COMPUTER OPERATIONS
UNIT CODE : ICT311203
UNIT DESCRIPTOR : This unit covers the knowledge, skills, (and) attitudes and values needed to perform computer operations which include inputting, accessing, producing and transferring data using the appropriate hardware and software

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Plan and prepare for task to be undertaken	1.1. Requirements of task are determined 1.2. Appropriate ***hardware*** and ***software*** are selected according to task assigned and required outcome 1.3. Task is planned to ensure ***OH&S guidelines*** and procedures are followed	1.1. Main types of computers and basic features of different operating systems 1.2. Main parts of a computer 1.3. Information on hardware and software 1.4. Data security guidelines	1.1. Reading and comprehension skills required to interpret work instruction and to interpret basic user manuals. 1.2. Communication skills to identify lines of communication, request advice, follow instructions and receive feedback. 1.3. Interpreting user manuals and security guidelines
2. Input data into computer	2.1. Data are entered into the computer using appropriate program/application in accordance with company procedures 2.2. Accuracy of information is checked and information is saved in accordance with standard operating procedures 2.3. Inputted data are stored in ***storage media*** according to requirements 2.4. Work is performed within ***ergonomic guidelines***	2.1. Basic ergonomics of keyboard and computer user 2.2. Storage devices and basic categories of memory 2.3. Relevant types of software	2.1. Technology skills to use equipment safely including keyboard skills. 2.2. Entering data
3. Access information using computer	3.1. Correct program/application is selected based on job requirements 3.2. Program/application containing the information required is accessed according to company procedures 3.3. ***Desktop icons*** are correctly selected, opened and closed for navigation purposes	3.1. General security, privacy legislation and copyright 3.2. Productivity Application 3.3. Business Application	3.1. Accessing information 3.2. Searching and browsing files and data

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	3.4. Keyboard techniques are carried out in line with OH&S requirements for safe use of keyboards		
4. Produce/ output data using computer system	4.1. Entered data are processed using appropriate software commands 4.2. Data printed out as required using computer hardware/peripheral devices in accordance with standard operating procedures 4.3. Files, data are transferred between compatible systems using computer software, hardware/ peripheral devices in accordance with standard operating procedures	4.1. Computer application in printing, scanning and sending facsimile 4.2. Types and function of computer peripheral devices	4.1. Computer data processing 4.2. Printing of data 4.3. Transferring files and data
5. Maintain computer equipment and systems	5.1. Systems for cleaning, minor ***maintenance*** and replacement of consumables are implemented 5.2. Procedures for ensuring security of data, including regular back-ups and virus checks are implemented in accordance with standard operating procedures 5.3. Basic file maintenance procedures are implemented in line with the standard operating procedures	5.1 Computer equipment/system basic maintenance procedures 5.2 Viruses 5.3 OH&S principles and responsibilities 5.4 Calculating computer capacity 5.5 System Software 5.6 Basic file maintenance procedures	5.1 Removing computer viruses from infected machines 5.2 Making backup files

RANGE OF VARIABLES

VARIABLE	RANGE
1. Hardware and peripheral devices	1.1. Personal computers 1.2. Networked systems 1.3. Communication equipment 1.4. Printers 1.5. Scanners 1.6. Keyboard 1.7. Mouse
2. Software	Software includes the following but not limited to: 2.1. Word processing packages 2.2. Data base packages 2.3. Internet 2.4. Spreadsheets
3. OH & S guidelines	3.1. OHS guidelines 3.2. Enterprise procedures
4. Storage media	Storage media include the following but not limited to: 4.1. diskettes 4.2. CDs 4.3. zip disks 4.4. hard disk drives, local and remote
5. Ergonomic guidelines	5.1. Types of equipment used 5.2. Appropriate furniture 5.3. Seating posture 5.4. Lifting posture 5.5. Visual display unit screen brightness
6. Desktop icons	Icons include the following but not limited to: 6.1. directories/folders 6.2. files 6.3. network devices 6.4. recycle bin
7. Maintenance	7.1. Creating more space in the hard disk 7.2. Reviewing programs 7.3. Deleting unwanted files 7.4. Backing up files 7.5. Checking hard drive for errors 7.6. Using up to date security solution programs 7.7. Cleaning dust from internal and external surfaces

EVIDENCE GUIDE

1. Critical aspect of competency	Assessment requires evidence that the candidate: 1.1. Selected and used hardware components correctly and according to the task requirement 1.2. Identified and explain the functions of both hardware and software used, their general features and capabilities 1.3. Produced accurate and complete data in accordance with the requirements 1.4. Used appropriate devices and procedures to transfer files/data accurately 1.5. Maintained computer system
2. Method of assessment	2.1. The assessor may select two of the following assessment methods to objectively assess the candidate: 2.1.1. Observation 2.1.2. Questioning 2.1.3. Practical demonstration
3. Resource implication	3.1. Computer hardware with peripherals 3.2. Appropriate software
4. Context of Assessment	4.1. Assessment may be conducted in the workplace or in a simulated work environment

CORE COMPETENCIES

UNIT OF COMPETENCY : MONITOR AND REPORT CYBER THREATS
UNIT CODE : CS-ICT251101
UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitude required to monitor and report cyber threats. This includes competencies in checking for alerts, checking status of third-party security solutions, performing manual checking and verification, conducting case follow-up and performing alert reporting.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Check for alerts	1.1. ***Detection alert*** is received as per company Standard Operating Procedure (SOP). 1.2. ***Incident report*** is received as per company Standard Operating Procedure (SOP). 1.3. ***Red flag detection*** is checked according company SOP 1.4. Alert is assessed based on ***pre-identified criteria*** 1.5. Ticket is issued upon confirmation of detection.	1.1. Basic knowledge with Windows, MAC & Linux OS 1.2. Basic knowledge with Web server and website design and architecture 1.3. Basic knowledge with scripting and coding language, i.e. PHP, Python, Java, Visual Basic and others 1.4. Basic knowledge with network infrastructure and architecture, i.e. LAN, WAN, port forwarding 1.5. Sources of detection alert / incident reports 1.6. Log and detection management 1.7. Security solution scan and operations procedure 1.8. Security solution management application 1.9. Security solution severity classifications 1.10. Malicious software behaviors 1.11. Knowledge of attack framework	1.1. Computer operation skills 1.2. Communication skills 1.3. Interpreting work instructions 1.4. Interpersonal skills 1.5. Analytical skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
2. Check status of third-party security solution	2.1. Enterprise security solution software is checked if there is one installed as per company SOP. 2.2. ***Security solution*** software is checked if operational as per company SOP. 2.3. Security solution software is checked if it can clean or delete the issue	2.1. Log and detection management 2.2. Security solution usage and operations 2.3. Knowledge in organization SOP	2.1. Computer operation skills 2.2. Communication skills 2.3. Interpreting work instructions 2.4. Interpersonal skills 2.5. Analytical skills
3. Perform manual checking and verification	3.1. Detection from the security solution software is checked as per procedure 3.2. ***Action*** of the security solution software is checked as per company SOP. 3.3. Security solution software updates are checked and patched as required 3.4. Security solution software is used to scan infected system/s	3.1. Log and detection management 3.2. Security solution scan and operations procedure 3.3. Knowledge in organization SOP	3.1. Computer operation skills 3.2. Communication skills 3.3. Interpreting work instructions 3.4. Interpersonal skills 3.5. Analytical skills 3.6. Verification Skills
4. Conduct case follow-up	4.1. Results of the scan are verified to customer/ client/ stakeholder 4.2. Security solution scan logs are checked for failed action as per company SOP 4.3. Failed action is escalated to ***appropriate authority*** as per company SOP	4.1. Log and detection management 4.2. Knowledge in organization SOP	4.1. Computer operation skills 4.2. Communication skills 4.3. Interpreting work instructions 4.4. Interpersonal skills 4.5. Analytical skills
5. Perform alert reporting	5.1. Stakeholder/client with high and critical threats are notified 5.2. Activity of the threats are reported based on the spread and lateral movement 5.3. Activity of the threats are reported based on egress and ingress 5.4. Threats are identified based on exploitation activity and installation behavior	5.1 Malicious software behaviors 5.2 Threats 5.3 Knowledge in attack framework	5.1 Computer operation skills 5.2 Communication skills 5.3 Interpreting work instructions 5.4 Interpersonal skills 5.5 Analytical skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Detection alert	May include: 1.1. SIEM alert 1.2. AV alert 1.3. Firewall alert 1.4. Web application firewall alert 1.5. DLP alert 1.6. EDR alert 1.7. NDR alert
2. Detection report	May include: 2.1. phone call 2.2. walk-in 2.3. email 2.4. SMS 2.5. Chat 2.6. Video-conferences
3. Red flag detection	May include: 3.1. ransomware 3.2. PE Infection /Virus
4. Pre-identified criteria	May include criteria based on: 4.1. Threat 4.2. Detection 4.3. Routine
5. Security solution	May include: 5.1. anti-virus 5.2. common firewall 5.3. threat intelligence 5.4. TDR - Threat Detection and Response 5.5. WAF - Web Application Firewall 5.6. IDS - Intrusion Detection System 5.7. IPS - Intrusion Prevention System 5.8. DLP - Data Loss Prevention 5.9. Operational technology (OT)/ Industrial Control System (ICS) / Supervisory Control and Data Acquisition (SCADA) security 5.10. Internet of Things (IoT) 5.11. EDR/MDR - Endpoint Detection & Response and Managed Detection and Response 5.12. SIEM - Security Information & Event Management 5.13. SOAR - Security Orchestration, Automation and Response 5.14. XDR - Extended Detection and Response
6. Action	May include: 6.1. Failed 6.2. Clean 6.3. Delete 6.4. Quarantine 6.5. Blocked

VARIABLE	RANGE
	6.6. Re-image
7. Appropriate authority	May include: 7.1. IT department manager 7.2. Information security manager 7.3. Security solution/security vendor 7.4. Chief information security officer

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Checked for alerts 1.1.1 Received detection alert as per company Standard Operating Procedure (SOP). 1.1.2 Received incident report as per company Standard Operating Procedure (SOP). 1.1.3 Checked red flag detection according company SOP 1.1.4 Assessed alert is based on pre-identified criteria 1.1.5 Issued ticket upon confirmation of detection 1.2 Checked status of third-party security solution 1.2.1 Checked enterprise security solution software if there is one installed as per company SOP 1.2.2 Checked security solution software if operational as per company SOP 1.2.3 Checked security solution software if it can clean or delete the issue 1.3 Performed manual checking and verification 1.3.1 Checked detection from the security solution software as per procedure 1.3.2 Checked action of the security solution software as per company SOP 1.3.3 Checked and patched security solution software updates as required 1.3.4 Used security solution software to scan infected system/s 1.4 Conducted case follow-up 1.4.1 Verified results of the scan to customer/client/ stakeholder 1.4.2 Checked security solution scan logs for failed action as per company SOP 1.4.3 Escalated failed action to appropriate authority as per company SOP 1.5 Performed alert reporting 1.5.1 Notified stakeholder/client with high and critical threats 1.5.2 Reported activity of the threats based on the spread and lateral movement 1.5.3 Reported activity of the threats based on egress and ingress 1.5.4 Identified threats based on exploitation activity and installation behavior

2. Resource Implications	The following resources should be provided: 2.1 Appropriate supplies and materials 2.2 Applicable equipment 2.3 Appropriate software 2.4 Workplace or assessment area
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1 Demonstration with oral questioning 3.2 Written Exam 3.3 Portfolio with interview
4. Context for Assessment	4.1 Competency maybe assessed in actual workplace or at the designated TESDA Accredited Assessment Center.

UNIT OF COMPETENCY : CONDUCT VULNERABILITY SCANNING
UNIT CODE : CS-ICT251102
UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitude required to conduct vulnerability scanning. It includes checking schedule for scanning, conducting scanning of assets and providing report of scanning.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Check schedule for scanning	1.1. Vulnerability management is consulted with the ***immediate supervisor*** 1.2. Access to vulnerability scanning calendar and timeline is requested based on scope of work 1.3. Number of assets to be scanned are identified based on the particular schedule 1.4. Signed off on scope of work is performed and accomplished according to prescribed timeline	1.1. Ticket management systems 1.2. Vulnerability management solution 1.3. Scanning procedures based on vulnerability management solution 1.4. Knowledge Management usage	1.1. Computer operation skills 1.2. Communication skills 1.3. Interpreting work instructions 1.4. Interpersonal skills 1.5. Vulnerability Scanning skills
2. Conduct scanning of assets	2.1. List of ***assets*** for vulnerability scanning are verified with supervisor and change manager based on scope of work 2.2. Assets to be prioritized are verified with the immediate supervisor and change manager 2.3. Prescribed schedule for vulnerability scanning is adhered to 2.4. Scanning of assets are performed based on industry standards (*NIST 800-115, Chapter 4.3 & 4.4*) 2.5. CPU usage, storage usage and network latency are monitored based on software capability 2.6. Vulnerability scanning is terminated and immediately reported to IT when issue arises with regards to slowness of network and endpoint	2.1. Ticket management systems 2.2. Vulnerability management solution 2.3. Scanning procedures based on vulnerability management solution 2.4. Knowledge Management usage 2.5. Vulnerability management solution usage and operations 2.6. List of assets 2.7. Familiarity on NIST 800-115	2.1. Computer operation skills 2.2. Communication skills 2.3. Interpreting work instructions 2.4. Interpersonal skills 2.5. Vulnerability Scanning skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Provide report of scanning	3.1. Failed scan on assets are recorded based on established company procedures 3.2. Success scan on assets are recorded based on established company procedures 3.3. Vulnerability assessment report is submitted to immediate supervisor and change manager	3.1. Log and scan management 3.2. Vulnerability management solution scan and operations procedure 3.3. Documentation procedures on scan output	3.1. Computer operation skills 3.2. Communication skills 3.3. Interpreting work instructions 3.4. Interpersonal skills 3.5. Documentation skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Immediate supervisor	May include 1.1. IT Department Manager 1.2. Information security Manager 1.3. Security solution/security vendor 1.4. Chief Information Security Officer
2. Assets	May include 2.1. Servers 2.2. Endpoints 2.3. Mobile devices 2.4. Web-applications

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Checked schedule for scanning 1.1.1 Consulted vulnerability management with the immediate supervisor 1.1.2 Requested access to vulnerability scanning calendar and timeline based on scope of work 1.1.3 Identified number of assets to be scanned based on the particular schedule 1.1.4 Performed and accomplished signed off on scope of work according to prescribed timeline 1.2 Conducted scanning of assets 1.2.1 Verified list of assets for vulnerability scanning with supervisor and change manager based on scope of work 1.2.2 Verified assets to be prioritized with the immediate supervisor and change manager 1.2.3 Adhered to prescribed schedule for vulnerability scanning 1.2.4 Performed scanning of assets based on industry standards 1.2.5 Monitored CPU usage, storage usage and network latency based on software capability 1.2.6 Terminated vulnerability scanning and immediately reported to IT when issue arises with regards to slowness of network and endpoint 1.3 Provided report of scanning 1.3.1 Recorded failed scan on assets based on established company procedures 1.3.2 Recorded success scan on assets based on established company procedures 1.3.3 Submitted vulnerability assessment report to immediate supervisor and change manager
2. Resource Implications	The following resources should be provided: 2.1 Appropriate supplies and materials 2.2 Applicable equipment 2.3 Appropriate software 2.4 Workplace or assessment area
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1 Demonstration with oral questioning 3.2 Written Exam 3.3 Portfolio with interview
4. Context of Assessment	4.1 Competency maybe assessed in actual workplace or at the designated TESDA Accredited Assessment Center.

GLOSSARY OF TERMS

GENERAL

1) **Certification -** is the process of verifying and validating the competencies of a person through assessment

2) **Certificate of Competency (COC)** – is a certification issued to individuals who pass the assessment for a single unit or cluster of units of competency

3) **Common Competencies** - are the skills and knowledge needed by all people working in a particular industry

4) **Competency** - is the possession and application of knowledge, skills and attitudes to perform work activities to the standard expected in the workplace

5) **Competency Assessment -** is the process of collecting evidence and making judgements on whether competency has been achieved

6) **Competency Standard (CS)** - is the industry-determined specification of competencies required for effective work performance

7) **Context of Assessment** - refers to the place where assessment is to be conducted or carried out

8) **Core Competencies - are** the specific skills and knowledge needed in a particular area of work - industry sector/occupation/job role

9) **Critical aspects of competency -** refers to the evidence that is essential for successful performance of the unit of competency

10) **Elective Competencies -** are the additional skills and knowledge required by the individual or enterprise for work

11) **Elements** - are the building blocks of a unit of competency. They describe in outcome terms the functions that a person performs in the workplace

12) **Evidence Guide** - is a component of the unit of competency that defines or identifies the evidences required to determine the competence of the individual. It provides information on critical aspects of competency, underpinning knowledge, underpinning skills, resource implications, assessment method and context of assessment

13) **Level -** refers to the category of skills and knowledge required to do a job

14) **Method of Assessment** - refers to the ways of collecting evidence and when evidence should be collected

15) **National Certificate (NC)** – is a certification issued to individuals who achieve all the required units of competency for a national qualification defined under the Competency Standards. NCs are aligned to specific levels within the PTQF

16) **Performance Criteria** - are evaluative statements that specify what is to be assessed and the required level of performance

17) **Qualification** - is a cluster of units of competencies that meets job roles and is significant in the workplace. It is also a certification awarded to a person on successful completion of a course in recognition of having demonstrated competencies in an industry sector

18) **Range of Variables** - describes the circumstances or context in which the work is to be performed

19) **Recognition of Prior Learning (RPL)** – is the acknowledgement of an individual's skills, knowledge and attitudes gained from life and work experiences outside registered training programs

20) **Resource Implications -** refers to the resources needed for the successful performance of the work activity described in the unit of competency. It includes work environment and conditions, materials, tools and equipment

21) **Basic Competencies -** are the skills and knowledge that everyone needs for work

22) **Underpinning Knowledge -** refers to the competency that involves in applying knowledge to perform work activities. It includes specific knowledge that is essential to the performance of the competency

23) **Underpinning Skills** - refers to the list of the skills needed to achieve the elements and performance criteria in the unit of competency. It includes generic and industry specific skills

24) **Unit of Competency** – is a component of the competency standards stating a specific key function or role in a particular job or occupation; it is the smallest component of achievement that can be assessed and certified under the PTQF

SECTOR SPECIFIC

1. **Attack** - Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has value to the organization
2. **Asset** - Any item that has value to the organization
3. **Attribute** - Property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means
4. **Authentication** - Provision of assurance that a claimed characteristic of an entity is correct
5. **Authenticity** - Property that an entity is what it claims to be

6. **Availability** - Property of being accessible and usable upon demand by an authorized entity
7. **Business Continuity** - Procedures and/or processes for ensuring continued business operations
8. **CERT** - Computer Emergency Response Team (CERT) or Computer Security and Incident Response Team (CSIRT) refers to “an organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security”. At present, “both terms (CERT and CSIRT) are used in a synonymous manner” (ENISA, 2015 and ENISA, 2015a).
9. **Computer security** also known as **cyber security or IT security** - Is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.
10. **Confidentiality** - Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
11. **Consequence** - Outcome of an event affecting objectives.
12. **Control** - Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.
13. **Control Objective** - Statement describing what is to be achieved as a result of implementing controls.
14. **Corrective Action** - Action to eliminate the cause of a detected non-conformity or other undesirable situation
15. **Cyber threat monitoring** - is a solution that uses strategic intelligence to continuously analyze, evaluate, and monitor an organization's networks and endpoints for evidence of security threats, such as network intrusion, ransomware, and other malware attacks
16. **Data** - objective measurements of the attributes (characteristics) of entities such as people, places, things, and events.
17. **Data** - Collection of values assigned to base measures, derived measures and/or indicators. This definition applies only within the context of ISO/IEC 27004:2009
18. **DICT** - Department of Information and Communications Technology
19. **DDoS** - Distributed Denial of Service
20. **Documentation** – a collection of documents or information.
21. **Edit** – to modify the form or format of data
22. **Effect** - Is a deviation from the expected — positive and/or negative.
23. **Effectiveness** - Extent to which planned activities are realized and planned results achieved.
24. **Efficiency** - Relationship between the results achieved and the resources used.

25. **Electronic Discovery (e-Discovery)** - is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored information ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries.
26. **End-user –** anyone who uses an information system or the information it produces.
27. **Ergonomics** - the science and technology emphasizing the safety, comfort, and ease of use of human-operated machines. The goal of ergonomics is to produce systems that are user-friendly: safe, comfortable and easy to use.
28. **Event** - Occurrence or change of a particular set of circumstances
29. **File folders**, also called directories, - a way to organize computer files.
30. **Guideline** - Description that clarifies what should be done and how, to achieve the objectives set out in policies.
31. **ICT systems** - Hardware, software, firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment.
32. **Incident** – any flagged alert of threat/s detected by the security solution product.
33. **IDS** - Intrusion Detection System
34. **IEC** - International Electrotechnical Commission
35. **Information** – data placed in a meaningful and useful context for an end user.
36. **Information and Communication Technology (ICT) -** refers to technologies associated with the transmission and exchange of data in the form of sound, text, visual images, signals or any combination of those forms through the use of digital technology. It encompasses such services as telecommunications, posts, multimedia, electronic commerce, broadcasting, and information technology.
37. **Information security** - Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
38. **Information security event** - It refers to an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
39. **Information security incident** - It is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threating information security
40. **Information system** - Application, service, information technology asset, or any other information handling component
41. **Infrastructure** - Facilities and equipment to enable the ICT DR services, including but not limited to power supply, telecommunications connections and environmental controls
42. **Integrity** - Property of protecting the accuracy and completeness of assets
43. **ISMS** - Information Security Management System

44. **ISO** - International Standards Organization
45. **Local Area Network (LAN) –** a communications network that typically connects computers, terminals, and other computerized devices within a limited physical area such as an office, building, manufacturing plant and other work sites.
46. **Management** - Coordinated activities to direct and control an organization
47. **Management system** - Framework of guidelines, policies, procedures, processes and associated resources aimed at ensuring an organization meets its objectives Measure Variable to which a value is assigned as the result of measurement
48. **Measurement** - Process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measurement function, an analytical model, and decision criteria
49. **NCERT** - National Computer Emergency Response Team
50. **Object** - Item characterized through the measurement of its attributes
51. **Organizations** - Entities which utilize ICT DR services
52. **Owner** - Identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. This term does not mean that the person actually has any property rights to the asset.
53. **POC** - Point of Contact
54. **Policy** - Overall intention and direction as formally expressed by management
55. **Problem solving skills** – able to discern the questions raised by stakeholder on security solution operation and handling; included but not limited to problems and the threats identified by the security solution.
56. **Procedure** - Specified way to carry out an activity or a process
57. **Process** - Set of interrelated or interacting activities which transforms inputs into outputs
58. **Quality Assurance –** methods for ensuring that information systems are free from errors and fraud and provide information products of high quality.
59. **Record** - Document stating results achieved or providing evidence of activities performed
60. **Reliability** - Property of consistent intended behavior and results
61. **Review** - Activity undertaken to determine the suitability, adequacy and effectiveness (2.22) of the subject matter to achieve established objectives
62. **Review object** - Specific item being reviewed
63. **Risk** - Combination of the probability of an event and its consequence
64. **Risk acceptance** - Decision to accept a risk
65. **Risk analysis** - Process to comprehend the nature of risk and to determine the level of risk
66. **Risk assessment** - Overall process of risk identification, risk analysis and risk evaluation

67. **Risk management** - Coordinated activities to direct and control an organization with regard to risk.
68. **SIEM** - Security Information and Event Management
69. **Simulation** - the process of imitating a real phenomenon with a set of mathematical formulas. Advanced computer programs can simulate weather conditions, chemical reactions, atomic reactions, even biological processes.
70. **Software –** computer programs and procedures concerned with the operation of an information system.
71. **Standards –** measures of performance developed to evaluate the progress of a system toward its objectives
72. **Stakeholder** - Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
73. **System –** an assembly of methods, procedures, or techniques unified by regulated interaction to form an organized whole
74. **Third party** - Person or body that is recognized as being independent of the parties involved, as concerns the issue in question
75. **Threat** - Potential cause of an unwanted incident, which may result in harm to a system or organization
76. **Threat monitoring** - refers to a type of solution or process dedicated to continuously monitoring across networks and/or endpoints for signs of security threats such as attempts at intrusions or data exfiltration.
77. **Ticket management system** – ant document (physical or digital) that possessed the following – reporter, time, date, details of incident and status of the case.
78. **User- friendly** – a characteristic of human-operated equipment and systems that makes them safe, comfortable, and easy to use.
79. **Validation** - Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
80. **Verification** - Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
81. **Vulnerability** - Weakness of an asset or control that can be exploited by one or more threats

ACKNOWLEDGEMENTS

The Technical Education and Skills Development Authority (TESDA) would like to recognize the commitment of industry stakeholders who provided their time and expertise for the development of this Competency Standards (CS).

THE TECHNICAL EXPERTS PANEL (TEP)

MR. JOSEPH FELIX V. PACAMARRA, MVP MSFT, DPO
Chief Executive Officer (CEO) and Co-Founder
Cyber Security Philippines - Computer Emergency Response Team (CSP-CERT®)

DR. NIÑA ANA MARIE JOCELYN ALINDOGAN SALES, CLSSGB, DPO
Certification Program Manager
Bankers Institute of the Philippines Inc. (BAIPHIL)
and
Chief Operating Officer (COO) and Co-Founder
Cyber Security Philippines–Computer Emergency Response Team (CSP-CERT ®)

MS. FLEUR-DE-LIS A. NADUA
Critical Infostructure Evaluation and Cybersecurity Standards
Monitoring Division, Cybersecurity Bureau, DICT

MR. ALWELL MULSID
Chief, Cyber Incident Response Section
DICT

MR. MOSLEMEN MACARAMBON JR.
President & Co-Convenor
Democracy.Net.Ph

SSGT. MARK DAVE M. TACADENA
First Sergeant, 1st Cyber Mission Unit
Armed Forces of the Philippines Cyber Group

- **THE PARTICIPANTS IN THE NATIONAL VALIDATION OF THIS COMPETENCY STANDARDS**
    1. Arturo H. Samaniego, Jr.
    2. Denon G. Anchinges
    3. Garett L. Silao
    4. Jarek Boilo T. Cabautan
    5. Jessie James P. Custodio
    6. Nathanael S. Alcain
    7. Pierre Tito A. Galla
    8. Renato C. Del Rosario Jr.
    9. Rodolfo B. Bernabe Jr.

- **CYBER SECURITY PHILIPPINES – CERT**

- **DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY**

- **THE AFP – CYBER COMMAND GROUP**

- **MANDIANT (now part of Google Cloud)**

- **THE MANAGEMENT AND STAFF OF TESDA SECRETARIAT**

Qualifications and Standards Office (QSO)

Name	Company/industry	Email Address
El Cid H. Castillo	TESDA	ehcastillo@tesda.gov.ph
Bernadette S. Audije	TESDA	bsaudije@tesda.gov.ph
Samuel E. Calado Jr.	TESDA	secaladojr@tesda.gov.ph
Adrian Brian C. Sabanal	TESDA	acsabanal@tesda.gov.ph

Competency Standards are available in electronic copies for more information, please contact:

Technical Education and Skills Development Authority (TESDA)

Tele Fax No.: 8818-7728

or visit our website: www.tesda.gov.ph