COMPETENCY STANDARDS

SECURITY OPERATIONS CENTER (SOC) ANALYSIS LEVEL III

INFORMATION AND COMMUNICATIONS TECHNOLOGY 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. Registration and delivery of training programs;
2. Development of curriculum and assessment instruments; and

Each CS has two sections:

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

Section 2 **Competency Standards** gives the specifications of competencies required for effective work performance.

TABLE OF CONTENTS

INFORMATION AND COMMUNICATIONS TECHNOLOGY SECTOR
SECURITY OPERATIONS CENTER (SOC) ANALYSIS LEVEL III

COMPETENCY STANDARDS FOR
SECURITY OPERATIONS CENTER (SOC) ANALYSIS LEVEL III

SECTION 1: DEFINITION OF QUALIFICATION

The **SECURITY OPERATIONS CENTER (SOC) ANALYSIS LEVEL III** Qualification consists of competencies that a person must achieve to apply cybersecurity concepts, carry out network administration, secure network application, and hand cybersecurity incidents.

The Units of Competency comprising this Qualification include the following:

UNIT CODE	BASIC COMPETENCIES
400311319	Lead workplace communication
400311320	Lead small teams
400311321	Apply critical thinking and problem-solving techniques in the workplace
400311322	Work in a diverse environment
400311323	Propose methods of applying learning and innovation in the organization
400311324	Use information systematically
400311325	Evaluate occupational safety and health work practices
400311326	Evaluate environmental work practices
400311327	Facilitate entrepreneurial skills for micro-small-medium enterprises (MSMEs)

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

Unit Code	CORE COMPETENCIES
CS-ICT251109	Apply cybersecurity concepts
CS-ICT251110	Carry out network administration
CS-ICT251111	Secure network and application
CS-ICT251112	Handle cybersecurity incidents

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

- SOC analyst L1

SECTION 2: COMPETENCY STANDARDS

This section gives the details of the contents of the units of competency required in **SECURITY OPERATIONS CENTER (SOC) ANALYSIS LEVEL III**

BASIC COMPETENCIES

UNIT OF COMPETENCY : LEAD WORKPLACE COMMUNICATION

UNIT CODE : 400311319

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to lead in the dissemination and discussion of ideas, information and issues in the workplace.

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Communicate information about workplace processes	1.1 Relevant ***communication method*** is selected based on workplace procedures 1.2 Multiple operations involving several topics/areas are communicated following enterprise requirements 1.3 Questioning is applied to gain extra information 1.4 Relevant sources of information are identified in accordance with workplace/ client requirements 1.5 Information is selected and organized following enterprise procedures 1.6 Verbal and written reporting is undertaken when required 1.7 Communication and negotiation skills are applied and maintained in all relevant situations	1.1. Organization requirements for written and electronic communication methods 1.2. Effective verbal communication methods 1.3. Business writing 1.4. Workplace etiquette	1.1. Organizing information 1.2. Conveying intended meaning 1.3. Participating in a variety of workplace discussions 1.4. Complying with organization requirements for the use of written and electronic communication methods 1.5. Effective business writing 1.6. Effective clarifying and probing skills 1.7. Effective questioning techniques (clarifying and probing)
2. Lead workplace discussions	2.1 Response to workplace issues are sought following enterprise procedures 2.2 Response to workplace issues are provided immediately	2.1 Organization requirements for written and electronic communication methods	2.1 Organizing information 2.2 Conveying intended meaning 2.3 Participating in variety of

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	2.3 Constructive contributions are made to ***workplace discussions*** on such issues as production, quality and safety 2.4 Goals/objectives and action plans undertaken in the workplace are communicated promptly	2.2 Effective verbal communication methods 2.3 Workplace etiquette	workplace discussions 2.4 Complying with organization requirements for the use of written and electronic communication methods 2.5 Effective clarifying and probing skills
3. Identify and communicate issues arising in the workplace	3.1 Issues and problems are identified as they arise 3.2 Information regarding problems and issues are organized coherently to ensure clear and effective communication 3.3 Dialogue is initiated with appropriate personnel 3.4 Communication problems and issues are raised as they arise 3.5 Identify barriers in communication to be addressed appropriately	3.1 Organization requirements for written and electronic communication methods 3.2 Effective verbal communication methods 3.3 Workplace etiquette 3.4 Communication problems and issues 3.5 Barriers in communication	3.1 Organizing information 3.2 Conveying intended meaning 3.3 Participating in a variety of workplace discussions 3.4 Complying with organization requirements for the use of written and electronic communication methods 3.5 Effective clarifying and probing skills 3.6 Identifying issues 3.7 Negotiation and communication skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Methods of communication	May include: 1.1. Non-verbal gestures 1.2. Verbal 1.3. Face-to-face 1.4. Two-way radio 1.5. Speaking to groups 1.6. Using telephone 1.7. Written 1.8. Internet
2. Workplace discussions	May include: 2.1. Coordination meetings 2.2. Toolbox discussion 2.3. Peer-to-peer discussion

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Dealt with a range of communication/information at one time 1.2. Demonstrated leadership skills in workplace communication 1.3. Made constructive contributions in workplace issues 1.4. Sought workplace issues effectively 1.5. Responded to workplace issues promptly 1.6. Presented information clearly and effectively written form 1.7. Used appropriate sources of information 1.8. Asked appropriate questions 1.9. Provided accurate information
2. Resource Implications	The following resources should be provided: 2.1. Variety of Information 2.2. Communication tools 2.3. Simulated workplace
3. Methods of Assessment	Competency in this unit must be assessed through 3.1. Case problem 3.2. Third-party report 3.3. Portfolio 3.4. Interview 3.5. Demonstration/Role-playing
4. Context for Assessment	4.1. Competency may be assessed in the workplace or in simulated workplace environment

UNIT OF COMPETENCY : LEAD SMALL TEAMS

UNIT CODE : 400311320

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes to lead small teams including setting, maintaining and monitoring team and individual performance standards.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Provide team leadership	1.1. ***Work requirements*** are identified and presented to team members based on company policies and procedures 1.2. Reasons for instructions and requirements are communicated to team members based on company policies and procedures 1.3. ***Team members' queries and concerns*** are recognized, discussed and dealt with based on company practices	1.1 Facilitation of Team work 1.2 Company policies and procedures relating to work performance 1.3 Performance standards and expectations 1.4 Monitoring individual's and team's performance vis a vis client's and group's expectations	1.1 Communication skills required for leading teams 1.2 Group facilitation skills 1.3 Negotiating skills 1.4 Setting performance expectation
2. Assign responsibilities	2.1. Responsibilities are allocated having regard to the skills, knowledge and aptitude required to undertake the assigned task based on company policies. 2.2. Duties are allocated having regard to individual preference, domestic and personal considerations, whenever possible	2.1 Work plan and procedures 2.2 Work requirements and targets 2.2 Individual and group expectations and assignments 2.3 Ways to improve group leadership and membership	2.1 Communication skills 2.2 Management skills 2.3 Negotiating skills 2.4 Evaluation skills 2.5 Identifying team member's strengths and rooms for improvement
3. Set performance expectations	3.1 Performance expectations are	3.1 One's roles and responsibilities in the team	3.1 Communication skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
for team members	established based on client needs 3.2 Performance expectations are based on individual team members knowledge, skills and aptitude 3.3 Performance expectations are discussed and disseminated to individual team members	3.2 Feedback giving and receiving 3.3 Performance expectation	3.2 Accurate empathy 3.3 Congruence 3.4 Unconditional positive regard 3.5 Handling of Feedback
4. Supervised team performance	4.1 Performance is ***monitored*** based on defined performance criteria and/or assignment instructions 4.2 Team members are provided with ***feedback***, positive support and advice on strategies to overcome any deficiencies based on company practices 4.3 ***Performance issues*** which cannot be rectified or addressed within the team are referenced to appropriate personnel according to employer policy 4.4 Team members are kept informed of any changes in the priority allocated to assignments or tasks which might impact on client/customer needs and satisfaction 4.5 Team operations are monitored to ensure that employer/client	4.1 Performance Coaching 4.2 Performance management 4.3 Performance Issues	4.1 Communication skills required for leading teams 4.2 Coaching skill

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	needs and requirements are met 4.6 Follow-up communication is provided on all issues affecting the team 4.7 All relevant documentation is completed in accordance with company procedures		

RANGE OF VARIABLES

VARIABLE	RANGE
1. Work requirements	May include: 1.1. Client Profile 1.2. Assignment instructions
2. Team member's concerns	May include: 2.1. Roster/shift details
3. Monitor performance	May include: 3.1. Formal process 3.2. Informal process
4. Feedback	May include: 4.1. Formal process 4.2. Informal process
5. Performance issues	May include: 5.1. Work output 5.2. Work quality 5.3. Team participation 5.4. Compliance with workplace protocols 5.5. Safety 5.6. Customer service

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Maintained or improved individuals and/or team performance given a variety of possible scenario 1.2. Assessed and monitored team and individual performance against set criteria 1.3. Represented concerns of a team and individual to next level of management or appropriate specialist and to negotiate on their behalf 1.4. Allocated duties and responsibilities, having regard to individual's knowledge, skills and aptitude and the needs of the tasks to be performed 1.5. Set and communicated performance expectations for a range of tasks and duties within the team and provided feedback to team members
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 Examination 3.2. Oral Questioning 3.3. Portfolio
4. Context for Assessment	4.1. Competency may be assessed in actual workplace or at the designated TESDA Accredited Assessment Center

UNIT OF COMPETENCY: APPLY CRITICAL THINKING AND PROBLEM-SOLVING TECHNIQUES IN THE WORKPLACE

UNIT CODE : 400311321

UNIT DESCRIPTOR : This unit 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/s of specific problems in the workplace.

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Examine specific workplace challenges	1.1. Variances are examined from normal operating **parameters;** and product quality. 1.2. Extent, cause and nature of the specific problem are defined through observation, investigation and ***analytical techniques***. 1.3. ***Problems*** are clearly stated and specified.	1.1. Competence includes a thorough 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, enough for the identification of fundamental causes of specific workplace challenges. 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 analytical techniques (e.g., planning, attention, simultaneous and successive processing of information) in examining specific challenges in the workplace. 1.2. Identifying extent and causes of specific challenges in the workplace.
2. Analyze the causes of specific workplace challenges.	2.1. Possible causes of specific problems are identified based on experience and the use of problem solving tools **/** analytical techniques. 2.2. Possible cause statements are	2.1 Competence includes a thorough knowledge and understanding of the process, normal operating parameters, and product quality to	2.1 Using range of analytical techniques (e.g., planning, attention, simultaneous and successive processing of information) in

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	developed based on findings. 2.3. Fundamental causes are identified per results of investigation conducted.	recognize non-standard situations. 2.2 Competence to include the ability to apply and explain, sufficient for the identification of fundamental cause, determining the corrective action and provision of recommendations. 2.3 Relevant equipment and operational processes. 2.4 Enterprise goals, targets and measures. 2.5 Enterprise quality OSH and environmental requirement. 2.6 Enterprise information systems and data collation. 2.7 Industry codes and standards.	examining specific challenges in the workplace. 2.2 Identifying extent and causes of specific challenges in the workplace. 2.3 Providing clear-cut findings on the nature of each identified workplace challenges.
3. Formulate resolutions to specific workplace challenges	3.1. All possible options are considered for resolution of the problem. 3.2. Strengths and weaknesses of possible options are considered. 3.3. Corrective actions are determined to resolve the problem and possible future causes. 3.4. **Action *plans*** are developed identifying measurable objectives, resource needs and timelines in accordance with safety and operating procedures	3.1. Competence to include the ability to apply and explain, sufficient for the identification of fundamental cause, determining the corrective action and provision of recommendations 3.2. Relevant equipment and operational processes 3.3. Enterprise goals, targets and measures 3.4. Enterprise quality OSH and environmental requirement 3.5. Principles of decision making strategies and techniques 3.6. Enterprise information systems and data collation	3.1. Using range of analytical techniques (e.g., planning, attention, simultaneous and successive processing of information) in examining specific challenges in the workplace. 3.2. Identifying extent and causes of specific challenges in the workplace. 3.3. Providing clear-cut findings on the nature of each identified workplace challenges.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
		3.7. Industry codes and standards	3.4. Devising, communicating, implementing and evaluating strategies and techniques in addressing specific workplace challenges.
4. Implement action plans and communicate results	4.1. Action plans are implemented and evaluated. 4.2. Results of plan implementation and recommendations are prepared. 4.3. Recommendations are presented to appropriate personnel. 4.4. Recommendations are followed-up, if required.	4.1 Competence to include the ability to apply and explain, sufficient for the identification of fundamental cause, determining the corrective action and provision of recommendations 4.2. Relevant equipment and operational processes 4.3 Enterprise goals, targets and measures 4.4 Enterprise quality, OSH and environmental requirement 4.5 Principles of decision making strategies and techniques 4.6 Enterprise information systems and data collation 4.7 Industry codes and standards	4.1 Using range of analytical techniques (e.g., planning, attention, simultaneous and successive processing of information) in examining specific challenges in the workplace. 4.2 Identifying extent and causes of specific challenges in the workplace. 4.3 Providing clear-cut findings on the nature of each identified workplace challenges. 4.4 Devising, communicating, implementing and evaluating strategies and techniques in addressing specific workplace challenges.

RANGE OF VARIABLES

VARIABLES	RANGE
1. Parameters	May include: 1.1 Processes 1.2 Procedures 1.3 Systems
2. Analytical techniques	May include: 2.1. Brainstorming 2.2. Intuitions/Logic 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. Problem	May include: 3.1. Routine, non – routine and complex workplace and quality problems 3.2. Equipment selection, availability and failure 3.3. Teamwork and work allocation problem 3.4. Safety and emergency situations and incidents 3.5. Risk assessment and management
4. Action plans	May include: 4.1. Priority requirements 4.2. Measurable objectives 4.3. Resource requirements 4.4. Timelines 4.5. Co-ordination and feedback requirements 4.6. Safety requirements 4.7. Risk assessment 4.8. Environmental requirements

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Examined specific workplace challenges. 1.2. Analyzed the causes of specific workplace challenges. 1.3. Formulated resolutions to specific workplace challenges. 1.4. Implemented action plans and communicated results on specific workplace challenges.
2. Resource Implications	2.1. Assessment will require access to an operating plant over an extended period of time, or a suitable method of gathering evidence of operating ability over a range of situations. A bank of scenarios / case studies / what ifs will be required as well as bank of questions which will be used to probe the reason behind the observable action.
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Observation 3.2. Case Formulation 3.3. Life Narrative Inquiry 3.4. 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. In all workplace, it may be appropriate to assess this unit concurrently with relevant teamwork or operation units.

UNIT OF COMPETENCY : WORK IN A DIVERSE ENVIRONMENT

UNIT CODE : 400311322

UNIT DESCRIPTOR : This unit covers the outcomes required to work effectively in a workplace characterized by diversity in terms of religions, beliefs, races, ethnicities and other differences.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Develop an individual's cultural awareness and sensitivity	1.1. Individual differences with clients, customers and fellow workers are recognized and respected in accordance with enterprise policies and core values. 1.2. Differences are responded to in a sensitive and considerate manner 1.3. ***Diversity*** is accommodated using appropriate verbal and non-verbal communication.	1.1. Understanding cultural diversity in the workplace 1.2. Norms of behavior for interacting and dialogue with specific groups (e. g., Muslims and other non-Christians, non-Catholics, tribes/ethnic groups, foreigners) 1.3. Different methods of verbal and non-verbal communication in a multicultural setting	1.1. Applying cross-cultural communication skills (i.e. different business customs, beliefs, communication strategies) 1.2. Showing affective skills – establishing rapport and empathy, understanding, etc. 1.3. Demonstrating openness and flexibility in communication 1.4. Recognizing diverse groups in the workplace and community as defined by divergent culture, religion, traditions and practices
2. Work effectively in an environment that acknowledges and values cultural diversity	2.1 Knowledge, skills and experiences of others are recognized and documented in relation to team objectives. 2.2 Fellow workers are encouraged to utilize and share their specific qualities, skills or backgrounds with other team members and clients to enhance work outcomes. 2.3 Relations with customers and clients are maintained to show that	2.1 Value of diversity in the economy and society in terms of Workforce development 2.2 Importance of inclusiveness in a diverse environment 2.3 Shared vision and understanding of and commitment to team, departmental, and organizational goals and objectives 2.4 Strategies for customer service excellence	2.1 Demonstrating cross-cultural communication skills and active listening 2.2 Recognizing diverse groups in the workplace and community as defined by divergent culture, religion, traditions and practices 2.3 Demonstrating collaboration skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	diversity is valued by the business.		2.4 Exhibiting customer service excellence
3. Identify common issues in a multicultural and diverse environment	3.1 ***Diversity-related conflicts*** within the workplace are effectively addressed and resolved. 3.2 Discriminatory behaviors towards customers/stakeholders are minimized and addressed accordingly. 3.3 Change management policies are in place within the organization.	3.1 Value, and leverage of cultural diversity 3.2 Inclusivity and conflict resolution 3.3 Workplace harassment 3.4 Change management and ways to overcome resistance to change 3.5 Advanced strategies for customer service excellence	3.1 Addressing diversity-related conflicts in the workplace 3.2 Eliminating discriminatory behavior towards customers and co-workers 3.3 Utilizing change management policies in the workplace

RANGE OF VARIABLES

VARIABLE	RANGE
1. Diversity	This refers to diversity in both the workplace and the community and may include divergence in : 1.1 Religion 1.2 Ethnicity, race or nationality 1.3 Culture 1.4 Gender, age or personality 1.5 Educational background
2. Diversity-related conflicts	May include conflicts that result from: 2.1 Discriminatory behaviors 2 Differences of cultural practices 3 Differences of belief and value systems 4 Gender-based violence 5 Workplace bullying 6 Corporate jealousy 7 Language barriers 8 Individuals being differently-abled persons 2.9 Ageism (negative attitude and behavior towards old people)

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Adjusted language and behavior as required by interactions with diversity 1.2 Identified and respected individual differences in colleagues, clients and customers 1.3 Applied relevant regulations, standards and codes of practice
2. Resource Implications	The following resources should be provided: 2.1 Access to workplace and resources 2.2 Manuals and policies on Workplace Diversity
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1 Demonstration or simulation with oral questioning 3.2 Group discussions and interactive activities 3.3 Case studies/problems involving workplace diversity issues 3.4 Third-party report 3.5 Written examination 3.6 Role Plays
4. Context for Assessment	Competency assessment may occur in workplace or any appropriately simulated environment

UNIT OF COMPETENCY: PROPOSE METHODS OF APPLYING LEARNING AND INNOVATION IN THE ORGANIZATION

UNIT CODE : 400311323

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to assess general obstacles in the application of learning and innovation in the organization and to propose practical methods of such in addressing organizational challenges.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Assess work procedures, processes and systems in terms of innovative practices	1.1. R***easons*** for innovation are incorporated to work procedures. 1.2. ***Models of innovation*** are researched. 1.3. G***aps or barriers*** to innovation in one's work area are analyzed. 1.4. Staff who can support and foster innovation in the work procedure are identified.	1.1 Seven habits of highly effective people. 1.2 Character strengths that foster innovation and learning (Christopher Peterson and Martin Seligman, 2004) 1.3 Five minds of the future concepts (Gardner, 2007). 1.4 Adaptation concepts in neuroscience (Merzenich, 2013). 1.5 Transtheoretical model of behavior change (Prochaska, DiClemente, & Norcross, 1992).	1.1 Demonstrating collaboration and networking skills. 1.2 Applying basic research and evaluation skills 1.3 Generating insights on how to improve organizational procedures, processes and systems through innovation.
2. Generate practical action plans for improving work procedures, processes	2.1 Ideas for innovative work procedure to foster innovation using individual and group techniques are conceptualized 2.2 Range of ideas with other team members and colleagues are evaluated and discussed 2.3 Work procedures and processes subject to change are selected based on ***workplace requirements*** (feasible and innovative). 2.4 Practical action plans are proposed to facilitate simple changes in the work procedures, processes and systems. 2.5 ***Critical inquiry*** is applied and used to	2.1 Seven habits of highly effective people. 2.2 Character strengths that foster innovation and learning (Christopher Peterson and Martin Seligman, 2004) 2.3 Five minds of the future concepts (Gardner, 2007). 2.4 Adaptation concepts in neuroscience (Merzenich, 2013). 2.5 Transtheoretical model of behavior change (Prochaska, DiClemente, & Norcross, 1992).	2.1 Assessing readiness for change on simple work procedures, processes and systems. 2.2 Generating insights on how to improve organizational procedures, processes and systems through innovation. 2.3 Facilitating action plans on how to apply innovative procedures in the organization.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	facilitate discourse on adjustments in the simple work procedures, processes and systems.		
3. Evaluate the effectiveness of the proposed action plans	3.1 Work structure is analyzed to identify the impact of the new work procedures 3.2 Co-workers/key personnel is consulted to know who will be involved with or affected by the work procedure 3.3 Work instruction operational plan of the new work procedure is developed and evaluated. 3.4 Feedback and suggestion are recorded. 3.5 Operational plan is updated. 3.6 Results and impact on the developed work instructions are reviewed 3.7 Results of the new work procedure are evaluated 3.8 Adjustments are recommended based on results gathered	3.1 Five minds of the future concepts (Gardner, 2007). 3.2 Adaptation concepts in neuroscience (Merzenich, 2013). 3.3 Transtheoretical model of behavior change (Prochaska, DiClemente, & Norcross, 1992).	3.1 Generating insights on how to improve organizational procedures, processes and systems through innovation. 3.2 Facilitating action plans on how to apply innovative procedures in the organization. 3.3 Communicating results of the evaluation of the proposed and implemented changes in the workplace procedures and systems. 3.4 Developing action plans for continuous improvement on the basic systems, processes and procedures in the organization.

RANGE OF VARIABLES

VARIABLE	RANGE
1. Reasons	May include: 1.1. Strengths and weaknesses of the current systems, processes and procedures. 1.2. Opportunities and threats of the current systems, processes and procedures.
2. Models of innovation	May include: 2.1. Seven habits of highly effective people. 2.2. Five minds of the future concepts (Gardner, 2007). 2.3. Neuroplasticity and adaptation strategies.
3. Workplace requirements	May include: 3.1. Feasible 3.2. Innovative
4. Gaps or barriers	May include: 4.1. Machine 4.2. Manpower 4.3. Methods 4.4. Money
5. Critical Inquiry	May include: 5.1. Preparation. 5.2. Discussion. 5.3. Clarification of goals. 5.4. Negotiate towards a Win-Win outcome. 5.5. Agreement. 5.6. Implementation of a course of action. 5.7. Effective verbal communication. See our pages: Verbal Communication and Effective Speaking. 5.8. Listening. 5.9. Reducing misunderstandings is a key part of effective negotiation. 5.10. Rapport Building. 5.11. Problem Solving. 5.12. Decision Making. 5.13. Assertiveness. 5.14. Dealing with Difficult Situations.

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Established the reasons why innovative systems are required 1.2. Established the goals of a new innovative system 1.3. Analyzed current organizational systems to identify gaps and barriers to innovation. 1.4. Assessed work procedures, processes and systems in terms of innovative practices. 1.5. Generated practical action plans for improving work procedures, and processes. 1.6. Reviewed the trial innovative work system and adjusted reflect evaluation feedback, knowledge management systems and future planning. 1.7. Evaluated the effectiveness of the proposed action plans.
2. Resource Implications	The following resources should be provided: 2.1. Pens, papers and writing implements. 2.2. Cartolina. 2.3. Manila papers
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Psychological and behavioral Interviews. 3.2. Performance Evaluation. 3.3. Life Narrative Inquiry. 3.4. Review of portfolios of evidence and third-party workplace reports of on-the-job performance. 3.5. Sensitivity analysis. 3.6. Organizational analysis. 3.7. Standardized assessment of character strengths and virtues applied.
4. Context for Assessment	Competency may be assessed individually in the actual workplace or simulation environment in TESDA accredited institutions.

UNIT OF COMPETENCY: USE INFORMATION SYSTEMATICALLY

UNIT CODE : 400311324

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to use technical information systems, apply information technology (IT) systems and edit, format & check information.

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Use technical information	1.1. ***Information*** are collated and organized into a suitable form for reference and use 1.2. Stored information are classified so that it can be quickly identified and retrieved when needed 1.3. Guidance are advised and offered to people who need to find and use information	1.1. Application in collating information 1.2. Procedures for inputting, maintaining and archiving information 1.3. Guidance to people who need to find and use information 1.4. Organize information 1.5. classify stored information for identification and retrieval 1.6. Operate the technical information system by using agreed procedures	1.1. Collating information 1.2. Operating appropriate and valid procedures for inputting, maintaining and archiving information 1.3. Advising and offering guidance to people who need to find and use information 1.4. Organizing information into a suitable form for reference and use 1.5. Classifying stored information for identification and retrieval 1.6. Operating the technical information system by using agreed procedures
2. Apply information technology (IT)	2.1. ***Technical information*** system is operated using agreed procedures 2.2. Appropriate and valid procedures are operated for inputting, maintaining and archiving information 2.3. ***Software*** required are utilized to execute the project activities 2.4. Information and data obtained are handled, edited, formatted and checked from a range of	2.1. Attributes and limitations of available software tools 2.2. Procedures and work instructions for the use of IT 2.3. Operational requirements for IT systems 2.4. Sources and flow paths of data 2.5. Security systems and measures that can be used 2.6. Extract data and format reports	2.1. Identifying attributes and limitations of available software tools 2.2. Using procedures and work instructions for the use of IT 2.3. Describing operational requirements for IT systems 2.4. Identifying sources and flow paths of data

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	internal and external ***sources*** 2.5. Information are extracted, entered, and processed to produce the outputs required by ***customers*** 2.6. Own skills and understanding are shared to help others 2.7. Specified ***security measures*** are implemented to protect the confidentiality and integrity of project data held in IT systems	2.7. Methods of entering and processing information 2.8. WWW enabled applications	2.5. Determining security systems and measures that can be used 2.6. Extracting data and format reports 2.7. Describing methods of entering and processing information 2.8. Using WWW applications
3. Edit, format and check information	3.1 Basic editing techniques are used 3.2 Accuracy of documents are checked 3.3 Editing and formatting tools and techniques are used for more complex documents 3.4 Proof reading techniques is used to check that documents look professional	3.1 Basic file-handling techniques 3.2 Techniques in checking documents 3.3 Techniques in editing and formatting 3.4 Proof reading techniques	3.1 Using basic file-handling techniques is used for the software 3.2 Using different techniques in checking documents 3.3 Applying editing and formatting techniques 3.4 Applying proof reading techniques

RANGE OF VARIABLES

VARIABLE	RANGE
1. Information	May include: 1.1. Property 1.2. Organizational 1.3. Technical reference
2. Technical information	May include: 2.1. paper based 2.2. electronic
3. Software	May include: 3.1. spreadsheets 3.2. databases 3.3. word processing 3.4. presentation
4. Sources	May include: 4.1. other IT systems 4.2. manually created 4.3. within own organization 4.4. outside own organization 4.5. geographically remote
5. Customers	May include: 5.1. colleagues 5.2. company and project management 5.3. clients
6. Security measures	May include: 6.1. access rights to input; 6.2. passwords; 6.3. access rights to outputs; 6.4. data consistency and back-up; 6.5. recovery plans

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Used technical information systems and information technology 1.2. Applied information technology (IT) systems 1.3. Edited, formatted and checked information
2. Resource Implications	The following resources should be provided: 2.1. Computers 2.2. Software and IT system
3. Methods of Assessment	Competency in this unit MUST be assessed through: 3.1. Direct Observation 3.2. Oral interview and written test
4. Context for Assessment	4.1. Competency may be assessed individually in the actual workplace or through accredited institution

UNIT OF COMPETENCY : EVALUATE OCCUPATIONAL SAFETY AND HEALTH WORK PRACTICES

UNIT CODE : 400311325

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to interpret-Occupational Safety and Health practices, set OSH work targets, and evaluate effectiveness of Occupational Safety and Health work instructions

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Interpret Occupational Safety and Health practices	1.1 ***OSH work practices issues*** are identified relevant to work requirements 1.2 OSH work standards and procedures are determined based on applicability to nature of work 1.3 Gaps in work practices are identified related to relevant OSH work standards	1.1. OSH work practices issues 1.2. OSH work standards 1.3. General OSH principles and legislations 1.4. Company/ workplace policies/ guidelines 1.5. Standards and safety requirements of work process and procedures	1.1. Communication skills 1.2. Interpersonal skills 1.3. Critical thinking skills 1.4. Observation skills
2. Set OSH work targets	2.1 Relevant work information are gathered necessary to determine OSH work targets 2.2 ***OSH Indicators*** based on gathered information are agreed upon to measure effectiveness of workplace OSH policies and procedures 2.3 Agreed OSH indicators are endorsed for approval from appropriate personnel 2.4 ***OSH work instructions*** are received in accordance with workplace policies and procedures*	2.1. OSH work targets 2.2. OSH Indicators 2.3. OSH work instructions 2.4. Safety and health requirements of tasks 2.5. Workplace guidelines on providing feedback on OSH and security concerns 2.6. OSH regulations Hazard control procedures 2.7. OSH trainings relevant to work	2.1. Communication skills 2.2. Collaborating skills 2.3. Critical thinking skills 2.4. Observation skills
3. Evaluate effectiveness of Occupational Safety and Health work instructions	3.1 OSH Practices are observed based on workplace standards 3.2 Observed OSH practices are measured against approved ***OSH metrics*** 3.3 Findings regarding effectiveness are assessed and gaps identified are implemented based on OSH work standards	3.1. OSH Practices 3.2. OSH metrics 3.3. OSH Evaluation Techniques 3.4. OSH work standards	3.1. Critical thinking skills 3.2. Evaluating skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. OSH Work Practices Issues	May include: 1.1 Workers' experience/observance on presence of work hazards 1.2 Unsafe/unhealthy administrative arrangements (prolonged work hours, no break-time, constant overtime, scheduling of tasks) 1.3 Reasons for compliance/non-compliance to use of PPEs or other OSH procedures/policies/ guidelines
2. OSH Indicators	May include: 2.1 Increased of incidents of accidents, injuries 2.2 Increased occurrence of sickness or health complaints/symptoms 2.3 Common complaints of workers' related to OSH 2.4 High absenteeism for work-related reasons
3. OSH Work Instructions	May include: 3.1 Preventive and control measures**,** and targets 3.2 Eliminate the hazard (i.e., get rid of the dangerous machine 3.3 Isolate the hazard (i.e. keep the machine in a closed room and operate it remotely; barricade an unsafe area off) 3.4 Substitute the hazard with a safer alternative (i.e., replace the machine with a safer one) 3.5 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) 3.6 Use engineering controls to reduce the risk (i.e. use safety guards to machine) 3.7 Use personal protective equipment 3.8 Safety, Health and Work Environment Evaluation 3.9 Periodic and/or special medical examinations of workers
4. OSH metrics	May include: 4.1 Statistics on incidence of accidence and injuries 4.2 Morbidity (Type and Number of Sickness) 4.3 Mortality (Cause and Number of Deaths) 4.4 Accident Rate

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Identify OSH work practices issues relevant to work requirements 1.2. Identify gaps in work practices related to relevant OSH work standards 1.3. Agree upon OSH Indicators based on gathered information to measure effectiveness of workplace OSH policies and procedures 1.4. Receive OSH work instructions in accordance with workplace policies and procedures 1.5. Compare Observed OSH practices with against approved OSH work instructions 1.6. Assess findings regarding effectiveness based on OSH work standards
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 3.3 Written exam
4. Context for Assessment	4.1 Competency may be assessed in the work place or in a simulated work place setting

UNIT OF COMPETENCY : EVALUATE ENVIRONMENTAL WORK PRACTICES
UNIT CODE : 400311326
UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitude to interpret environmental Issues, establish targets to evaluate environmental practices and evaluate effectiveness of environmental practices

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Interpret environmental practices, policies and procedures	1.1 Environmental work practices issues are identified relevant to work requirements 1.2 Environmental Standards and Procedures nature of work are determined based on Applicability to nature of work 1.3 Gaps in work practices related to Environmental Standards and Procedures are identified	1.1 Environmental Issues 1.2 Environmental Work Procedures 1.3 Environmental Laws 1.4 Environmental Hazardous and Non-Hazardous Materials 1.5 Environmental required license, registration or certification	1.1. Analyzing Environmental Issues and Concerns 1.2. Critical thinking 1.3. Problem Solving 1.4. Observation Skills
2. Establish targets to evaluate environmental practices	2.1. Relevant information is gathered necessary to determine environmental work targets 2.2. Environmental Indicators based on gathered information are set to measure environmental work targets 2.3. Indicators are verified with appropriate personnel	2.1. Environmental Indicators 2.2. Relevant Environment Personnel or expert 2.3. Relevant Environmental Trainings and Seminars	2.1. Investigative Skills 2.2. Critical thinking 2.3. Problem Solving 2.4. Observation Skills
3. Evaluate effectiveness of environmental practices	3.1. Work environmental practices are recorded based on workplace standards 3.2. Recorded work environmental practices are compared against planned indicators 3.3. Findings regarding effectiveness are assessed and gaps identified are implemented based on environment work standards and procedures 3.4. Results of environmental assessment are conveyed to appropriate personnel	1.1. Environmental Practices 1.2. Environmental Standards and Procedures	3.1 Documentation and Record Keeping Skills 3.2 Critical thinking 3.3 Problem Solving 3.4 Observation Skills

RANGE OF VARIABLES

VARIABLE	R A N G E
1. Environmental Practices Issues	May include: 1.1 Water Quality 1.2 National and Local Government Issues 1.3 Safety 1.4 Endangered Species 1.5 Noise 1.6 Air Quality 1.7 Historic 1.8 Waste 1.9 Cultural
2. Environmental Indicators	May include: 2.1 Noise level 2.2 Lighting (Lumens) 2.3 Air Quality - Toxicity 2.4 Thermal Comfort 2.5 Vibration 2.6 Radiation 2.7 Quantity of the Resources 2.8 Volume

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Identified environmental issues relevant to work requirements 1.2. Identified gaps in work practices related to Environmental Standards and Procedures 1.3. Gathered relevant information necessary to determine environmental work targets 1.4. Set environmental indicators based on gathered information to measure environmental work targets 1.5. Recorded work environmental practices are recorded based on workplace standards 1.6. Conveyed results of environmental assessment to appropriate personnel
2. Resource Implications	The following resources should be provided: 2.1 Workplace/Assessment location 2.2 Legislation, policies, procedures, protocols and local ordinances relating to environmental protection 2.3 Case studies/scenarios relating to environmental protection
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1 Written/ Oral Examination 3.2 Interview/Third Party Reports 3.3 Portfolio (citations/awards from GOs and NGOs, certificate of training – local and abroad) 3.4 Simulations and role-plays
4. Context for Assessment	4.1 Competency may be assessed in actual workplace or at the designated TESDA center.

UNIT OF COMPETENCY : FACILITATE ENTREPRENEURIAL SKILLS FOR MICRO-SMALL-MEDIUM ENTERPRISES (MSMEs)

UNIT CODE : 400311327

UNIT DESCRIPTOR : This unit covers the outcomes required to build, operate and grow a micro/small-scale enterprise.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Develop and maintain micro-small-medium enterprise (MSMEs) skills in the organization	1.1 Appropriate ***business strategies*** are determined and set for the enterprise based on current and emerging business environment. 1.2 ***Business operations*** are monitored and controlled following established procedures. 1.3 Quality assurance measures are implemented consistently. 1.4 Good relations are maintained with staff/workers. 1.5 Policies and procedures on occupational safety and health and environmental concerns are constantly observed.	1.1 Business models and strategies 1.2 Types and categories of businesses 1.3 Business operation 1.4 Basic Bookkeeping 1.5 Business internal controls 1.6 Basic quality control and assurance concepts 1.7 Government and regulatory processes	1.1 Basic bookkeeping/ accounting skills 1.2 Communication skills 1.3 Building relations with customer and employees 1.4 Building competitive advantage of the enterprise
2. Establish and Maintain client-base/market	2.1 Good customer relations are maintained 2.2 New customers and markets are identified, explored and reached out to. 2.3 Promotions/Incentives are offered to loyal customers 2.4 Additional products and services are evaluated and tried where feasible. 2.5 ***Promotional/advertising initiatives*** are carried out where necessary and feasible.	2.1 Public relations concepts 2.2 Basic product promotion strategies 2.3 Basic market and feasibility studies 2.4 Basic business ethics	2.1 Building customer relations 2.2 Individual marketing skills 2.3 Using basic advertising (posters/ tarpaulins, flyers, social media, etc.)
3. Apply budgeting and financial management skills	3.1 Enterprise is built up and sustained through judicious control of cash flows. 3.2 Profitability of enterprise is ensured though appropriate ***internal controls***. 3.3 Unnecessary or lower-priority expenses and purchases are avoided.	3.1 Cash flow management 3.1 Basic financial management 3.2 Basic financial accounting 3.3 Business internal controls	3.1 Setting business priorities and strategies 3.2 Interpreting basic financial statements 3.3 Preparing business plans

RANGE OF VARIABLES

VARIABLE	RANGE
1. Business strategies	May include: 1.1. Developing/Maintaining niche market 1.2. Use of organic/healthy ingredients 1.3. Environment-friendly and sustainable practices 1.4. Offering both affordable and high-quality products and services 1.5. Promotion and marketing strategies (e. g., on-line marketing)
2. Business operations	May include: 2.1 Purchasing 2.2 Accounting/Administrative work 2.3 Production/Operations/Sales
3. Internal controls	May include: 3.1 Accounting systems 3.2 Financial statements/reports 3.3 Cash management
4. Promotional/ Advertising initiatives	May include: 4.1 Use of tarpaulins, brochures, and/or flyers 4.2 Sales, discounts and easy payment terms 4.3 Use of social media/Internet 4.4 "Service with a smile" 4.5 Extra attention to regular customers

EVIDENCE GUIDE

1. Critical aspects of competency	**Assessment requires evidence that the candidate :** 1.1. Demonstrated basic entrepreneurial skills 1.2. Demonstrated ability to conceptualize and plan a micro/small enterprise 1.3. Demonstrated ability to manage/operate a micro/small-scale business
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. Portfolio assessment with interview 3.4. Case problems
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

CORE COMPETENCIES

UNIT OF COMPETENCY: APPLY CYBERSECURITY CONCEPTS

UNIT CODE: CS-ICT251109

UNIT DESCRIPTOR: This unit covers the outcomes required in identifying types of attaches, their capabilities, strategies and the various malwares used to target victims.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	Required Knowledge	Required Skills
1. Identify vulnerabilities, risks and threats	1.1 ***Vulnerabilities*** are identified based on industry standards 1.2 ***Risks*** are identified based on industry standards 1.3 ***Threats*** are identified based on industry standards	1.1 Introduction to cybersecurity 1.2 Cybersecurity principles and concepts 1.3 Cybersecurity threats: • Malware • Risks • Vulnerabilities • Attackers 1.4 Security architecture and models 1.5 Introduction to cryptography 1.6 Network security 1.7 Operating systems • Windows • Linux • macOS 1.8 MITRE Att&ck Framework 1.9 NIST	1.1 Learning agility 1.2 Threat/malware analysis skills 1.3 Digital forensics 1.4 Effective communication 1.5 Problem-solving skills 1.6 Strategic planning 1.7 Critical thinking skills 1.8 Computer application skills 1.9 Networking skills 1.10 Using MITRE Att&ck framework
2. Identify malwares and attackers	2.1 ***Malwares*** are identified based on industry standards 2.2 ***Attackers*** are identified based on industry standards 2.3 ***Cyber incidents*** are identified based on industry standards	2.1 Introduction to cybersecurity 2.2 Cybersecurity principles and concepts 2.3 Cybersecurity threats: • Malware • Risks • Vulnerabilities	2.1 Learning agility 2.2 Threat/malware analysis skills 2.3 Digital forensics 2.4 Effective communication

		• Attackers 2.4 Security architecture and models 2.5 Introduction to cryptography 2.6 Network security 2.7 Operating systems • Windows • Linux • macOS 2.8 MITRE Att&ck Framework 2.4 NIST	2.5 Problem-solving skills 2.6 Strategic planning 2.7 Critical thinking skills 2.8 Computer application skills 2.9 Networking skills 2.1 Using MITRE Att&ck framework

RANGE OF VARIABLES

VARIABLE	RANGE
1. Vulnerabilities	May include but not limited to: 1.1 Unpatched Software 1.2 Weak Passwords 1.3 Misconfigured Firewalls
2. Risks	May include but not limited to: 2.1 Data Breach 2.2 Legal and Regulatory Non-Compliance 2.3 Business Disruption
3. Threats	May include but not limited to: 3.1 phishing Attacks 3.2 Ransomware
4. Malwares	May include but not limited to: 4.1 Trojan Horse 4.2 Worms 4.3 Spyware
5. Attackers	May include but not limited to: 5.1 Hackers 5.2 Cybercriminals 5.3 State-Sponsored Actors
6. Cyber incidents	May include but not limited to: 6.1 Distributed Denial of Service (DDoS) Attack 6.2 Insider Data Theft:

EVIDENCE GUIDE

1. Critical aspects of competency	1.1 Identified vulnerabilities, risks and threats 1.2 Identified malwares and attackers
2. Resource implications	The following resources should be provided: 2.1 Facilities, equipment, tools, materials and supplies relevant to the unit of competency
3. Methods of assessment	Competency in this unit must be assessed through any or combination of the following: 3.1 Demonstration with questioning 3.2 Written Test 3.3 Oral questioning/interview
4. Context for assessment	4.1 Competency maybe assessed in actual workplace or at the designated TESDA accredited Assessment Center

UNIT OF COMPETENCY: CARRY OUT NETWORK ADMINISTRATION

UNIT CODE: CS-ICT251110

UNIT DESCRIPTOR: This unit covers the outcomes required in configuring network and troubleshooting and monitoring network.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	Required Knowledge	Required Skills
1. Configure network	1.1 Network requirements are defined based on the needs 1.2 ***Network devices*** are gathered and prepared 1.3 IP address scheme is planned based on the need 1.4 Physical connections are set up based on industry standards 1.5 Network devices are configured based on industry standards 1.6 Subnets, VLANs or segmentation are created based on the need 1.7 Network devices are connected and configured 1.8 Wireless connection is set up based on industry standards 1.9 Connectivity is tested based on industry standards 1.10 Network security is applied based on industry standards	1.1 Introduction to networking 1.2 Network topologies 1.3 Network Devices and Hardware 1.4 IP Addressing 1.5 Network Protocols 1.6 Routing and Switching 1.7 Network Services 1.8 Wireless Networking 1.9 Network Security 1.10 Network virtualization 1.11 Network Services and Applications 1.12 Network segmentation and subnetting 1.13 System administration	1.1 Computer operation skills 1.2 Networking skills 1.3 Documentation skills 1.4 Problem-solving skills 1.5 Analytical skills 1.6 Learning agility 1.7 Applying security in networks 1.8 Effective communication skills
2. Troubleshoot and monitor network	2.1 ***Problems in the network*** are identified based on industry standards 2.2 Physical connections are checked based on industry standards 2.3 DNS configuration are checked based on industry standards 2.4 Logs are reviewed and checked based on industry standards	2.1 Office productivity tools 2.2 DNS configuration 2.3 Introduction to networking 2.4 Network topologies 2.5 Network Devices and Hardware	2.1 Computer operation skills 2.2 Networking skills 2.3 Documentation skills 2.4 Problem-solving skills 2.5 Analytical skills

	2.5 Firewall and security settings are checked and reviewed based on industry standards 2.6 Bandwidth is monitored based on company rules and regulations 2.7 ***Networking monitoring tools*** are utilized based on industry standards 2.8 Syslog servers are collected and analyzed based on industry standards 2.9 Errors, threats and other incidents are documented and reported to authorized personnel	2.6 IP Addressing 2.7 Network Protocols 2.8 Routing and Switching 2.9 Network Services 2.10 Syslogs servers 2.11 Firewall and security settings 2.12 Bandwidth allocation and administration 2.13 Errors and threats in networks	2.6 Learning agility 2.7 Applying security in networks 2.8 Effective communication skills 2.9 Digital forensics

RANGE OF VARIABLES

VARIABLE	RANGE
1. Network devices	May include but not limited to: 1.1 Router 1.2 Switch 1.3 Modem
2. Problems in the network	May include but not limited to: 2.1 Network Congestion 2.2 Packet Loss 2.3 DNS Resolution Failure
3. Network monitoring tools	May include but not limited to: 3.1 Wireshark 3.2 Nagios 3.3 PRTG Network Monitor

EVIDENCE GUIDE

1. Critical aspects of competency	1.1 Configured network 1.2 Troubleshoot and monitored network
2. Resource implications	The following resources should be provided: 2.1 Facilities, equipment, tools, materials and supplies relevant to the unit of competency
3. Methods of assessment	Competency in this unit must be assessed through any or combination of the following: 3.1 Demonstration with questioning 3.2 Written Test 3.3 Oral questioning/interview
4. Context for assessment	4.1 Competency maybe assessed in actual workplace or at the designated TESDA accredited Assessment Center

UNIT OF COMPETENCY: SECURE NETWORK AND APPLICATION

UNIT CODE: CS- ICT251111

UNIT DESCRIPTOR: This unit covers the outcomes required in Utilizing firewall, antivirus, IDS/IPS, SIEM DLP and EDR, Applying Cryptography, Applying encryption/decryption, and Implementing network access control methods

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	Required Knowledge	Required Skills
1. Utilize firewall, antivirus, IDS/IPS, SIEM, DLP and EDR	1.1 Firewall is setup on the network or system based on industry standards 1.2 Antivirus is set up and utilized based on industry standards 1.3 Security information and event management (SIEM) is set up and utilized based on industry standards 1.4 Intrusion detection systems (IDS) and intrusion prevention systems (IPS) is set up and utilized based on industry standards 1.5 Endpoint Detection and Response (EDR) is set up and utilized based on industry standards	1.1 Office productivity tools 1.2 Firewall concepts, set up, utilization and uses 1.3 Antivirus • Overview • installation • Deployment • Updating 1.4 SIEM • Overview • Components • Data source 1.5 IDS and IPS • Overview • Network-based vs host-based • Deployment • Monitoring 1.6 EDR • Overview • Deployment • Monitoring • Detection and analysis • Incident response 1.7 NIST	1.1 Computer operation skills 1.2
2. Apply Cryptography	2.1 Basic concepts of cryptography are applied to secure the systems 2.2 ***Symmetric algorithms*** are utilized to secure the system	1.1 Cryptography 1.2 Symmetric Encryption 1.3 Asymmetric Encryption	1.1 Learning agility 1.2 Effective communication

	based on the company requirements 2.3 ***Cipher modes*** are utilized to secure the system based on the company requirements 2.4 ***Asymmetric algorithms*** are utilized to secure the system based on the company requirements 2.5 ***Hashing algorithms*** are utilized to secure the system based on the company requirements 2.6 ***Key stretching algorithms*** are utilized to secure the system based on the company requirements 2.7 ***Obfuscation*** is utilized to secure the system based on the company requirements	1.4 Hash Functions 1.5 Digital Signatures 1.6 Cryptographic Protocols 1.7 Cryptographic Attacks and Countermeasures 1.8 Cryptographic Best Practices Emerging trends in cryptography 1.9 NIST	1.3 Problem-solving skills 1.4 Strategic planning 1.5 Critical thinking skills 1.6 Computer application skills 1.7 Cryptographic skills 1.8 Analytical skills
3. Apply Encryption/ Decryption	3.1 Sensitive data are identified based on company procedure 3.2 Appropriate ***encryption methods*** are utilized based on job requirements 3.3 ***Encryption software or tools*** are utilized based on job requirements 3.4 Encryption keys are generated 3.5 Encryption is applied on data at rest or on transit 3.6 Keys are managed based on industry standards 3.7 Proper documentation is carried out based on company procedures	3.1 Encryption • Overview • Purpose • Usage 3.2 Encryption methods 3.3 Encryption software/tools 3.4 NIST SP 800-57	3.1 Learning agility 3.2 Effective communication 3.3 Problem-solving skills 3.4 Strategic planning 3.5 Critical thinking skills 3.6 Computer application skills 3.7 Analytical skills 3.8 Generating keys for encryption 3.9 Documentation skills
4. Implement network access control methods	4.1 Access control methods are identified based industry standards 4.2 Access control list is identified and set up based on job requirements 4.3 ***Network access control solutions*** are deployed and utilized based on job requirements	4.1 Access control • Principles • Set up • 4.2 Network access control solutions • Deployment • monitoring 4.3 Multi factor authentication	4.1 Learning agility 4.2 Effective communication 4.3 Problem-solving skills 4.4 Strategic planning 4.5 Critical thinking skills

	4.4 Guest network access is set up based on company requirements 4.5 Multi factor authentication is set up for all network configurations 4.6 ***Authentication protocols*** are set up and utilized based on job requirements	4.4 Authentication protocols • Overview • Types • Setup • Deployment 4.5 NIST 4.6 ISO 27001	4.6 Computer application skills 4.7 Analytical skills 4.8 Generating keys for encryption 4.9 Documentation skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Symmetric algorithms	May include but not limited to: 1.1 AES 1.2 DES 1.3 3DES 1.4 RC4 1.1 Blowfish/Twofish
2. Cipher modes	May include but not limited to: 2.1 CBC 2.2 GCM 2.3 ECB 2.4 CTR 2.5 Stream vs. block
3. Asymmetric algorithms	May include but not limited to: 3.1 RSA 3.2 DSA 3.3 Diffie-Hellman
4. Hashing algorithms	May include but not limited to: 4.1 MD5 4.2 SHA 4.3 HMAC 4.4 RIPEMD
5. Key stretching algorithms	May include but not limited to: 5.1 BCRYPT PBKDF2
6. Obfuscation	May include but not limited to: 6.1 XOR 6.2 ROT13 6.3 Substitution ciphers
7. encryption methods	May include but not limited to: 7.1 AES (Advanced Encryption Standard) 7.2 RSA (Rivest-Shamir-Adleman) 7.3 Blowfish
8. Authentication protocols	May include but not limited to: 8.1 Kerberos 8.2 LDAP (Lightweight Directory Access Protocol) 8.3 SAML (Security Assertion Markup Language)
9. Network access control solutions	May include but not limited to: 9.1 Cisco Identity Services Engine (ISE) 9.2 Aruba ClearPass 9.3 Forescout 9.4 CounterACT
10. Encryption software or tools	May include but not limited to: 10.1 BitLocker 10.2 VeraCrypt 10.3 OpenSSL

11. Network access control solutions	May include but not limited to: 11.1 Cisco Identity Services Engine (ISE) 11.2 SAML (Security Assertion Markup Language)
12. Authentication protocols	May include but not limited to: 12.1 LDAP (Lightweight Directory Access Protocol) 12.2 RADIUS (Remote Authentication Dial-In User Service)

EVIDENCE GUIDE

1. Critical aspects of competency	1.1 Utilized firewall, antivirus, IDS/IPS, SIEM, DLP and EDR 1.2 Applied Cryptography 1.3 Applied Encryption/Decryption 1.4 Implemented network access control methods
2. Resource implications	The following resources should be provided: 2.1 Facilities, equipment, tools, materials and supplies relevant to the unit of competency
3. Methods of assessment	Competency in this unit must be assessed through any or combination of the following: 3.1 Demonstration with questioning 3.2 Written Test 3.3 Oral questioning/interview
4. Context for assessment	4.1 Competency maybe assessed in actual workplace or at the designated TESDA accredited Assessment Center

UNIT OF COMPETENCY: HANDLE CYBERSECURITY INCIDENTS

UNIT CODE: CS- ICT251112

UNIT DESCRIPTOR: This unit covers the outcomes required in detecting and analyzing alerts and incidents and documenting and reporting incident

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	Required Knowledge	Required Skills
1. Detect and analyze alerts and incidents	1.1 ***Security monitoring tools*** are set up and configured 1.2 Alert threshold and rules to trigger alerts are defined 1.3 Alerts are monitored to identify potential security incidents 1.4 Incidents are determined and classified based on severity of impact 1.5 Threat intelligence feeds are utilized 1.6 Alerts are investigated to validate as a real incident 1.7 Incident is escalated to authorized personnel for proper action	1.1 Security monitoring tools • Overview • Installation • usage 1.2 Alerts 1.3 Incidents 1.4 Indicators of compromise	1.1 Learning agility 1.2 Effective communication 1.3 Problem-solving skills 1.4 Strategic planning 1.5 Critical thinking skills 1.6 Computer application skills 1.7 Analytical skills 1.8 Generating keys for encryption 1.9 Documentation skills 1.10 Digital forensics
2. Document and report incident	2.1 Incidents are identified based on job requirements 2.2 Incident are classified based severity of impact 2.3 Incident is documented based on industry standard procedure 2.4 Incident is reported using appropriate ticketing tool/software	2.1 Security monitoring tools • Overview • Installation • usage 2.2 Alerts 2.3 Incidents 2.4 Indicators of compromise	2.1 Learning agility 2.2 Effective communication 2.3 Problem-solving skills 2.4 Strategic planning 2.5 Critical thinking skills 2.6 Computer application skills

			2.7 Analytical skills 2.8 Generating keys for encryption 2.9 Documentation skills 2.10 Digital forensics

RANGE OF VARIABLES

VARIABLE	RANGE
1. Security monitoring tools	May include but not limited to: 1.5 Splunk 1.6 Wireshark 1.7 OSSEC

EVIDENCE GUIDE

1. Critical aspects of competency	1.1 Detected and analyze alerts and incidents 1.2 Documented and report incident
2. Resource implications	The following resources should be provided: 2.1 Facilities, equipment, tools, materials and supplies relevant to the unit of competency
3. Methods of assessment	Competency in this unit must be assessed through any or combination of the following: 3.1 Demonstration with questioning 3.2 Written Test 3.3 Oral questioning/interview
4. Context for assessment	4.1 Competency maybe assessed in actual workplace or at the designated TESDA accredited Assessment Center

GLOSSARY OF TERMS

Access control	Methods and mechanisms to regulate who can access what resources, including user authentication, authorization levels, and permissions.
Alerts	Notifications triggered by security systems indicating potential threats or suspicious activity.
Antivirus	Software specifically designed to detect, prevent, and remove malware from devices.
Asymmetric algorithms	Encryption algorithms that use different keys for encrypting and decrypting data, offering enhanced security than symmetric algorithms.
Attackers	Individuals or groups attempting to gain unauthorized access to systems or information for malicious purposes.
Bandwidth	The amount of data that can be transmitted over a network connection per unit of time, impacting download speeds and potential attack vectors.
Cipher modes	Techniques used to apply encryption algorithms to data, defining how blocks of data are processed and combined.
Cryptography	The science and art of protecting information by transforming it into an unreadable form using encryption algorithms and keys.
Cyber incidents	Events that negatively impact the security of information systems and networks, ranging from data breaches to malware infections.
DNS	Domain Name System, a directory service that translates website names into numerical IP addresses for computers to understand.
Encryption	The process of transforming data into an unreadable form using cryptography, requiring a decryption key to access the original information.
Encryption keys	Strings of data used in conjunction with encryption algorithms to scramble and unscramble information.
Endpoint Detection and Response (EDR)	Security solutions that monitor endpoints (devices) for threats and provide automated or manual response capabilities.
Firewall	Security software or hardware that controls incoming and outgoing network traffic based on predetermined rules, blocking malicious traffic.
Hashing algorithms	One-way mathematical functions that convert data into unique fixed-size strings (hashes), used for verifying data integrity and detecting modifications.
Incident	Any event that might violate security policies or lead to negative consequences, requiring investigation and response.
Key stretching algorithms	Techniques used to increase the complexity and security of encryption keys by applying cryptographic hash functions multiple times.
Malware	Malicious software designed to harm systems or steal data, including viruses, worms, ransomware, and Trojan horses.
MITRE Att&ck Framework	A widely used knowledge base of attacker tactics, techniques, and procedures (TTPs) for understanding and defending against cyber threats.
Multi-factor authentication (MFA)	An authentication method requiring two or more factors to verify a user's identity, enhancing security beyond just passwords.

Network access control solutions	Technologies that enforce network access policies, controlling who and what devices can connect to the network.
Network devices	Physical or virtual hardware components that facilitate network communication, such as routers, switches, and firewalls.
NIST	National Institute of Standards and Technology, a US government agency that develops cybersecurity standards and guidelines.
Obfuscation	Techniques used to make code or data harder to understand and analyze, hindering attackers' efforts to identify vulnerabilities or exploit systems.
Risks	Potential threats that could cause harm to systems or data, requiring assessment and mitigation strategies.
Security information and event management (SIEM)	Systems that collect and analyze security logs from various sources to identify suspicious activity and security incidents.
Subnets	Logical divisions within a network that create smaller segments with separate addressing and security controls.
Symmetric algorithms	Encryption algorithms that use the same key for both encryption and decryption, offering faster processing but potentially less secure than asymmetric algorithms.
Syslog servers	Systems that centralize and store logs generated by devices and applications, providing valuable data for security monitoring and analysis.
Threats	Potential actors or events that could exploit vulnerabilities and cause harm to systems or data.
VLANs	Virtual LANs, logical subdivisions within a physical network that isolate traffic between different groups of devices and users.
Vulnerabilities	Weaknesses in systems, software, or configurations that attackers can exploit to gain unauthorized access.

ACKNOWLEDGEMENTS

The MANAGEMENT and STAFF of the TESDA Secretariat

Qualifications and Standards Office (QSO)
- **Dir. EL CID H. CASTILLO**, Executive Director

Competency Standards Development Division (CSDD)
- **MS. BERNADETTE S. AUDIJE**, Division Chief
- **MR. ADRIAN BRIAN C. SABANAL**, Senior TESD Specialist

A special thanks to CybersCool Defcon Inc for validating this Competency Standards (CS)

www.cyberscooldefcon.com

Competency Standards are available in both printed and 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