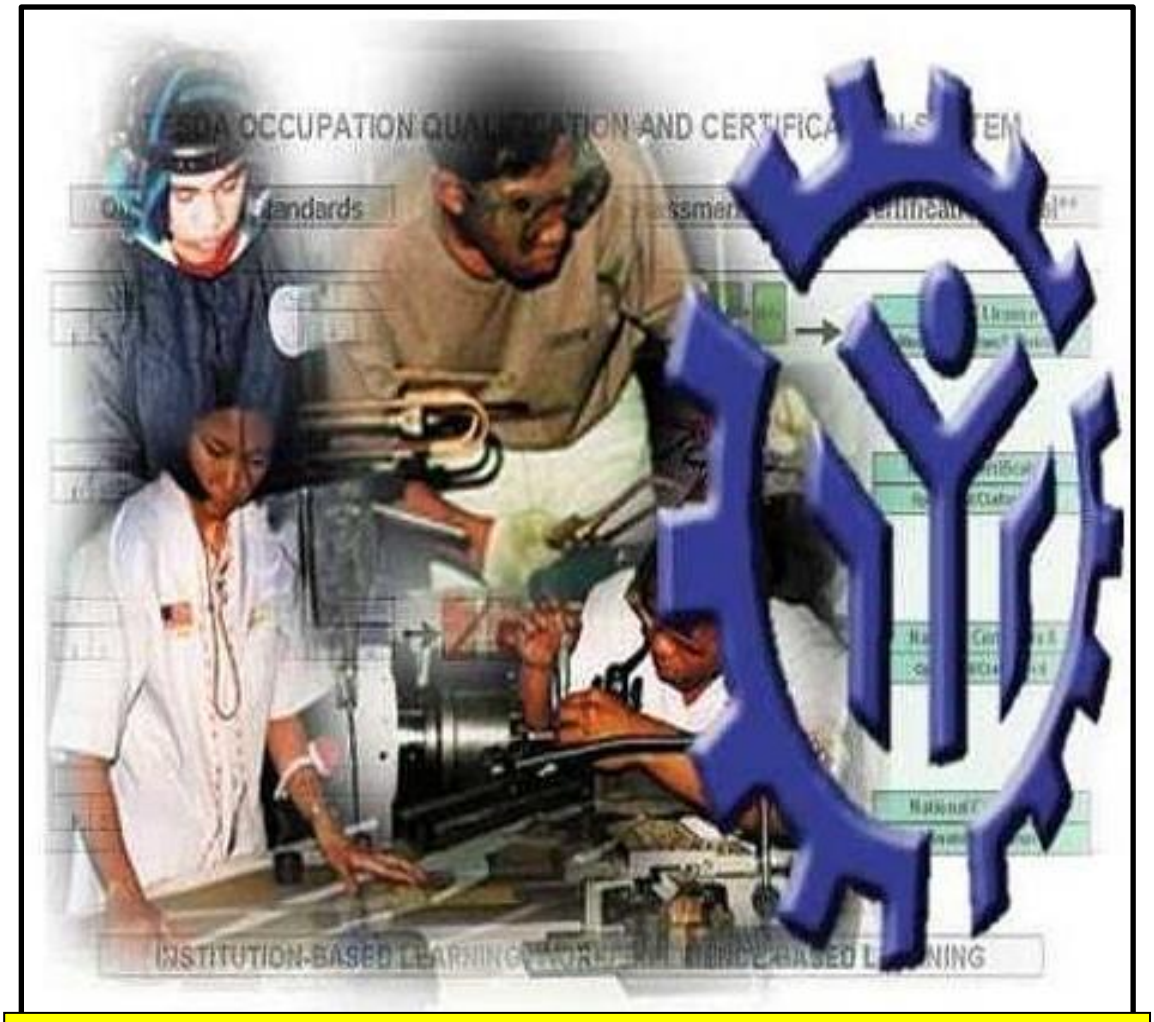
COMPETENCY STANDARDS

CYBER THREAT MITIGATION LEVEL II



INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) SECTOR

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

TABLE OF CONTENTS

ICT SECTOR
CYBER THREAT MITIGATION LEVEL II

COMPETENCY STANDARDS FOR

CYBER THREAT MITIGATION LEVEL II

Section 1 DEFINITION OF QUALIFICATION

The Cyber Threat Mitigation Level II consists of competencies that must be possessed to enable a person to perform threat mitigation and perform vulnerability management/control.

The units of competency comprising this qualification include the following:

Unit Code	BASIC COMPETENCIES
400311210	Participate in workplace communication
400311211	Work in a team environment
400311212	Solve/address general workplace problems
400311213	Develop career and life decisions
400311214	Contribute to workplace innovation
400311215	Present relevant information
400311216	Practice occupational safety and health policies and procedures
400311217	Exercise efficient and effective sustainable practices in the workplace
400311218	Practice entrepreneurial skills in the workplace

Unit Code	COMMON COMPETENCIES
ICT315202	Apply quality standards
ICT311203	Perform computer operations

Unit Code	CORE COMPETENCIES
CS-ICT251203	Perform threat mitigation
CS-ICT251204	Perform vulnerability management/control

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

- Cyber Threat Analyst
- Security Support Specialist
- Cyber Defense Analyst
- IT Security Support (L1)

SECTION 2: COMPETENCY STANDARDS

This section gives the details of the contents of the basic, common, and core units of competency required for Cyber Threat Mitigation Level II**.**

BASIC COMPETENCIES

UNIT OF COMPETENCY : PARTICIPATE IN WORKPLACE COMMUNICATION

UNIT CODE : 400311210

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to gather, interpret and convey information in response to workplace requirements.

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Obtain and convey workplace information	1.1 Specific and relevant information is accessed from ***appropriate sources*** 1.2 Effective questioning , active listening and speaking skills are used to gather and convey information 1.3 Appropriate ***medium*** is used to transfer information and ideas 1.4 Appropriate non- verbal communication is used 1.5 Appropriate lines of communication with supervisors and colleagues are identified and followed 1.6 Defined workplace procedures for the location and ***storage*** of information are used 1.7 Personal interaction is carried out clearly and concisely	1.1 Effective communication 1.2 Different modes of communication 1.3 Medium of communication in the workplace 1.4 Organizational policies 1.5 Communication procedures and systems 1.6 Lines of communication 1.7 Technology relevant to the enterprise and the individual's work responsibilities 1.8 Workplace etiquette	1.1 Following simple spoken language 1.2 Performing routine workplace duties following simple written notices 1.3 Participating in workplace meetings and discussions 1.4 Preparing work- related documents 1.5 Estimating, calculating and recording routine workplace measures 1.6 Relating/ Interacting with people of various levels in the workplace 1.7 Gathering and providing basic information in response to workplace requirements 1.8 Basic business writing skills 1.9 Interpersonal skills in the workplace 1.10 Active-listening skills
2. Perform duties following workplace instructions	2.1 Written notices and instructions are read and interpreted in accordance with organizational guidelines 2.2 Routine written instruction are followed based on established procedures	2.1 Effective verbal and non-verbal communication 2.2 Different modes of communication 2.3 Medium of communication in the workplace	2.1 Following simple spoken instructions 2.2 Performing routine workplace duties following simple written notices 2.3 Participating in workplace meetings and discussions

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	2.3 Feedback is given to workplace supervisor based instructions/ information received 2.4 ***Workplace interactions*** are conducted in a courteous manner 2.5 Where necessary, clarifications about routine workplace procedures and matters concerning conditions of employment are sought and asked from appropriate sources 2.6 Meetings outcomes are interpreted and implemented	2.4 Organizational/ Workplace policies 2.5 Communication procedures and systems 2.6 Lines of communication 2.7 Technology relevant to the enterprise and the individual's work responsibilities 2.8 Effective questioning techniques (clarifying and probing) 2.9 Workplace etiquette	2.4 Completing work-related documents 2.5 Estimating, calculating and recording routine workplace measures 2.6 Relating/ Responding to people of various levels in the workplace 2.7 Gathering and providing information in response to workplace requirements 2.8 Basic questioning/ querying 2.9 Skills in reading for information 2.10 Skills in locating
3. Complete relevant work related documents	3.1 Range of ***forms*** relating to conditions of employment are completed accurately and legibly 3.2 Workplace data is recorded on standard workplace forms and documents 3.3 Errors in recording information on forms/ documents are identified and properly acted upon 3.4 Reporting requirements to supervisor are completed according to organizational guidelines	3.1 Effective verbal and non-verbal communication 3.2 Different modes of communication 3.3 Workplace forms and documents 3.4 Organizational/ Workplace policies 3.5 Communication procedures and systems 3.6 Technology relevant to the enterprise and the individual's work responsibilities	3.1 Completing work-related documents 3.2 Applying operations of addition, subtraction, division and multiplication 3.3 Gathering and providing information in response to workplace requirements 3.4 Effective record keeping skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. Appropriate sources	May include: 1.1. Team members 1.2. Suppliers 1.3. Trade personnel 1.4. Local government 1.5. Industry bodies
2. Medium	May include: 2.1. Memorandum 2.2. Circular 2.3. Notice 2.4. Information discussion 2.5. Follow-up or verbal instructions 2.6. Face to face communication
3. Storage	May include: 3.1. Manual filing system 3.2. Computer-based filing system
4. Workplace interactions	May include: 4.1. Face to face 4.2. Telephone 4.3. Electronic and two way radio 4.4. Written including electronic, memos, instruction and forms, 4.5. Non-verbal including gestures, signals, signs and diagrams
5. Forms	May include: 5.1. HR/Personnel forms, telephone message forms, safety reports

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Prepared written communication following standard format of the organization 1.2. Accessed information using workplace communication equipment/systems 1.3. Made use of relevant terms as an aid to transfer information effectively 1.4. Conveyed information effectively adopting the formal or informal communication
2. Resource Implications	The following resources should be provided: 2.1. Fax machine 2.2. Telephone 2.3. Notebook / Writing materials 2.4. Computer with internet connection
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Demonstration with oral questioning 3.2. Interview 3.3. Written test 3.4. Third-party report
4. Context for Assessment	4.1. Competency may be assessed individually in the actual workplace or through accredited institution

UNIT OF COMPETENCY: WORK IN TEAM ENVIRONMENT

UNIT CODE : 400311211

UNIT DESCRIPTOR : This unit covers the skills, knowledge and attitudes to identify one's roles and responsibilities as a member of a team.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Describe team role and scope	1.1. The ***role and objective of the team*** is identified from available ***sources of information*** 1.2. Team parameters, reporting relationships and responsibilities are identified from team discussions and appropriate external sources	1.1 Group structure 1.2 Group development 1.3 Sources of information	1.1 Communicating with others, appropriately consistent with the culture of the workplace 1.2 Developing ways in improving work structure and performing respective roles in the group or organization
2. Identify one's role and responsibility within team	2.1. Individual role and responsibilities within the team environment are identified 2.2. Roles and objectives of the team is identified from available ***source of information*** 2.3. Team parameters, reporting relationships and responsibilities are identified based on team discussions and appropriate external sources	2.1. Team roles and objectives 2.2. Team structure and parameters 2.3. Team development 2.4. Sources of information	2.1. Communicating with others, appropriately consistent with the culture of the workplace 2.2. Developing ways in improving work structure and performing respective roles in the group or organization
3. Work as a team member	3.1. Effective and appropriate forms of communications are used and interactions undertaken with team members based on company practices 3.2. Effective and appropriate contributions is made to complement team activities and objectives based on ***workplace context*** 3.3. Protocols in reporting are observed based on standard company practices 3.4. Contribute to the development of team work plans based on an understanding of team's role and objectives	3.1. Communication process 3.2. Workplace communication protocol 3.3. Team planning and decision making 3.4. Team thinking 3.5. Team roles 3.6. Process of team development 3.7. Workplace context	3.1. Communicating with others, appropriately consistent with the culture of the workplace 3.2. Interacting effectively with others 3.3. Deciding as an individual and as a group using group think strategies and techniques 3.4. Contributing to Resolution of issues and concerns

RANGE OF VARIABLES

VARIABLE	RANGE
1. Role and objective of team	May include but not limited to: 1.1. Work activities in a team environment with enterprise or specific sector 1.2. Limited discretion, initiative and judgement maybe demonstrated on the job, either individually or in a team environment
2. Sources of information	May include but not limited to: 2.1. Standard operating and/or other workplace procedures 2.2. Job procedures 2.3. Machine/equipment manufacturer's specifications and instructions 2.4. Organizational or external personnel 2.5. Client/supplier instructions 2.6. Quality standards 2.7. OHS and environmental standards
3. Workplace context	May include but not limited to: 3.1. Work procedures and practices 3.2. Conditions of work environments 3.3. Legislation and industrial agreements 3.4. Standard work practice including the storage, safe handling and disposal of chemicals 3.5. Safety, environmental, housekeeping and quality guidelines

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Worked in a team to complete workplace activity 1.2. Worked effectively with others 1.3. Conveyed information in written or oral form 1.4. Selected and used appropriate workplace language 1.5. Followed designated work plan for the job
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 tasks
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1. Role play involving the participation of individual member to the attainment of organizational goal 3.3. Case studies and scenarios as a basis for discussion of issues and strategies in teamwork 3.4 Socio-drama and socio-metric methods 3.5 Sensitivity techniques 3.6 Written Test
4. Context for Assessment	4.1. Competency may be assessed in workplace or in a simulated workplace setting 4.2. Assessment shall be observed while task are being undertaken whether individually or in group

UNIT OF COMPETENCY: SOLVE/ADDRESS GENERAL WORKPLACE PROBLEMS

UNIT CODE : 400311212

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to apply problem-solving techniques to determine the origin of problems and plan for their resolution. It also includes addressing procedural problems through documentation, and referral.

ELEMENT	PERFORMANCE CRITERIA *Italicized* terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify routine problems	1.1 Routine ***problems or procedural problem*** areas are identified 1.2 Problems to be investigated are defined and determined 1.3 Current conditions of the problem are identified and documented	1.1 Current industry hardware and software products and services 1.2 Industry maintenance, service and helpdesk practices, processes and procedures 1.3 Industry standard diagnostic tools 1.4 Malfunctions and resolutions	1.1 Identifying current industry hardware and software products and services 1.2 Identifying current industry maintenance, services and helpdesk practices, processes and procedures. 1.3 Identifying current industry standard diagnostic tools 1.4 Describing common malfunctions and resolutions. 1.5 Determining the root cause of a routine malfunction
2. Look for solutions to routine problems	2.1 Potential solutions to problem are identified 2.2 Recommendations about possible solutions are developed, ***documented***, ranked and presented to ***appropriate person*** for decision	2.1 Current industry hardware and software products and services 2.2 Industry service and helpdesk practices, processes and procedures 2.3 Operating systems 2.4 Industry standard diagnostic tools 2.5 Malfunctions and resolutions. 2.6 Root cause analysis	2.1 Identifying current industry hardware and software products and services 2.2 Identifying services and helpdesk practices, processes and procedures. 2.3 Identifying operating system 2.4 Identifying current industry standard diagnostic tools 2.5 Describing common malfunctions and resolutions. 2.6 Determining the root cause of a routine malfunction

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Recommend solutions to problems	3.1 Implementation of solutions are ***planned*** 3.2 Evaluation of implemented solutions are planned 3.3 Recommended solutions are documented and submit to appropriate person for confirmation	3.1 Standard procedures 3.2 Documentation produce	3.1 Producing documentation that recommends solutions to problems 3.2 Following established procedures

RANGE OF VARIABLES

VARIABLE	RANGE
1. Problems/Procedural Problem	May include but not limited to: 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 1.5 Work-related problems outside of own work area
2. Appropriate person	May include but not limited to: 2.1 Supervisor or manager 2.2 Peers/work colleagues 2.3 Other members of the organization
3. Document	May include but not limited to: 3.1 Electronic mail 3.2 Briefing notes 3.3 Written report 3.4 Evaluation report
4. Plan	May include but not limited to: 4.1 Priority requirements 4.2 Co-ordination and feedback requirements 4.3 Safety requirements 4.4 Risk assessment 4.5 Environmental requirements

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Determined the root cause of a routine problem 1.2. Identified solutions to procedural problems. 1.3. Produced documentation that recommends solutions to problems. 1.4. Followed established procedures. 1.5. Referred unresolved problems to support persons.
2. Resource Implications	2.1. 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 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.
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 : DEVELOP CAREER AND LIFE DECISIONS

UNIT CODE : 400311213

UNIT DESCRIPTOR : This unit covers the knowledge, skills, and attitudes in managing one's emotions, developing reflective practice, and boosting self-confidence and developing self-regulation.

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Manage one's emotion	1.1. ***Self-management strategies*** are identified 1.2. Skills to work independently and to show initiative, to be conscientious, and persevering in the face of setbacks and frustrations are developed 1.3. Techniques for effectively handling negative emotions and **unpleasant situation i**n the workplace are examined	1.1 Self-management strategies that assist in regulating behavior and achieving personal and learning goals (e.g. Nine self-management strategies according to Robert Kelley) 1.2 Enablers and barriers in achieving personal and career goals 1.3 Techniques in handling negative emotions and unpleasant situation in the workplace such as frustration, anger, worry, anxiety, etc.	1.1 Managing properly one's emotions and recognizing situations that cannot be changed and accept them and remain professional 1.2 Developing self-discipline, working independently and showing initiative to achieve personal and career goals 1.3 Showing confidence, and resilience in the face of setbacks and frustrations and other negative emotions and unpleasant situations in the workplace
2. Develop reflective practice	2.1. Personal strengths and achievements, based on self-assessment strategies and teacher feedback are contemplated 2.2. Progress when seeking and responding to feedback from teachers to assist them in consolidating strengths, addressing weaknesses and fulfilling their potential are monitored 2.3. Outcomes of personal and academic challenges by reflecting on previous problem solving and decision making strategies and feedback	2.1 Basic SWOT analysis 2.2 Strategies to improve one's attitude in the workplace 2.3 Gibbs' Reflective Cycle/Model (Description, Feelings, Evaluation, Analysis, Conclusion, and Action plan)	2.1 Using the basic SWOT analysis as self-assessment strategy 2.2 Developing reflective practice through realization of limitations, likes/ dislikes; through showing of self-confidence 2.3 Demonstrating self-acceptance and being able to accept challenges

ELEMENT	PERFORMANCE CRITERIA ***Italicized*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	from peers and teachers are predicted		
3. Boost self-confidence and develop self-regulation	3.1. Efforts for continuous self-improvement are demonstrated 3.2. Counter-productive tendencies at work are eliminated 3.3. Positive outlook in life are maintained.	3.1 Four components of self-regulation based on Self-Regulation Theory (SRT) 3.2 Personality development concepts 3.3 Self-help concepts (e. g., 7 Habits by Stephen Covey, transactional analysis, psycho-spiritual concepts)	3.1 Performing effective communication skills – reading, writing, conversing skills 3.2 Showing affective skills – flexibility, adaptability, etc. 3.3 Self-assessment for determining one's strengths and weaknesses

RANGE OF VARIABLES

VARIABLE	RANGE
1. Self-management strategies	May include but not limited to: 1.1 Seeking assistance in the form of job coaching or mentoring 1.2 Continuing dialogue to tackle workplace grievances 1.3 Collective negotiation/bargaining for better working conditions 1.4 Share your goals to improve with a trusted co-worker or supervisor 1.5 Make a negativity log of every instance when you catch yourself complaining to others 1.6 Make lists and schedules for necessary activities
2. Unpleasant situation	May include but not limited to: 2.1 Job burn-out 2.2 Drug dependence 2.3 Sulking

EVIDENCE GUIDE

1 Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Express emotions appropriately 1.2 Work independently and show initiative 1.3 Consistently demonstrate self-confidence and self-discipline
2 Resource Implications	The following resources should be provided: 2.1 Access to workplace and resource s 2.2 Case studies
3 Methods of Assessment	Competency in this unit may be assessed through: 3.1 Demonstration or simulation with oral questioning 3.2 Case problems involving work improvement and sustainability 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 : **CONTRIBUTE TO WORKPLACE INNOVATION**

UNIT CODE : **400311214**

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to make a pro-active and positive contribution to workplace innovation.

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify opportunities to do things better.	1.1 ***Opportunities for improvement*** are identified proactively in own area of work. 1.2 ***Information*** are gathered and reviewed which may be relevant to ideas and which might assist in gaining support for idea.	1.1 Roles of individuals in suggesting and making improvements. 1.2 Positive impacts and challenges in innovation. 1.3 Types of changes and responsibility. 1.4 Seven habits of highly effective people.	1.1 Identifying opportunities to improve and to do things better. Involvement. 1.2 Identifying the positive impacts and the challenges of change and innovation. 1.3 Identifying examples of the types of changes that are within and outside own scope of responsibility
2. Discuss and develop ideas with others	2.1 ***People who could provide input*** to ideas for improvements are identified. 2.2 Ways of approaching people to begin sharing ideas are selected. 2.3 Meeting is set with relevant people. 2.4 Ideas for follow up are review and selected based on feedback. 2.5 ***Critical inquiry method*** is used to discuss and develop ideas with others.	2.1 Roles of individuals in suggesting and making improvements. 2.2 Positive impacts and challenges in innovation. 2.3 Types of changes and responsibility. 2.4 Seven habits of highly effective people.	2.1 Identifying opportunities to improve and to do things better. Involvement. 2.2 Identifying the positive impacts and the challenges of change and innovation. 2.3 Providing examples of the types of changes that are within and outside own scope of responsibility 2.4 Communicating ideas for change through small group discussions and meetings.
3. Integrate ideas for change in the workplace.	3.1 Critical inquiry method is used to integrate different ideas for change of key people. 3.2 Summarizing, analyzing and generalizing skills are used to extract salient points in the pool of ideas. 3.3 ***Reporting skills*** are likewise used to communicate results. 3.4 ***Current Issues and concerns*** on the	3.1 Roles of individuals in suggesting and making improvements. 3.2 Positive impacts and challenges in innovation. 3.3 Types of changes and responsibility. 3.4 Seven habits of highly effective people.	3.1 Identifying opportunities to improve and to do things better. Involvement. 3.2 Identifying the positive impacts and the challenges of change and innovation. 3.3 Providing examples of the types of changes that are within and

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	systems, processes and procedures, as well as the need for simple innovative practices are identified.	3.5 Basic research skills.	outside own scope of responsibility. 3.4 Communicating ideas for change through small group discussions and meetings. 3.5 Demonstrating skills in analysis and interpretation of data.

RANGE OF VARIABLES

VARIABLES	RANGE
1. Opportunities for improvement	May include: 1.1 Systems. 1.2 Processes. 1.3 Procedures. 1.4 Protocols. 1.5 Codes. 1.6 Practices.
2. Information	May include: 2.1 Workplace communication problems. 2.2 Performance evaluation results. 2.3 Team dynamics issues and concerns. 2.4 Challenges on return of investment 2.5 New tools, processes and procedures. 2.6 New people in the organization.
3. People who could provide input	May include: 3.1 Leaders 3.2 Managers 3.3 Specialists 3.4 Associates 3.5 Researchers 3.6 Supervisors 3.7 Staff 3.8 Consultants (external) 3.9 People outside the organization in the same field or similar expertise/industry. 3.10 Clients
4. Critical inquiry method	May include: 4.1 Preparation. 4.2 Discussion. 4.3 Clarification of goals. 4.4 Negotiate towards a Win-Win outcome. 4.5 Agreement. 4.6 Implementation of a course of action. 4.7 Effective verbal communication. See pages: Verbal Communication and Effective Speaking. 4.8 Listening. 4.9 Reducing misunderstandings is a key part of effective negotiation. 4.10 Rapport Building. 4.11 Problem Solving. 4.12 Decision Making. 4.13 Assertiveness. 4.14 Dealing with Difficult Situations.
5. Reporting skills	May include: 5.1 Data management. 5.2 Coding. 5.3 Data analysis and interpretation. 5.4 Coherent writing. 5.5 Speaking.

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Identified opportunities to do things better. 1.2 Discussed and developed ideas with others on how to contribute to workplace innovation. 1.3 Integrated ideas for change in the workplace. 1.4 Analyzed and reported rooms for innovation and learning in the workplace.
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	4.1 Competency may be assessed individually in the actual workplace or simulation environment in TESDA accredited institutions.

UNIT OF COMPETENCY : PRESENT RELEVANT INFORMATION

UNIT CODE : 400311215

UNIT DESCRIPTOR : This unit of covers the knowledge, skills and attitudes required to present data/information appropriately.

ELEMENTS	PERFORMANCE CRITERIA *Italicized terms* are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Gather data/ information	1.1 Evidence, facts and information are collected 1.2 Evaluation, terms of reference and conditions are reviewed to determine whether data/information falls within project scope	1.1 Organisational protocols 1.2 Confidentiality 1.3 Accuracy 1.4 Business mathematics and statistics 1.5 Data analysis techniques/procedures 1.6 Reporting requirements to a range of audiences 1.7 Legislation, policy and procedures relating to the conduct of evaluations 1.8 Organisational values, ethics and codes of conduct	1.1 Describing organisational protocols relating to client liaison 1.2 Protecting confidentiality 1.3 Describing accuracy 1.4 Computing business mathematics and statistics 1.5 Describing data analysis techniques/ procedures 1.6 Reporting requirements to a range of audiences 1.7 Stating legislation, policy and procedures relating to the conduct of evaluations 1.8 Stating organisational values, ethics and codes of conduct
2. Assess gathered data/ information	2.1 Validity of data/ information is assessed 2.2 Analysis techniques are applied to assess data/ information. 2.3 Trends and anomalies are identified 2.4 ***Data analysis techniques*** and procedures are documented 2.5 Recommendations are made on areas of possible improvement.	2.1 Business mathematics and statistics 2.2 Data analysis techniques/ procedures 2.3 Reporting requirements to a range of audiences 2.4 Legislation, policy and procedures relating to the conduct of evaluations 2.5 Organisational values, ethics and codes of conduct	2.1 Computing business mathematics and statistics 2.2 Describing data analysis techniques/ procedures 2.3 Reporting requirements to a range of audiences 2.4 Stating legislation, policy and procedures relating to the conduct of evaluations 2.5 Stating organisational values, ethics and codes of conduct

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Record and present information	3.1 Studied data/information are recorded. 3.2 Recommendations are analysed for action to ensure they are compatible with the project's scope and terms of reference. 3.3 Interim and final reports are analysed and outcomes are compared to the criteria established at the outset. 3.4 Findings are presented to stakeholders.	3.1 Data analysis techniques/ procedures 3.2 Reporting requirements to a range of audiences 3.3 Legislation, policy and procedures relating to the conduct of evaluations 3.4 Organisational values, ethics and codes of conduct	3.1 Describing data analysis techniques/ procedures 3.2 Reporting requirements to a range of audiences 3.3 Stating legislation, policy and procedures relating to the conduct of evaluations 3.4 Stating organisational values, ethics and codes of conduct practices

RANGE OF VARIABLES

VARIABLES	RANGE
1. Data analysis techniques	May include but not limited to: 1.1. Domain analysis 1.2. Content analysis 1.3. Comparison technique

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Determine data / information 1.2 Studied and applied gathered data/information 1.3 Recorded and studied studied data/information These aspects may be best assessed using a range of scenarios what ifs as a stimulus with a walk through forming part of the response. These assessment activities should include a range of problems, including new, unusual and improbable situations that may have happened.
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 : PRACTICE OCCUPATIONAL SAFETY AND HEALTH POLICIES AND PROCEDURES

UNIT CODE : 400311216

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitudes required to identify OSH compliance requirements, prepare OSH requirements for compliance, and perform tasks in accordance with relevant OSH policies and procedures

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify OSH compliance requirements	1.1. Relevant ***OSH requirements, regulations, policies and procedures*** are identified in accordance with workplace policies and procedures 1.2. OSH activity non-conformities are conveyed to ***appropriate personnel*** 1.3. ***OSH preventive and control requirements*** are identified in accordance with OSH work policies and procedures	1.1. OSH preventive and control requirements 1.2. Hierarchy of Controls 1.3. Hazard Prevention and Control 1.4. General OSH principles 1.5. Work standards and procedures 1.6. Safe handling procedures of tools, equipment and materials 1.7. Standard emergency plan and procedures in the workplace	1.1. Communication skills 1.2. Interpersonal skills 1.3. Critical thinking skills 1.4. Observation skills
2. Prepare OSH requirements for compliance	2.1. OSH work activity material, tools and equipment requirements are identified in accordance with workplace policies and procedures 2.2. Required OSH materials, tools and equipment are acquired in accordance with workplace policies and procedures 2.3. Required OSH materials, tools and equipment are arranged/ placed in accordance with OSH work standards	2.1. Resources necessary to execute hierarchy of controls 2.2. General OSH principles 2.3. Work standards and procedures 2.4. Safe handling procedures of tools, equipment and materials 2.5. Different OSH control measures	2.1. Communication skills 2.2. Estimation skills 2.3. Interpersonal skills 2.4. Critical thinking skills 2.5. Observation skills 2.6. Material, tool and equipment identification skills
3. Perform tasks in accordance with relevant OSH policies and procedures	3.1. Relevant OSH work procedures are identified in accordance with workplace policies and procedures 3.2. Work Activities are executed in accordance with OSH work standards 3.3. ***Non-compliance work activities*** are reported to appropriate personnel	3.1. OSH work standards 3.2. Industry related work activities 3.3. General OSH principles 3.4. OSH Violations 3.5. Non-compliance work activities	3.1. Communication skills 3.2. Interpersonal skills 3.3. Troubleshooting skills 3.4. Critical thinking skills 3.5. Observation skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. OSH Requirements, Regulations, Policies and Procedures	May include: 1.1 Clean Air Act 1.2 Building code 1.3 National Electrical and Fire Safety Codes 1.4 Waste management statutes and rules 1.5 Permit to Operate 1.6 Philippine Occupational Safety and Health Standards 1.7 Department Order No. 13 (Construction Safety and Health) 1.8 ECC regulations
2. Appropriate Personnel	May include: 2.1 Manager 2.2 Safety Officer 2.3 EHS Offices 2.4 Supervisors 2.5 Team Leaders 2.6 Administrators 2.7 Stakeholders 2.8 Government Official 2.9 Key Personnel 2.10 Specialists 2.11 Himself
3. OSH Preventive and Control Requirements	May include: 3.1 Resources needed for removing hazard effectively 3.2 Resources needed for substitution or replacement 3.3 Resources needed to establishing engineering controls 3.4 Resources needed for enforcing administrative controls 3.5 Personal Protective equipment
4. Non OSH-Compliance Work Activities	May include non-compliance or observance of the following safety measures: 4.1 Violations that may lead to serious physical harm or death 4.2 Fall Protection 4.3 Hazard Communication 4.4 Respiratory Protection 4.5 Power Industrial Trucks 4.6 Lockout/Tag-out 4.7 Working at heights (use of ladder, scaffolding) 4.8 Electrical Wiring Methods 4.9 Machine Guarding 4.10 Electrical General Requirements 4.11 Asbestos work requirements 4.12 Excavations work requirements

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Convey OSH work non-conformities to appropriate personnel 1.2. Identify OSH preventive and control requirements in accordance with OSH work policies and procedures 1.3. Identify OSH work activity material, tools and equipment requirements in accordance with workplace policies and procedures 1.4. Arrange/Place required OSH materials, tools and equipment in accordance with OSH work standards 1.5. Execute work activities in accordance with OSH work standards 1.6. Report OSH activity non-compliance work activities to appropriate personnel
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. 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 : EXERCISE EFFICIENT AND EFFECTIVE SUSTAINABLE PRACTICES IN THE WORKPLACE

UNIT CODE : 400311217

UNIT DESCRIPTOR : This unit covers knowledge, skills and attitude to identify the efficiency and effectiveness of resource utilization, determine causes of inefficiency and/or ineffectiveness of resource utilization and Convey inefficient and ineffective environmental practices

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Identify the efficiency and effectiveness of resource utilization	1.1. Required resource utilization in the workplace is measured using appropriate techniques 1.2. Data are recorded in accordance with workplace protocol 1.3. Recorded data are compared to determine the efficiency and effectiveness of resource utilization according to established ***environmental work procedures***	1.1. Importance of Environmental Literacy 1.2. Environmental Work Procedures 1.3. Waste Minimization 1.4. Efficient Energy Consumptions	1.1 Recording Skills 1.2 Writing Skills 1.3 Innovation Skills
2. Determine causes of inefficiency and/or ineffectiveness of resource utilization	2.1. Potential causes of inefficiency and/or ineffectiveness are listed 2.2. Causes of inefficiency and/or ineffectiveness are identified through deductive reasoning 2.3. Identified causes of inefficiency and/or ineffectiveness are validated thru established environmental procedures	2.1. Causes of environmental inefficiencies and ineffectiveness	2.1. Deductive Reasoning Skills 2.2. Critical thinking 2.3. Problem Solving 2.4. Observation Skills
3. Convey inefficient and ineffective environmental practices	3.1. Efficiency and effectiveness of resource utilization are reported to ***appropriate personnel*** 3.2. Concerns related resource utilization are discussed with appropriate personnel 3.3. Feedback on information/ concerns raised are clarified with appropriate personnel	3.1. Appropriate Personnel to address the environmental hazards 3.2. Environmental corrective actions	3.1. Written and Oral Communication Skills 3.2. Critical thinking 3.3. Problem Solving 3.4. Observation Skills 3.5. Practice Environmental Awareness

RANGE OF VARIABLES

VARIABLE	RANGE	
1. Environmental Work Procedures	May include: 1.1. Utilization of Energy, Water, Fuel Procedures 1.2. Waster Segregation Procedures 1.3. Waste Disposal and Reuse Procedures 1.4. Waste Collection Procedures 1.5. Usage of Hazardous Materials Procedures 1.6. Chemical Application Procedures 1.7. Labeling Procedures	
2. Appropriate Personnel	May include: 2.1. Manager 2.2. Safety Officer 2.3. EHS Offices 2.4. Supervisors 2.5. Team Leaders	2.6. Administrators 2.7. Stakeholders 2.8. Government Official 2.9. Key Personnel 2.10. Specialists 2.11. Himself

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1. Measured required resource utilization in the workplace using appropriate techniques 1.2. Recorded data in accordance with workplace protocol 1.3. Identified causes of inefficiency and/or ineffectiveness through deductive reasoning 1.4. Validate the identified causes of inefficiency and/or ineffectiveness thru established environmental procedures 1.5. Report efficiency and effectives of resource utilization to appropriate personnel 1.6. Clarify feedback on information/concerns raised with appropriate personnel
2. Resource Implications	The following resources should be provided: 2.1 Workplace 2.2 Tools, materials and equipment relevant to the tasks 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 : PRACTICE ENTREPRENEURIAL SKILLS IN THE WORKPLACE

UNIT CODE : 400311218

UNIT DESCRIPTOR : This unit covers the outcomes required to apply entrepreneurial workplace best practices and implement cost-effective operations

ELEMENTS	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Apply entrepreneurial workplace best practices	1.1. ***Good practices*** relating to workplace operations are observed and selected following workplace policy. 1.2. Quality procedures and practices are complied with according to workplace requirements. 1.3. Cost-conscious habits in ***resource utilization*** are applied based on industry standards.	1.1. Workplace best practices, policies and criteria 1.2. Resource utilization 1.3. Ways in fostering entrepreneurial attitudes: 1.3.1. Patience 1.3.2. Honesty 1.3.3. Quality-consciousness 1.3.4. Safety-consciousness 1.3.5. Resourcefulness	1.1. Communication skills 1.2. Complying with quality procedures
2. Communicate entrepreneurial workplace best practices	1.3. Observed good practices relating to workplace operations are communicated to **appropriate person**. 1.4. Observed quality procedures and practices are communicated to appropriate person 1.5. Cost-conscious habits in resource utilization are communicated based on industry standards.	2.1. Workplace best practices, policies and criteria 2.2. Resource utilization 2.3. Ways in fostering entrepreneurial attitudes: 2.3.1. Patience 2.3.2. Honesty 2.3.3. Quality-consciousness 2.3.4. Safety-consciousness 2.3.5. Resourcefulness	2.1. Communication skills 2.2. Complying with quality procedures 2.3. Following workplace communication protocol
3. Implement cost-effective operations	2.4. Preservation and optimization of workplace resources is implemented in accordance with enterprise policy 2.5. Judicious use of workplace tools, equipment and materials are observed according to manual and work requirements. 2.6. Constructive contributions to office operations are made according to enterprise requirements. 2.7. Ability to work within one's allotted time and finances is sustained.	3.1. Optimization of workplace resources 3.2. 5S procedures and concepts 3.3. Criteria for cost-effectiveness 3.4. Workplace productivity 3.5. Impact of entrepreneurial mindset to workplace productivity 3.6. Ways in fostering entrepreneurial attitudes: 3.6.1. Quality-consciousness 3.6.2. Safety-consciousness	3.1. Implementing preservation and optimizing workplace resources 3.2. Observing judicious use of workplace tools, equipment and materials 3.3. Making constructive contributions to office operations 3.4. Sustaining ability to work within allotted time and finances

RANGE OF VARIABLES

VARIABLE	RANGE
1. Good practices	May include: 1.1 Economy in use of resources 1.2 Documentation of quality practices
2. Resources utilization	May include: 2.1 Consumption/ use of consumables 2.2 Use/Maintenance of assigned equipment and furniture 2.3 Optimum use of allotted /available time

EVIDENCE GUIDE

1. Critical aspects of competency	Assessment requires evidence that the candidate: 1.1. Demonstrated ability to identify and sustain cost-effective activities in the workplace 1.2. Demonstrated ability to practice entrepreneurial knowledge, skills and attitudes in the workplace.
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 2.3.1 Enterprise procedures manuals 2.3.2 Company quality policy
3. Methods of Assessment	Competency in this unit should be assessed through: 3.1. Interview 3.2. Third-party report
4. Context for 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 : ELC315202

UNIT DESCRIPTOR : This unit covers the knowledge, skills, (and) 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 Bold*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Assess quality of received materials or components	1.1. Work instructions are obtained and work is carried out in accordance with standard operating procedures 1.2. Received ***materials or component parts*** are checked against workplace standards and specifications 1.3. Faulty material or components 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 or components 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 is recorded in accordance with workplace procedures 2.5. In cases of deviations from specified ***quality standards***, causes are documented and reported in accordance with	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 Bold*** terms are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	the workplace' standards operating procedures		
3. Engage in quality improvement	3.1. Process improvement procedures are participated in relation to workplace assignment 3.2. Work is carried out in accordance with process improvement procedures 3.3. Performance of operation or quality of product or 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	Materials may include but not limited to: 1.1. Manuals 1.2. Job orders 1.3. Instructional videos
2. Faults	Faults may include but not limited to: 2.1. Materials not to specification 2.2. Materials contain incorrect/outdated information 2.3. Hardware defects 2.4. Materials that do not conform with any regulatory agencies
3. Documentation	Documentation may include: 3.1. Organization work procedures 3.2. Manufacturer's instruction manual 3.3. Customer requirements 3.4. Forms
4. Errors	Errors may be related but not limited to the following: 4.1. Deviation from the requirements of the Client 4.2. Deviation from the requirement of the organization
5. Quality standards	Quality standards may be related but not limited to the following: 5.1. Materials 5.2. Hardware 5.3. Final product 5.4. Production processes 5.5. Customer service
6. Customer	Customer may include: 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 must show that the 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	The following resources should be provided: 3.1. Materials and component parts and equipment to be used in a real or simulated electronic production situation
4. Context for Assessment	4.1. Assessment may be conducted in the workplace or in a simulated environment.

UNIT TITLE : PERFORM COMPUTER OPERATIONS

UNIT CODE : ELC311203

UNIT DESCRIPTOR : This unit covers the knowledge, skills, (and) attitudes and values needed to perform computer operations that 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	May include: 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	May include: 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 4.5. cloud storage
5. Ergonomic guidelines	May include: 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	May include: 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	The assessor may select two of the following assessment methods to objectively assess the candidate: 2.1. Observation 2.2. Questioning 2.3. Practical demonstration
3. Resource implication	The following resources should be provided: 3.1. Computer hardware with peripherals 3.2. Appropriate software
4. Context for Assessment	4.1. Assessment may be conducted in the workplace or in a simulated work environment

CORE COMPETENCIES

UNIT OF COMPETENCY: PERFORM THREAT MITIGATION

UNIT CODE : CS-ICT251203

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitude required to perform threat mitigation. This includes competencies in evaluating incidents; using threat intelligence; analyzing running processes and configurations on affected systems; carrying out in-depth threat intelligence analysis; and creating and implementing strategy for containment and recovery.

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Evaluate incidents	1.1. Alerts are validated based on the report. 1.2. Product detection is performed based on the 8-point incidence response. 1.3. Incident classification is identified based on ***environment***. 1.4. Incident criticality is prioritized according to impact on the asset.	1.1. Knowledge in Incident Response 1.2. Basic knowledge with Windows, MAC & Linux OS 1.3. Basic knowledge with Web server and website design and architecture 1.4. Basic knowledge with any scripting and coding language, i.e. PHP, Python, Java, Visual Basic and others 1.5. Basic knowledge with network infrastructure and architecture, i.e. LAN, WAN, port forwarding 1.6. Basic knowledge on detection and alerting (log management) 1.7. Basic knowledge in operating security solution (i.e. scanning and operations procedure) 1.8. Security solution severity classifications 1.9. Malicious software behaviors	1.1. Incident response Skills 1.2. Determining the priority, scope and root cause of the incident 1.3. Computer operation skills 1.4. Communication skills 1.5. Interpreting work instructions 1.6. Interpersonal skills 1.7. Data analysis skills
2. Use cyber threat intelligence	2.1. Received threat intelligence is utilized to identify tactics, techniques and procedures (TTP) of threat actors (hackers).	2.1. Basic Cyber Threat Intelligence knowledge 2.1.1. Threat intelligence source 2.1.2. IOCs 2.1.3. NIST 800-150 2.1.4. NIST 800-172	2.1. Cyber Threat Intelligence (CTI) Skills 2.2. Using various threat intelligence platforms

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	[*NIST SP 800-150 & 800-172*] 2.2. ***Indicator of compromise (IOCs)*** is counter-checked with other sources 2.3. ***Applicability of IOC*** is checked versus available infrastructure 2.4. Preventive action/resolution is applied by blocking identified IOCs on available security technology appliances 2.5. Continuous monitoring is conducted to detect attempts of download, access and interaction with the malicious IOCs 2.6. Current threat intelligence and threat mitigation activities are defined and added to knowledge-based systems.	2.2. Basic knowledge on : 1.1.1. Cyber Kill Chain, 1.1.2. MITRE ATT&CK Framework, 1.1.3. Diamond Model, and 1.1.4. Pyramid of Pain for CTI 2.3. Knowledge in Incident Response 2.4. Basic knowledge with Windows, MAC & Linux OS 2.5. Basic knowledge with Web server and website design and architecture 2.6. Basic knowledge with any scripting and coding language, i.e. PHP, Python, Java, Visual Basic and others 2.7. Basic knowledge with network infrastructure and architecture, i.e. LAN, WAN, port forwarding 2.8. Basic knowledge on detection and alerting (log management) 2.9. Basic knowledge in operating security solution (i.e. scanning and operations procedure) 2.10. Security solution severity classifications 2.11. Malicious software behaviors	2.3. Able to analyze and provide Context for intel reports to their organization 2.4. CTI analysis skills 2.5. Leveraging/ Utilizing IOCs to improve security controls detections and mitigations 2.6. Providing CTI reports 2.7. Can Articulate the Cyber Kill Chain, MITRE ATT&CK Framework, Diamond Model, and Pyramid of Pain for CTI 2.8. Computer operation skills 2.9. Communication skills 2.10. Interpreting work instructions 2.11. Interpersonal skills 2.12. Data analysis skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Analyze running processes and configs on affected systems	3.1. ***Common security tools*** and ***security products*** available are utilized, when necessary 3.2. Known and ***common folder or location*** is checked for possible installed malicious files. [ref.: attack.mitre.org] 3.3. File integrity is verified and monitored by tools and security products based on original installation package or digitally signed files from vendors-white listing 3.4. Tools and security product are used to confirm detection of malicious activity, files, folder and packets	3.1. Systems operations 3.1.1. Linux, i.e. ProcMon-for-Linux 3.1.2. Windows, i.e. MS Sysinternals 3.2. Common security tools and security products 3.2.1. EDR 3.2.2. MDR 3.2.3. XDR 3.2.4. UEBA 3.3. Security solution usage and operations 3.4. File level analysis	3.1. Operating systems operation 3.2. Computer operation skills 3.3. Communication skills 3.4. Interpreting work instructions 3.5. Interpersonal skills 3.6. Monitoring skills 3.7. Data analysis skills
4. Create and implement strategy for containment and recovery	4.1. TTP and IOCs are identified based on the detection and recommendation of the security products 4.2. IOCs are blocked and contained using the features of EDR, NGAV and next generation firewall (NGFW) 4.3. Continuous monitoring is conducted to detect attempts of download, access and interaction with the malicious IOCs 4.4. Current threat mitigation activities are defined and added to knowledge-based systems. 4.5. System or infra recovery is conducted by checking the last known good or viable image, configuration or instance of backup. 4.6. Rollback activity is conducted based on the availability of last known good image, configuration and instance	4.1. Knowledge in NIST 800-61- Containment and Recovery phase 4.2. Incident management particular to 4.2.1. Response 4.2.2. Mitigation 4.2.3. Reporting 4.2.4. Containment 4.2.5. Recovery 4.3. Use of EDR, NGAV and NGFW 4.4. Malicious IOCs 4.5. Familiarity in the use of security products on blocking: 4.5.1. IP 4.5.2. Port 4.5.3. URL 4.5.4. Hash 4.5.5. packet 4.5.6. files 4.5.7. script 4.6. Familiarity in the use of security product on containing: 4.6.1. network segment 4.6.2. cloud instance 4.6.3. endpoint 4.6.4. mobile device	4.1. Computer operation skills 4.2. Communication skills 4.3. Interpreting work instructions 4.4. Interpersonal skills 4.5. Data analysis skills 4.6. Incident Response Skills 4.7. Can leverage EDR, NGAV and NGFW (if available) for incident response 4.8. Documentation skills 4.9. Operating systems operation 4.10. stakeholder management skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	4.7. Removal of malicious IOCs, registry hives, files, folders is conducted using security products 4.8. Secondary scan is conducted using the security products to determine if there are still malicious elements in the enterprise and mobile environment 4.9. Documentation and reporting is conducted based on the activity of mitigation, containment and recovery	4.6.5. servers 4.6.6. virtual machines 4.6.7. containers 4.6.8. network storage 4.7. Use of backup management software (i.e Windows and Linux) 4.8. Systems operations 4.8.1. Linux, i.e. ProcMon-for-Linux 4.8.2. Windows, i.e. MS Sysinternals 4.9. Knowledge on log management to collect and document vital information regarding the threat vector, infection spread, containment strategy and recovery of the asset 4.10. Alert reporting	

RANGE OF VARIABLES

VARIABLE	RANGE
1. Environment	May include: 1.1. Cloud 1.2. Mobile 1.3. Network
2. Indicator of compromise (IOCs)	May include: 2.1. Hash 2.2. IP 2.3. URL 2.4. Packets 2.5. Behavior analysis
3. Applicability of IOC	Example of applicability of IOC maybe a banking threats doesn't apply to industrial infrastructure or facilities, e.g. Windows threat doesn't affect Linux or Unix native environment)
4. Common security tools	May include: 4.1. Mitre indicator 4.1.1. Windows, i.e. Sysinternals 4.1.2. Linux, i.e HTOP 4.1.3. MacOS, i.e DTrace Toolkit
5. Security products	May include: 5.1. Endpoint detection and response (EDR) 5.2. Next generation anti-virus (NGAV)
6. Common folder or location	Coverage may include: 6.1. Enterprise 6.1.1. Windows 6.1.2. Linux and 6.1.3. Mac OS 6.2. Mobile 6.2.1. Android 6.2.2. iOS

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Evaluated incidents 1.1.1 Validated alerts based on the report. 1.1.2 Performed product detection based on the 8-point incidence response. 1.1.3 Identified incident classification based on environment. 1.1.4 Prioritized incident criticality according to impact on the asset. 1.2 Used threat intelligence 1.2.1 Utilized received threat intelligence to identify tactics, techniques and procedures (TTP) of threat actors (hackers). 1.2.2 Counter-checked indicator of compromise (IOCs) with other sources 1.2.3 Checked applicability of IOC versus available infrastructure 1.2.4 Applied preventive action/resolution by blocking identified IOCs on available security technology appliances 1.2.5 Conducted continuous monitoring to detect attempts of download, access and interaction with the malicious IOCs 1.2.6 Defined and added current threat intelligence and threat mitigation activities to knowledge-based systems. 1.3 Analyzed running processes and configs on affected systems 1.3.1 Utilized Common security tools and security products available, when necessary 1.3.2 Checked known and common folder or location for possible installed malicious files. 1.3.3 Verified and monitored file integrity by tools and security products based on original installation package or digitally signed files from vendors-white listing 1.3.4 Files, folder, behavior and packets are confirmed malicious or compromised by the tools and security product 1.4 Created and implemented strategy for containment and recovery 1.4.1 Identified TTP and IOCs based on the detection and recommendation of the security products

	1.4.2 Blocked and contained IOCs using the features of EDR, NGAV and next generation firewall (NGFW) 1.4.3 Conducted continuous monitoring to detect attempts of download, access and interaction with the malicious IOCs 1.4.4 Defined and added current threat mitigation activities to knowledge-based systems. 1.4.5 Conducted system or infra recovery by checking last known good or viable image, configuration or instance of backup. 1.4.6 Conducted rollback activity based on the availability of last known good image, configuration and instance 1.4.7 Conducted removal of malicious IOCs, registry hives, files, folders using security products 1.4.8 Conducted secondary scan using the security products to determine if there are still malicious elements in the enterprise and mobile environment
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 may be assessed in the actual workplace or at the designated TESDA Accredited Assessment Center.

UNIT OF COMPETENCY : PERFORM VULNERABILITY MANAGEMENT/CONTROL

UNIT CODE : CS-ICT251204

UNIT DESCRIPTOR : This unit covers the knowledge, skills and attitude required to perform vulnerability management/control. It includes competencies in installing agent or identifying network infrastructure (product usage or management); setting schedule for scanning; performing vulnerability asset control (inventory/asset management); conducting audit of servers, endpoint and application; performing vulnerability Management (VM) change management (configuration management); and performing patch and remediation testing and deliver report (patch and capacity management).

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
1. Install agent	1.1. Vulnerability scanning and management software are identified based on ***NIST standards*** * 1.2. Core product management training of the software is conducted based on ***product*** * 1.3. Product installation is conducted based on product manual * 1.4. Product installation and configuration is verified based on NIST 800-115 *	1.1. Ticket management systems 1.2. Vulnerability management solution 1.3. Knowledge Management usage 1.4. Verification of installed product 1.5. Knowledge on NIST 800-115 1.6. Knowledge in Operating Systems	1.1. Computer operation skills 1.2. Operating systems operation 1.3. Communication skills 1.4. Interpreting work instructions 1.5. Interpersonal skills
2. Perform vulnerability asset control	2.1. Access to inventory management is coordinated with IT Service Management team 2.2. Inventory of assets is ***created*** for vulnerability scanning * 2.3. Sorting and grouping of assets inventory is performed based on ISO/IEC 19770 ***parameters****	2.1. Inventory check of devices assets and infrastructure that needs to undergo vulnerability scanning 2.2. Vulnerability management solution scan and operations procedure 2.3. Documentation of inventory check Familiarity on ISO/IEC 19770	2.1. Computer operation skills 2.2. Communication skills 2.3. Interpreting work instructions 2.4. Interpersonal skills 2.5. Documentation skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
3. Set schedule for scanning	3.1. Collaboration with IT and software development team on change management is performed based on NIST standards and ITIL version 4* 3.2. Production and staging load scheduling are checked based on NIST standards and ITIL version 4* 3.3. IT and software development team and third party provider's availability or schedule is checked based on NIST standards and ITIL version 4*	3.1. Ticket management systems 3.2. Vulnerability management solution 3.3. Scanning procedures based on vulnerability management solution 3.4. Knowledge Management usage 3.5. Vulnerability management solution usage and operations 3.6. List of assets 3.7. Knowledge on NIST 800-115 3.8. Knowledge on ITIL version 4	3.1. Computer operation skills 3.2. Communication skills 3.3. Interpreting work instructions 3.4. Interpersonal skills
4. Conduct evaluation of servers, endpoint and application	4.1. Access management of servers, endpoint and application is checked and reviewed based on ITIL version 4* 4.2. Configuration management of servers, endpoint and application is checked and reviewed based on based on ITIL version 4* 4.3. Encryption technology of servers, endpoint and application is evaluated based on ITIL version 4* 4.4. Review data retention and data destruction policy of servers, endpoint and application are reviewed based on ITIL version 4* 4.5. Preventive maintenance policy of servers, endpoint and application is reviewed based on ITIL version 4*	4.1. Ticket management systems 4.2. Vulnerability management solution 4.3. Scanning procedures based on vulnerability management solution 4.4. Knowledge Management usage 4.5. Vulnerability management solution usage and operations 4.6. List of assets 4.7. Knowledge on NIST 800-115 4.8. Knowledge in ITIL version 4 4.9. Knowledge in OWASP, stride and Mitre framework	4.1. Computer operation skills 4.2. Communication skills 4.3. Interpreting work instructions 4.4. Interpersonal skills 4.5. Vulnerability Scanning skills
5. Perform Vulnerability Management (VM) change management	5.1. Vulnerability Management change proposal is submitted to change advisory board (CAB) according to requirement* 5.2. Vulnerability Management change proposal is deliberated with the change advisory board (CAB)* 5.3. Approved Vulnerability Management change proposal is monitored as	5.1. Ticket management systems 5.2. Vulnerability management solution 5.3. Scanning procedures based on vulnerability management solution 5.4. KM usage 5.5. Vulnerability management solution usage and operations 5.6. List of assets	5.1. Computer operation skills 5.2. Communication skills 5.3. Interpreting work instructions 5.4. Interpersonal skills 5.5. Vulnerability Scanning skills

ELEMENT	PERFORMANCE CRITERIA ***Italicized terms*** are elaborated in the Range of Variables	REQUIRED KNOWLEDGE	REQUIRED SKILLS
	relayed by change manager to capacity team and subject matter expert regarding the requirement change/s * 5.4. ***Executed*** change/s of subject matter expert is observed and validated based on given requirement* 5.5. Feedback and conclusion of change/s request provided by the CAB manager is received and analyzed based on given requirement* 5.6. Scan is conducted based on schedule and scope of asset that needs to be scanned* 5.7. Vulnerability scanning results are documented and reported*	5.7. Familiarity on NIST 800-115 5.8. Knowledge in OWASP, stride and MITRE framework	5.6. Stakeholder management skills
6. Perform patch/ remediation testing and deliver report	6.1. Patch/remediation strategies and solutions are acquired from ***solution provider **** 6.2. Patch and remediation testing executed by the subject matter expert is monitored based on given requirement* 6.3. Number of failed update, failed patch and adverse effect on patch are documented based on given standards* 6.4. Report is delivered to patch management team*	6.1. Ticket management systems 6.2. Vulnerability management solution 6.3. Scanning procedures based on vulnerability management solution 6.4. Knowledge Management usage 6.5. Vulnerability management solution usage and operations 6.6. List of assets 6.7. Familiarity on NIST 800-115	6.1. Computer operation skills 6.2. Communication skills 6.3. Interpreting work instructions 6.4. Interpersonal skills 6.5. Patch Management skills 6.6. Stakeholder management skills

RANGE OF VARIABLES

VARIABLE	RANGE
1. NIST standards	NIST standards may include: 1.1. NIST 800-115 1.2. NIST 800 -53 vulnerability management
2. Product	Product may include: 2.1. Tenable, 2.2. Qualys, 2.3. Fortify
3. Created	Create inventory of assets may include: 3.1. Collect asset location (e.g, Clark, Davao, Cebu, MM, etc) 3.2. Collect asset IP and network architecture/design (e.g, segment or VLAN) 3.3. Collect operating system (e.g, MacOS, iOS, Windows, Linux, UNIX, Android, etc) 3.4. Collect third party software (e.g, CRM, web apps, APKs, productivity software) 3.5. Collect hosting providers (e.g, AWS, ALI cloud, Azure, Huawei, etc.) 3.6. Collect source code repositories (e.g, Bitbucket, SourceForge, ProjectLocker, GitLab, CloudForge, etc)
4. Parameters	Parameters on how to sort and grouped assets may include: 4.1. Standard asset classifications 4.2. Priority assets 4.3. Legacy assets
5. Executed	Executed changes on may include: 5.1. Staging environment, 5.2. If OK then proceed to production environment 5.3. If issue occur, roll back to production environment
6. Solution Provider	Solution Provider may include: 6.1. internal vendors 6.2. external vendors 6.3. software developer

EVIDENCE GUIDE

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1.1 Installed agent or identify network infrastructure 1.1.1 Identified vulnerability scanning and management software based on NIST standards 1.1.2 Conducted core product management training of the software based on product 1.1.3 Conducted product installation and troubleshooting based on product 1.2 Set schedule for scanning 1.2.1 Performed collaboration with IT and software development team on change management based on NIST standards and ITIL version 4 1.2.2 Checked production and staging load scheduling based on NIST standards and ITIL version 4 1.2.3 Checked IT, software developer and third-party provider's availability or schedule based on NIST standards and ITIL version 4 1.3 Performed vulnerability asset control (inventory/asset management) 1.3.1 Created inventory of assets for vulnerability scanning 1.3.2 Performed sorting and grouping of assets inventory based on ISO/IEC 19770 parameters 1.4 Conducted audit of servers, endpoint and application 1.4.1 Checked and reviewed access management 1.4.2 Checked and reviewed configuration management 1.4.3 Evaluated encryption technology 1.4.4 Reviewed data retention and data destruction policy 1.4.5 Reviewed preventive maintenance policy 1.5 Performed Vulnerability Management (VM) change management (configuration management) 1.5.1 Submitted change proposal by change requestor (CR) according requirement 1.5.2 Deliberated change proposal by the change advisory board (CAB) 1.5.3 Relayed approved proposal by change manager to capacity and subject matter expert regarding the requirement change/s 1.5.4 Executed change/s by the subject matter expert based on given requirement 1.5.5 Provided feedback and conclusion of change/s request based on procedures 1.6 Performed patch and remediation testing and deliver report (patch and capacity management) 1.6.1 Execute patch and remediation testing by based on given requirement 1.6.2 Delivered report to patch management team
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
4. Context for Assessment	4.1 Competency may be assessed in the actual workplace or at the designated TESDA Accredited Assessment Center.

ANNEX A. ICT COMPETENCY MAP – Cyber Threat Mitigation Level II

BASIC COMPETENCIES

Receive and respond to workplace communication	**Participate in workplace communication**	Lead workplace communication	Utilize specialized communication skill	Manage and sustain effective communication strategies
Work with others	**Work in team environment**	Lead small teams	Develop and lead teams	Manage and sustain high performing teams
Solve/address routine problems	**Solve/address general workplace problems**	Apply critical thinking and problem solving techniques in the workplace	Perform higher order thinking processes and apply techniques in the workplace	Evaluate higher order thinking skills and adjust problem solving techniques
Enhance self-management skills	**Develop career and life decisions**	Work in a diverse environment	Contribute to the practice of social justice in the workplace	Advocate strategic thinking for global citizenship
Support Innovation	**Contribute to workplace innovation**	Propose methods of applying learning and innovation in the organization	Manage innovative work instructions	Incorporate innovation into work procedures
Access and maintain information	**Present relevant information**	Use information systematically	Manage and evaluate usage of information	Develop systems in managing, and maintaining information
Follow occupational safety and health policies and procedures	**Practice occupational safety and health policies and procedures**	Evaluate occupational safety and health work practices	Lead in improvement of Occupational Safety and Health Program, Policies and Procedures	Manage implementation of occupational safety and health programs in the workplace
Apply environmental work standards	**Exercise efficient and effective sustainable practices in the workplace**	Evaluate environmental work practices	Lead towards improvement of environmental work programs, policies and procedures	Manage implementation of environmental programs in the workplace
Adopt entrepreneurial mindset in the workplace	**Practice entrepreneurial skills in the workplace**	Facilitate entrepreneurial skills for micro-small-medium enterprises (MSMEs)	Sustain entrepreneurial skills	Develop and sustain a high-performing enterprise

COMMON COMPETENCIES

Apply Quality Standards	**Perform Computer Operations**

CORE COMPETENCIES

Communicate effectively in a customer contact center	Render quality customer service	Utilize enterprise/ company technology	Conduct contact center campaign	Provide specialized support and assistance to customers
Lead a contact center work team	Manage the activities of a contact center work team	Use business technology	Use medical technology to carry out task	Produce text from audio transcription
Review/edit documents	Lead a team in delivering quality service	Apply traditional drawing techniques for animation	Produce traditional cleaned-up drawings	Produce traditional in-between drawings
Produce Traditional key poses/drawings for animation	Create 2D digital animation	Export Animation into Video file format	Produce digital cleaned-up drawings	Produce digital in-between drawings
Produce background designs	Composite and edit animation sequence	Create 3D digital animation	Produce storyboard for animation	Coordinate the production of animation
Produce over-all designs for animation	Produce key drawings for animation	Create 3D models for animation	Apply 3D texture and lighting to 3D models	Set character rigging
Animate character	Composite and render animation sequence	Create 2D digital animation	Produce cleaned-up and in-betweened drawings	Use an authoring tool to create an interactive sequence
Produce key drawings for animation	Utilize Software Methodologies	Develop Responsive Web Design	Create Interactive Websites (Using JavaScript)	Develop Website Backend Systems
Develop designs for a logo	Develop designs for print media	Develop designs for user experience	Develop designs for user interface	Develop designs for product packaging
Design booth and product/window display	Provide an appropriate response to an event/incident	Ensure efficient escalation and ticketing	Ensure privacy and confidentiality of all security event/incident	Monitor and report cybersecurity threats
Provide an appropriate action to prevent a possible event/incident	Ensure efficient case management of handled event/incident	Monitor volume case reporting	Ensure privacy and confidentiality of all security event/incident	Conduct vulnerability scanning
Perform threat mitigation	**Perform vulnerability management/control**			

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 for 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 perform 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 for 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 Training Regulations. 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) **Training Regulations (TR)** – refers to the document promulgated and issued by TESDA consisting of competency standards, national qualifications and training guidelines for specific sectors/occupations. The TR serves as basis for establishment of qualification and certification under the PTQF. It also serves as guide for development of competency-based curricula and instructional materials including registration of TVET programs offered by TVET providers

23) **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

24) **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

25) **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. **Data** - objective measurements of the attributes (characteristics) of entities such as people, places, things, and events.
16. **Data** - Collection of values assigned to base measures, derived measures and/or indicators. This definition applies only within the Context for ISO/IEC 27004:2009
17. **DICT** - Department of Information and Communications Technology
18. **DDoS** - Distributed Denial of Service
19. **Documentation** – a collection of documents or information.
20. **Edit** – to modify the form or format of data
21. **Effect** - Is a deviation from the expected — positive and/or negative.
22. **Effectiveness** - Extent to which planned activities are realized and planned results achieved.
23. **Efficiency** - Relationship between the results achieved and the resources used.
24. **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.

25. **End-user –** anyone who uses an information system or the information it produces.
26. **Endpoint Detection & Response -** also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.
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. **Extended detection and response (XDR) -** is a consolidation of tools and data that provides extended visibility, analysis, and response across endpoints, workloads, users, and networks.
30. **File folders**, also called directories, - a way to organize computer files.
31. **Guideline** - Description that clarifies what should be done and how, to achieve the objectives set out in policies.
32. **ICT systems** - Hardware, software, firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment.
33. **Incident** – any flagged alert of threat/s detected by the security solution product.
34. **IDS** - Intrusion Detection System
35. **IEC** - International Electrotechnical Commission
36. **Indicators of compromise (IOCs) -** are pieces of forensic data, such as data found in system log entries or files that identify potentially malicious activity on a system or network. Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or other threat.
37. **Information** – data placed in a meaningful and useful context for an end user.
38. **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.
39. **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.
40. **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
41. **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

42. **Information system** - Application, service, information technology asset, or any other information handling component
43. **Infrastructure** - Facilities and equipment to enable the ICT DR services, including but not limited to power supply, telecommunications connections and environmental controls
44. **Integrity** - Property of protecting the accuracy and completeness of assets
45. **ISMS** - Information Security Management System
46. **ISO** - International Standards Organization
47. **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.
48. **Management** - Coordinated activities to direct and control an organization
49. **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
50. **Managed detection and response (MDR) -** an MDR solution provides access to both the tools and security expertise that an organization needs to protect itself against cyber threats. An MDR provider will offer round-the-clock network monitoring and incident investigation and response.
51. **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
52. **NCERT** - National Computer Emergency Response Team
53. **NIST -** National Institute of Standards and Technology
54. **Object** - Item characterized through the measurement of its attributes
55. **Organizations** - Entities which utilize ICT DR services
56. **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.
57. **POC** - Point of Contact
58. **Policy** - Overall intention and direction as formally expressed by management
59. **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.
60. **Procedure** - Specified way to carry out an activity or a process
61. **Process** - Set of interrelated or interacting activities which transforms inputs into outputs
62. **Quality Assurance –** methods for ensuring that information systems are free from errors and fraud and provide information products of high quality.
63. **Record** - Document stating results achieved or providing evidence of activities performed

64. **Reliability** - Property of consistent intended behavior and results
65. **Review** - Activity undertaken to determine the suitability, adequacy and effectiveness (2.22) of the subject matter to achieve established objectives
66. **Review object** - Specific item being reviewed
67. **Risk** - Combination of the probability of an event and its consequence
68. **Risk acceptance** - Decision to accept a risk
69. **Risk analysis** - Process to comprehend the nature of risk and to determine the level of risk
70. **Risk assessment** - Overall process of risk identification, risk analysis and risk evaluation
71. **Risk management** - Coordinated activities to direct and control an organization with regard to risk.
72. **SIEM** - Security Information and Event Management
73. **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.
74. **Software –** computer programs and procedures concerned with the operation of an information system.
75. **Standards –** measures of performance developed to evaluate the progress of a system toward its objectives
76. **Stakeholder** - Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity
77. **System –** an assembly of methods, procedures, or techniques unified by regulated interaction to form an organized whole
78. **Third party** - Person or body that is recognized as being independent of the parties involved, as concerns the issue in question
79. **Threat** - Potential cause of an unwanted incident, which may result in harm to a system or organization
80. **Threat Mitigation -** also called cyber risk mitigation or cyber attack mitigation - is a term that describes the tools, processes, and strategies companies use to reduce the severity of or seriousness of a potential data breach or other cyber attack.
81. **Ticket management system** – any document (physical or digital) that possessed the following – reporter, time, date, details of incident and status of the case.
82. **User- friendly** – a characteristic of human-operated equipment and systems that makes them safe, comfortable, and easy to use.
83. **Validation** - Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled
84. **Verification** - Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
85. **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) wishes to extend thanks and appreciation to the many representatives of business, industry, academe and government agencies who donated their time and expertise to the development and validation of these Competency Standards.

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 COMPETENY 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