REPUBLIC OF KENYA

NATIONAL OCCUPATIONAL STANDARDS

FOR

CYBER SECURITY TECHNICIAN

LEVEL 6

TVET CDACC
P.O BOX 15745-00100
NAIROBI

First published 2019

Council Secretary/CEO
TVET Curriculum Development, Assessment and Certification Council
P.O. Box 15745–00100 Nairobi, Kenya
Email: info@tvetcdacc.go.ke

FOREWORD

The provision of quality education and training is fundamental to the Government's overall strategy for social economic development. Quality education and training will contribute to achievement of Kenya's development blue print and sustainable development goals.

Reforms in the education sector are necessary for the achievement of Kenya Vision 2030 and meeting the provisions of the Constitution of Kenya 2010. The education sector had to be aligned in the Constitution and this resulted to the formulation of the Policy Framework for Reforming Education and Training. A key feature of this policy is the radical change in the design and delivery of the TVET training. This policy document requires that training in TVET be competency based, curriculum development be industry led, certification be based on demonstration of competence and mode of delivery allows for multiple entry and exit in TVET programmes.

These reforms demand that Industry takes a leading role in curriculum development to ensure the curriculum addresses its competence needs. It is against this background that this Occupational Standard was developed for the purpose of developing a competency-based curriculum for Cyber Security Level 6. These Occupational Standards will also be the basis for assessment of an individual for competence certification.

It is my conviction that this Occupational Standard will play a great role towards development of competent human resource for the Security Sector's growth and sustainable development.

PRINCIPAL SECRETARY, VOCATIONAL AND TECHNICAL TRAINING
MINISTRY OF EDUCATION

PREFACE

Kenya Vision 2030 aims to transform the country into a newly industrializing, "middle-income country providing a high-quality life to all its citizens by the year 2030". Kenya intends to create a globally competitive and adaptive human resource base to meet the requirements of a rapidly industrializing economy through life-long education and training. TVET has a responsibility of facilitating the process of inculcating knowledge, skills and attitudes necessary for catapulting the nation to a globally competitive country, hence the paradigm shift to embrace Competency Based Education and Training (CBET).

The Technical and Vocational Education and Training Act No. 29 of 2013 and the Sessional Paper No. 4 of 2012 on Reforming Education and Training in Kenya, emphasized the need to reform curriculum development, assessment and certification. This called for shift to CBET to address the mismatch between skills acquired through training and skills needed by industry as well as increase the global competitiveness of Kenyan labour force.

The TVET Curriculum Development, Assessment and Certification Council (TVET CDACC), in conjunction with Security Sector Skills Advisory Committee (SSAC) have developed these Occupational Standards for a Cyber Security Operator. These standards will be the basis for development of a competency-based curriculum for cyber Security Level 6. These Standards will also be the basis for assessment of an individual for competence certification.

The occupational standards are designed and organized with clear performance criteria for each element of a unit of competency. These standards also outline the required knowledge and skills as well as evidence guide.

I am grateful to the Council Members, Council Secretariat, Security SSAC, expert workers and all those who participated in the development of these occupational standards.

Prof. CHARLES M. M. ONDIEKI, PhD, FIET (K), Con. Eng. Tech.
CHAIRMAN, TVET CDACC

ACKNOWLEDGMENT

These Occupational Standards were developed through combined effort of various stakeholders from private and public organizations. I am sincerely thankful to the management of these organizations for allowing their staff to participate in this course. I wish to acknowledge the invaluable contribution of industry players who provided inputs towards the development of these Standards.

I thank TVET Curriculum Development, Assessment and Certification Council (TVET CDACC) for providing guidance on the development of these Standards. My gratitude goes to the Security Sector Skills Advisory Committee (SSAC) members for their contribution to the development of these Standards. I thank all the individuals and organizations who participated in the validation of these Standards.

I acknowledge all other institutions which in one way or another contributed to the development of these Standards.

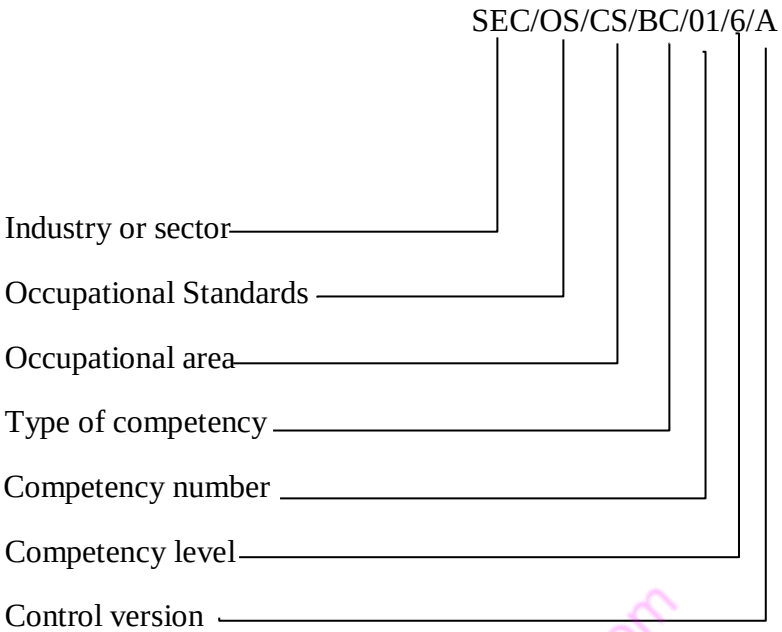
CHAIRPERSON
SECURITY SECTOR SKILLS ADVISORY COMMITTEE

TABLE OF CONTENT

ACRONYMS AND ABBREVIATIONS

A	Control Version
BC	Basic Competencies
CC	Common Competencies
CDACC	Curriculum Development, Assessment and Certification Council
CERT	Computer Incidence response team
CIRT	Computer Incidence response team
CS	Cyber Security
CR	Core Competencies
EHS	Environment, Health and Safety
IBMS	Integrated Building Management System
ICT	Information and communication Technology
IEE	Institute of Electrical Engineers
KEBS	Kenya Bureau of Standards
NCA	National Construction Authority
NIST	National institute of Standards and Technology
OS	Occupational Standards
OSHA	Occupational Safety and Health Act
OWASP	Open web application security Project
PPE	Personal Protective Equipment
SEC	Security
SIEM	Security Information and Event management
TVET	Technical and Vocational Education and Training
WIBA	Work injury benefits Act

KEY TO UNIT CODE



OVERVIEW

Cyber Security Level 6 qualification consists of competencies that a person must achieve to enable him/her to be certified as a Cyber Securiy technician.

A Cyber security technician is a person who will carry out Cyber security duties using a given design and customer's requirements. It involves performing Computer repair and maintenance, demonstrating understanding of security laws, policies and regulations, performing Computer Networking, building secure network, developing Computer software, securing Software application, databases, installing Cyber security system, managing Cyber Security risks, conducting security Assessment and testing and managing security Operations.

The units of competency comprising Cyber Security Technician level 6 qualifications include the following basic, common and core competencies:

BASIC COMPETENCY

Unit Code	Unit Title
SES/OS/CS/BC/01/6/A	Demonstrate communication skills
SEC/OS/CS/BC/02/6/A	Demonstrate Numeracy skills
SEC/OS/CS/BC/03/6/A	Demonstrate entrepreneurial skills
SEC/OS/CS/BC/04/6/A	Demonstrate employability skills
SEC/OS/CS/BC/05/6/A	Demonstrate environmental literacy
SEC/OS/CS/BC/06/6/A	Demonstrate occupational safety and health practices

COMMON COMPETENCIES

Unit Code	Unit Title
SEC/OS/CS/CC/01/6/A	Demonstrate Digital Literacy

CORE COMPETENCY

Unit Code	Unit Title
SEC/OS/CS/CR/01/6/A	Perform Computer repair and maintenance
SEC/OS/CS/CR/02/6/A	Demonstrate understanding of security laws, policies and regulations
SEC/OS/CS/CR/03/6/A	Perform Computer Networking
SEC/OS/CS/CR/04/6/A	Build secure network
SEC/OS/CS/CR/05/6/A	Develop Computer software
SEC/OS/CS/CR/06/6/A	Secure Software application
SEC/OS/CS/CR/07/6/A	Secure Databases
SEC/OS/CS/CR/08/6/A	Install Cyber security system
SEC/OS/CS/CR/09/6/A	Manage Cyber Security risks
SEC/OS/CS/CR/10/6/A	Conduct security Assessment and testing

SEC/OS/CS/CR/11/6/A	Manage security Operations

BASIC UNITS OF COMPETENCY

DEMONSTRATE COMMUNICATION SKILLS

UNIT CODE: SES/OS/CS/BC/01/6/A

UNIT DESCRIPTION

This unit covers the competencies required to demonstrate communication skills. It involves meeting communication needs of clients and colleagues, developing communication strategies, establishing and maintaining communication pathways, conducting interviews, facilitating group discussion and representing the organization.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range***
1. Meet communication needs of clients and colleagues	1.1 Specific communication needs of clients and colleagues are identified and met based on workplace requirements 1.2 Different communication approaches are identified and applied according to clients' needs 1.3 Conflict is identified and addressed as per the standards of the organization
2. Develop communication strategies	2.1 Strategies for effective internal and external dissemination of information are developed as per organization's requirements 2.2 Special communication needs are considered in developing strategies according workplace procedures 2.3 ***Communication strategies*** are analyzed, evaluated and revised based the workplace needs
3. Establish and maintain communication pathways	3.1 Pathways of communication are established as per organization policy 3.2 Pathways are maintained and reviewed according to organization procedures
4. Promote use of communication strategies	4.1 Information is provided to all areas of the organization as per strategy requirements 4.2 Effective communication techniques are articulated and modeled according work requirements 4.3 Personnel are given guidance about adapting communication strategies as per organization procedures
5. Conduct interview	5.1 A range of appropriate communication strategies are employed in ***interview situations*** based on the workplace requirements

	5.2 Records of interviews are made and maintained in accordance with organizational procedures 5.3 Effective questioning, listening and nonverbal communication techniques are used as per needs
6. Facilitate group discussion	6.1 Mechanisms to enhance ***effective group interaction*** are identified and implemented according to workplace requirements 6.2 Strategies to encourage group participation are identified and used as per organizations' procedures 6.3 Meetings objectives and agenda are set and followed based on workplace requirements 6.4 Relevant information is provided and feedback obtained according to set protocols 6.5 Evaluation of group communication strategies is undertaken in accordance with workplace guidelines 6.6 Specific communication needs of individuals are identified and addressed as per individual needs
7. Represent the organization	5.1 7Relevant presentation are researched and presented based on internal or external communication forums requirements 5.2 Presentation is delivered in a clear and sequential manner as per the predetermined time 5.3 Presentation is made as per appropriate media 5.4 Difference views are respected based on workplace procedures 5.5 Written communication is done as per organizational standards 5.6 Inquiries are responded according to organizational standard

RANGE

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

Variable	**Range**
1. Communication strategies may include but not limited to:	• Language switch • Comprehension check • Repetition • Asking confirmation • Paraphrase • Clarification request • Translation

	• Restructuring • Approximation • Generalization
2. Effective group interaction may include but not limited to:	• Identifying and evaluating what is occurring within an interaction in a nonjudgmental way • Using active listening • Making decision about appropriate words, behavior • Putting together response which is culturally appropriate • Expressing an individual perspective • Expressing own philosophy, ideology and background and exploring impact with relevance to communication
3. Situations may include but not limited to:	• Establishing rapport • Eliciting facts and information • Facilitating resolution of issues • Developing action plans • Diffusing potentially difficult situations

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Communication
- Active listening
- Interpretation
- Negotiation
- Writing

Required Knowledge

The individual needs to demonstrate knowledge of:

- Communication process
- Dynamics of groups
- Styles of group leadership
- Key elements of communications strategy

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical aspects	Assessment requires evidence that the candidate:

of Competency	1.1 Developed communication strategies to meet the organization requirements and applied in the workplace 1.2 Established and maintained communication pathways for effective communication in the workplace 1.3 Used communication strategies involving exchanges of complex oral information
2. Resource Implications for competence certification	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 Direct observation 3.2 Oral questioning 3.3 Written texts
4. Context of Assessment	Competency may be assessed: 4.1 On-the-job 4.2 Off-the –job 4.3 During Industrial attachment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

DEMONSTRATE NUMERACY SKILLS

UNIT CODE: SES/OS/CS/BC/02/6/A

UNIT DESCRIPTION

This unit describes the competencies required to demonstrate numeracy skills. It involves; applying a wide range of mathematical calculations for work; applying ratios, rates and proportions to solve problems; estimating, measuring and calculating measurement for work; using detailed maps to plan travel routes for work; using geometry to draw and construct 2D and 3D shapes for work; collecting, organizing and interpreting statistical data; using routine formula and algebraic expressions for work and using common functions of a scientific calculator.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range.***
1. Apply a wide range of mathematical calculations for work	1.1 Mathematical information embedded in a range of workplace tasks and texts is extracted as per workplace procedures. 1.2 Mathematical information is interpreted and comprehended as per job specifications 1.3 A range of mathematical and problem solving processes are selected and used as per job specification 1.4 Different forms of fractions, decimals and percentages are flexibly used as per SOPs 1.5 Calculation performed with positive and negative numbers as per SOPs 1.6 Numbers are expressed as powers and roots and are used in calculations as per SOPs 1.7 Calculations done using routine formulas as per SOPs 1.8 Estimation and assessment processes are used to check outcome as per workplace procedures 1.9 Mathematical language is used to discuss and explain the processes, results and implications of the task as per workplace procedures
2. Use and apply ratios, rates and proportions for work	2.1 Information regarding ratios, rates and proportions extracted from a range of workplace tasks and texts as per SOPs 2.2 Mathematical information related to ratios, rate and proportions is analysed as per SOPs

	2.3 Problem solving processes are used to undertake the task as per workplace procedures 2.4 Equivalent ratios and rates are simplified as per SOPs 2.5 Quantities are calculated using ratios, rates and proportions as per SOPS 2.6 Graphs, charts or tables are constructed to represent ratios, rates and proportions as per SOPs 2.7 The outcomes reviewed and checked as per job specifications 2.8 Information is record using mathematical language and symbols as per workplace procedures
3. Estimate, measure and calculate measurement for work	3.1 Measurement information embedded in workplace texts and tasks are extracted and interpreted as per job specifications 3.2 Appropriate workplace measuring equipment are identified and selected as per job specifications 3.3 Accurate measurements are estimated and made as per SOPs 3.4 The area of ***2D shapes*** including compound shapes are calculated as per SOPs 3.5 The volume of 3D shapes is calculated using relevant formulas as per SOPs 3.6 Sides of right angled triangles are calculated using Pythagoras' theorem as per SOPs 3.7 conversions are perform between units of measurement as per job specification 3.8 Problem solving processes are used to undertake the task as per workplace Procedures 3.9 The measurement outcomes are reviewed and checked as per workplace procedures 3.10 Information is recorded using mathematical language and symbols appropriate for the task as per workplace procedures
4. Use detailed maps to plan travel routes for work	4.1 Different types of maps are identified and interpreted as per job requirements 4.2 Key features of maps are identified as per job requirements 4.3 Scales are identified and interpreted as per job requirements 4.4 Scales are applied to calculate actual distances 4.5 Positions or locations are determined using directional information as per job requirements 4.6 Routes are planned by determining directions and

	calculating distances, speeds and times as per job requirements 4.7 Information is gathered and identified and relevant factors related to planning a route checked as per job requirements 4.8 Relevant equipment is select and checked for accuracy and operational effectiveness as per job requirements 4.9 Task is planned and recorded using specialized mathematical language and symbols appropriate for the task as per job requirements
5. Use geometry to draw 2D shapes and construct 3D shapes for work	5.1 A range of 2D shapes and 3D shapes and their uses in work contexts is identified as per job specifications 5.2 Features of 2D and 3D shapes are named and described as per job specifications 5.3 Types of angles in 2D and 3D shapes are identified as per job specifications 5.4 Angles are drawn, estimated and measured using geometric instruments as per job requirements 5.5 Angle properties of 2D shapes are named and identified as per SOPs 5.6 Angle properties are used to evaluate unknown angles in shapes as per SOPs 5.7 Properties of perpendicular and parallel lines are applied to shapes as per SOPs 5.8 Understanding and use of symmetry is demonstrated as per SOPs 5.9 Understanding and use of similarity is demonstrated as per SOPs 5.10 The workplace tasks and mathematical processes required are identified as per workplace procedures 5.11 2D shapes is drawn for work as per job specification 5.12 3D shapes is constructed for work as per job specification 5.13 The outcomes are reviewed and checked as per workplace procedures 5.14 Specialized mathematical language and symbols appropriate for the task are used as per SOPs
6. Collect, organize, and interpret statistical data	6.1 Workplace issue requiring investigation are identified as per workplace procedures 6.2 Audience / population / sample unit is determined as per workplace procedures as per workplace

for work	procedures 6.3 Data to be collected is identified as per workplace procedures 6.4 Data collection method is selected as per workplace procedures 6.5 Appropriate statistical data is collected and organized as per SOPs 6.6 Data is illustrated in appropriate formats as per SOPs 6.7 The effectiveness of different types of graphs are compared as per SOPs 6.8 The summary statistics for collected data is calculated as per SOPs 6.9 The results / findings are interpreted as per SOPs 6.10 Data is checked to ensure that it meets the expected results and content as per workplace procedures 6.11 Information from the results including tables, graphs and summary statistics is extracted and interpreted as per workplace procedure 6.12 Mathematical language and symbols are used to report results of investigation as per workplace procedure
7. Use routine formula and algebraic expressions for work	7.1 Understanding of informal and symbolic notation, representation and conventions of algebraic expressions is demonstrated as per SOPs 7.2 Simple algebraic expressions and equations are developed as per job specification 7.3 Operate on algebraic expressions as per job requirement 7.4 Algebraic expressions are simplified as per job requirement 7.5 Substitution into simple routine equations is done as per SOPs 7.6 Routine formulas used for work tasks are identified and comprehended as per SOPs 7.7 Routine formulas are evaluate by substitution as per SOPs 7.8 Routine formulas transposed as per SOPs 7.9 Appropriate formulas are identified and used for work related tasks as per workplace procedures 7.10 Outcomes are checked and result of calculation used as per workplace procedures
8. Use common functions of a	8.1 Required numerical information to perform tasks is located as per job specification

scientific calculator for work	8.2 The order of operations and function keys necessary to solve mathematical calculation are determined as per job specification 8.3 Function keys on a scientific calculator are identified and used as per SOPs 8.4 Estimations are referred to check reasonableness of problem solving process as per workplace procedures 8.5 Appropriate mathematical language, symbols and conventions are used to report results as per workplace procedures

RANGE

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

Variable	Range
1. 2D shapes may include but not limited may includ but not limited to:	• Triangles • Square • Rectangle • Triangle

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Measuring
- Logical thinking
- Computing
- Drawing of graphs
- Applying mathematical formulas
- Analytical

Required knowledge

The individual needs to demonstrate knowledge of:

- Types of common shapes
- Differentiation between two dimensional shapes / objects

- Formulae for calculating area and volume
- Types and purpose of measuring instruments
- Units of measurement and abbreviations
- Fundamental operations (addition, subtraction, division, multiplication)
- Rounding techniques
- Types of fractions
- Different types of tables and graphs
- Meaning of graphs, such as increasing, decreasing, and constant value
- Preparation of basic data, tables & graphs

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical aspects of Competency	Assessment requires evidence that the candidate: 1. 1Developed communication strategies to meet the organization requirements and applied in the workplace 1. 2Established and maintained communication pathways for effective communication in the workplace 1. 3 Used communication strategies involving exchanges of complex oral information
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 Observation 3.2 Oral questioning 3.3 Written test 3.4 Portfolio of Evidence 3.5 Interview 3.6 Third party report
4. Context of Assessment	Competency may be assessed: 4.1 On-the-job 4.2 Off-the –job 4.3 During Industrial attachment
5. Guidance information for	Holistic assessment with other units relevant to the industry sector, workplace and job role is

assessment	recommended.

DEMONSTRATE ENTREPRENEURIAL SKILLS

UNIT CODE : SES/OS/CS/BC/03/6/A

UNIT DESCRIPTION

This unit covers the competencies required to demonstrate understanding of entrepreneurship. It involves demonstrating understanding of an entrepreneur, entrepreneurship, and self-employment, identifying entrepreneurship opportunities, creating entrepreneurial awareness, applying entrepreneurial motivation, developing business innovative strategies and developing business plan.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
1. Demonstrate understanding of an Entrepreneur	1. 1 Entrepreneurs and Business persons are distinguished as per principles of entrepreneurship 1. 2 ***Types of entrepreneurs*** are identified as per principles of entrepreneurship 1. 3 Ways of becoming an Entrepreneur are identified as per principles of Entrepreneurship 1. 4 ***Characteristics of Entrepreneurs*** are identified as per principles of Entrepreneurship 1. 5 Factors affecting Entrepreneurship development are explored as per principles of Entrepreneurship
2. Demonstrate understanding of Entrepreneurship and self-employment	2. 1 Entrepreneurship and self-employment are distinguished as per principles of entrepreneurship 2. 2 Importance of self-employment is analysed based on business procedures and strategies 2. 3 ***Requirements for entry into self-employment*** are identified according to business procedures and strategies 2. 4 Role of an Entrepreneur in business is determined according to business procedures and strategies

	2. 5 Contributions of Entrepreneurs to National development are identified as per business procedures and strategies 2. 6 Entrepreneurship culture in Kenya is explored as per business procedures and strategies 2. 7 Born or made Entrepreneurs are distinguished as per entrepreneurial traits
3. Identify Entrepreneurship opportunities	3.1 Sources of business ideas are identified as per business procedures and strategies 3.2 Business ideas and opportunities are generated as per business procedures and strategies 3.3 Business life cycle is analysed as per business procedures and strategies 3.4 Legal aspects of business are identified as per procedures and strategies 3.5 Product demand is assessed as per market strategies 3.6 Types of ***business environment*** are identified and evaluated as per business procedures 3.7 Factors to consider when evaluating business environment are explored based on business procedure and strategies 3.8 Technology in business is incorporated as per best practice
4. Create entrepreneurial awareness	4.1 ***Forms of businesses*** are explored as per business procedures and strategies 4.2 Sources of business finance are identified as per business procedures and strategies 4.3 Factors in selecting source of business finance are identified as per business procedures and strategies 4.4 ***Governing policies*** on Small Scale Enterprises (SSEs) are determined as per business procedures and strategies 4.5 Problems of starting and operating SSEs are explored as per business procedures and strategies
5. Apply entrepreneurial motivation	5.1 ***Internal and external motivation*** factors are determined in accordance with motivational theories

	5.2 Self-assessment is carried out as per entrepreneurial orientation 5.3 Effective communications are carried out in accordance with communication principles 5.4 Entrepreneurial motivation is applied as per motivational theories
6. Develop innovative business strategies	6.1 Business innovation strategies are determined in accordance with the organization strategies 6.2 Creativity in business development is demonstrated in accordance with business strategies 6.3 ***Innovative business strategies*** are developed as per business principles 6.4 Linkages with other entrepreneurs are created as per best practice 6.5 ICT is incorporated in business growth and development as per best practice
7. Develop Business Plan	7.1 Identified Business is described as per business procedures and strategies 7.2 Marketing plan is developed as per business plan format 7.3 Organizational/Management plan is prepared in accordance with business plan format 7.4 Production/operation plan in accordance with business plan format 7.5 Financial plan is prepared in accordance with the business plan format 7.6 Executive summary is prepared in accordance with business plan format 7.7 Business plan is presented as per best practice

RANGE

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

Variable	**Range**
1. Types of entrepreneurs may include but not limited to:	• Innovators • Imitators • Craft

	• Opportunistic • Speculators
2. Characteristics of Entrepreneurs may include but not limited to:	• Creative • Innovative • Planner • Risk taker • Networker • Confident • Flexible • Persistent • Patient • Independent • Future oriented • Goal oriented
3. Requirements for entry into self-employment may include but not limited to	• Technical skills • Management skills • Entrepreneurial skills • Resources • Infrastructure
4. Internal and external motivation may include but not limited to:	• Interest • Passion • Freedom • Prestige • Rewards • Punishment • Enabling environment • Government policies
5. Business environment may include but not limited to:	• External • Internal • Intermediate
6. Forms of businesses may include but not limited to:	• Sole proprietorship • Partnership • Limited companies • Cooperatives
7. Governing policies may include but not limited to:	• Increasing scope for finance • Promoting cooperation between entrepreneurs and private sector • Reducing regulatory burden on entrepreneurs • Developing IT tools for

	entrepreneurs
8. Innovative business strategies may include but not limited to:	• New products • New methods of production • New markets • New sources of supplies • Change in industrialization

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Analytical
- Management
- Problem-solving
- Root-cause analysis
- Communication

Required Knowledge

The individual needs to demonstrate knowledge of:

- Decision making
    - Business communication
    - Change management
    - Competition
    - Risk
    - Net working
    - Time management
    - Leadership
- Factors affecting entrepreneurship development
- Principles of Entrepreneurship
- Features and benefits of common operational practices, e. g., continuous improvement (kaizen), waste elimination,
- Conflict resolution
- Health, safety and environment (HSE) principles and requirements
- Customer care strategies
- Basic financial management
- Business strategic planning
- Impact of change on individuals, groups and industries
- Government and regulatory processes
- Local and international market trends
- Product promotion strategies

- Market and feasibility studies
- Government and regulatory processes
- Local and international business environment
- Relevant developments in other industries
- Regional/ County business expansion strategies

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical Aspects of Competency	1. 1 Assessment requires evidence that the candidate: 1. 2 Distinguished entrepreneurs and businesspersons correctly 1. 3 Identified ways of becoming an entrepreneur appropriately 1. 4 Explored factors affecting entrepreneurship development appropriately 1. 5 Analysed importance of self-employment accurately 1. 6 Identified requirements for entry into self-employment correctly 1. 7 Identified sources of business ideas correctly 1. 8 Generated Business ideas and opportunities correctly 1. 9 Analysed business life cycle accurately 1. 10 Identified legal aspects of business correctly 1. 11 Assessed product demand accurately 1. 12 Determined Internal and external motivation factors appropriately 1. 13 Carried out communications effectively 1. 14 Identified sources of business finance correctly 1. 15 Determined Governing policy on small scale enterprise appropriately 1. 16 Explored problems of starting and operating SSEs effectively 1. 17 Developed Marketing, Organizational/Management, Production/Operation and Financial plans correctly 1. 18 Prepared executive summary correctly 1. 19 Determined business innovative strategies appropriately

	1. 20 Presented business plan effectively
2. Resource Implications	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place
3. Methods of Assessment	3.1 Written tests 3.2 Oral questions 3.3 Third party report 3.4 Interviews 3.5 Portfolio of Evidence
4. Context of Assessment	Competency may be assessed 4.1 On-the-job 4.2 Off-the –job 4.3 During Industrial attachment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

DEMONSTRATE EMPLOYABILITY SKILLS

UNIT CODE: SES/OS/CS/BC/04/6/A

UNIT DESCRIPTON

This unit covers competencies required to demonstrate employability skills. It involves conducting self-management, demonstrating interpersonal communication, critical safe work habits, leading a workplace team, planning and organizing work, maintaining professional growth and development, demonstrating workplace learning, problem solving skills and managing ethical performance.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range***
1. Conduct self-management	1.1 Personal vision, mission and goals are formulated based on potential and in relation to organization objectives 1.2 Emotional intelligence is demonstrated as per workplace requirements. 1.3 Individual performance is evaluated and monitored according to the agreed targets. 1.4 Assertiveness is developed and maintained based on the requirements of the job. 1.5 Accountability and responsibility for own actions are demonstrated based on workplace instructions. 1.6 Self-esteem and a positive self-image are developed and maintained based on values. 1.7 Time management, attendance and punctuality are observed as per the organization policy. 1.8 Goals are managed as per the organization's objective 1.9 Self-strengths and weaknesses are identified based on personal objectives
2. Demonstrate interpersonal communication	2.1 Writing skills are demonstrated as per communication policy 2.2 Negotiation and persuasion skills are demonstrated as per communication policy 2.3 Internal and external stakeholders' needs are identified and interpreted as per the communication policy

	2.4 Communication networks are established based on workplace policy 2.5 Information is shared as per communication policy
3. Demonstrate critical safe work habits	3.1 Stress is managed in accordance with workplace policy. 3.2 Punctuality and time consciousness is demonstrated in line with workplace policy. 3.3 Personal objectives are integrated with organization goals based on organization's strategic plan. 3.4 ***Resources*** are utilized in accordance with workplace policy. 3.5 Work priorities are set in accordance to workplace goals and objectives. 3.6 Leisure time is recognized and utilized in line with personal objectives. 3.7 ***Drugs and substances of abuse*** are identified and avoided based on workplace policy. 3.8 HIV and AIDS prevention awareness is demonstrated in line with workplace policy. 3.9 Safety consciousness is demonstrated in the workplace based on organization safety policy. 3.10 ***Emerging issues*** are identified and dealt with in accordance with organization policy.
4. Lead a workplace team	4.1 Performance targets for the ***team*** are set based on organization's objectives 4.2 Duties are assigned in accordance with the organization policy. 4.3 ***Forms of communication*** in a team are established according to organization's policy. 4.4 Team performance is evaluated based on set targets as per workplace policy. 4.5 Conflicts are resolved between team members in line with organization policy. 4.6 Gender related issues are identified and mainstreamed in accordance workplace policy. 4.7 Human rights and fundamental freedoms are identified and respected as Constitution of Kenya 2010. 4.8 Healthy relationships are developed and maintained in line with workplace.
5. Plan and organize work	5.1 Work plans are prepared based on activities and budget. 5.2 Assigned tasks are interpreted and expectations identified as per the workplace instructions.

	5.3 Task occupational safety and health requirements are identified and observed regulations. 5.4 Work resources are identified, mobilized, allocated and utilized based on organization work plans. 5.5 Work activities are monitored and evaluated in line with work plans and workplace policy. 5.6 Work plans are reviewed based on target and available resources.
6. Maintain professional growth and development	6.1 Personal training needs are identified and assessed in line with the requirements of the job. 6.2 ***Training and career opportunities*** are identified and utilized based on job requirements. 6.3 Resources for training are mobilized and allocated based organizations and individual skills needs. 6.4 Licensees and certifications relevant to job and career are obtained and renewed as per policy. 6.5 Work priorities and personal commitments are balanced and managed based on requirements of the job and personal objectives. 6.6 Recognitions are sought as proof of career advancement in line with professional requirements.
7. Demonstrate workplace learning	7.1 Learning opportunities are sought and managed based on job requirement and organization policy. 7.2 Improvement in performance is demonstrated based on courses attended. 7.3 Application of learning is demonstrated in both technical and non-technical aspects based on requirements of the job 7.4 Time and effort is invested in learning new skills based on job requirements 7.5 Initiative is taken to create more effective and efficient processes and procedures in line with workplace policy. 7.6 New systems are developed and maintained in accordance with the requirements of the job. 7.7 Awareness of personal role in workplace ***innovation*** is demonstrated based on requirements of the job.
8. Demonstrate problem solving skills	8.1 Creative, innovative and practical solutions are developed based on the problem 8.2 Independence and initiative in identifying and solving problems is demonstrated based on requirements of the job. 8.3 Team problems are solved as per the workplace

	guidelines 8.4 Problem solving strategies are applied as per the workplace guidelines 8.5 Problems are analyzed and assumptions tested as per the context of data and circumstances
9. Manage ethical performance	9.1 Policies and guidelines are observed as per the workplace requirements 9.2 Self-worth and professionalism is exercised in line with personal goals and organizational policies 9.3 Code of conduct is observed as per the workplace requirements 9.4 Integrity is demonstrated as per legal requirement

RANGE

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

Variable	**Range**
1. Drug and substance abuse may include but not limited to:	Commonly abused • Alcohol • Tobacco • Miraa • Over-the-counter drugs • Cocaine • Bhang • Glue
2. Feedback may include but not limited to:	• Verbal • Written • Informal • Formal
3. Relationships may include but not limited to:	• Man/Woman • Trainer/trainee • Employee/employer • Client/service provider • Husband/wife • Boy/girl • Parent/child • Sibling relationships
4. Forms of communication may include but not	• Written • Visual

limited to:	• Verbal • Non verbal • Formal and informal
5. Team may include but not limited to:	• Small work group • Staff in a section/department • Inter-agency group
6. Personal growth may include but not limited to:	• Growth in the job • Career mobility • Gains and exposure the job gives • Net workings • Benefits that accrue to the individual as a result of noteworthy performance
7. Personal objectives may include but not limited to:	• Long term • Short term • Broad • Specific
8. Trainings and career opportunities may includes but not limited to	• Participation in training programs • Serving as Resource Persons in conferences and workshops
9. Resource may include may but not limited to:	• Human • Financial • Technology
10. Innovation may include but not limited to:	• New ideas • Original ideas • Different ideas • Methods/procedures • Processes • New tools
11. Emerging issues may include but not limited to:	• Terrorism • Social media • National cohesion • Open offices
12. Range of media for learning may include but not limited to:	• Mentoring • peer support and networking • IT and courses

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Interpersonal
- Communication
- Critical thinking
- Organizational
- Negotiation
- Monitoring
- Evaluation
- Record keeping
- Problem solving
- Decision Making
- Resource utilization
- Resource mobilization

Required Knowledge

The individual needs to demonstrate knowledge of:

- Work values and ethics
- Company policies
- Company operations, procedures and standards
- Occupational Health and safety procedures
- Fundamental rights at work
- Workplace communication
- Concept of time
- Time management
- Decision making
- Types of resources
- Work planning
- Organizing work
- Monitoring and evaluation
- Record keeping
- Gender mainstreaming
- HIV and AIDS
- Drug and substance abuse
- Professional growth and development
- Technology in the workplace
- Innovation
- Emerging issues

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical	Assessment requires evidence that the candidate:

aspects of Competency	1.1 Conducted self-management 1.2 Demonstrated interpersonal communication 1.3 Demonstrated critical safe work habits 1.4 Demonstrated the ability to lead a workplace team 1.5 Planned and organized work 1.6 Maintained professional growth and development 1.7 Demonstrated workplace learning 1.8 Demonstrated problem solving skills 1.9 Demonstrated the ability to manage performance ethically
2. Resource Implications	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Written test 3.4 Portfolio of Evidence 3.5 Interview 3.6 Third party report
4. Context of Assessment	Competency may be assessed: 4.1 On-the-job 4.2 Off-the –job 4.3 During Industrial attachment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

DEMONSTRATE ENVIRONMENTAL LITERACY

UNIT CODE: SES/OS/CS/BC/05/6/A

UNIT DESCRIPTION

This unit specifies the competencies required to demonstrate environmental literacy. It involves, controlling environmental hazard and environmental pollution, demonstrating sustainable resource use, evaluating current practices in relation to resource usage, identifying environmental legislations/conventions for environmental concerns, implementing specific environmental programs, monitoring activities on environmental protection/Programs , analyzing resource use and developing resource conservation plans

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range***
1. Control environmental hazard	1. 1 Storage methods for environmentally hazardous materials are strictly followed according to environmental regulations and OSHS. 1. 2 Disposal methods of hazardous wastes are followed according to environmental regulations and OSHS. 1. 3 ***PPE*** is used according to OSHS.
2. Control environmental Pollution	2.1 Environmental pollution ***control measures*** are implemented in accordance with international protocols. 2.2 Procedures for solid waste management are observed according Environmental Management and Coordination Act 1999 2.3 Methods for minimizing noise pollution is complied with based on Noise and Excessive Vibration *Pollution and* Control *Regulations*, 2009
3. Demonstrate sustainable resource use	3.1 Methods for minimizing wastage are complied with based on organizational waste management guide 3.2 Waste management procedures are employed following principles of 3Rs (Reduce, Reuse,

	Recycle) 3.3 Methods for economizing and reducing resource consumption are practiced as per the Constitution of Kenya 2010 Article 69 .
4. Evaluate current practices in relation to resource usage	4.1 Information on resource efficiency systems and procedures are collected and provided as per work groups/sector 4.2 Current resource usage is measured and recorded as per work group 4.3 Current purchasing strategies are analyzed and recorded according to industry procedures. 4.4 Current work processes to access information and data is analyzed following enterprise protocol.
5. Identify environmental legislations/conventions for environmental concerns	5.1 Environmental legislations/conventions and local ordinances are identified according to the different environmental aspects/impact 5.2 Industrial standard/environmental practices are described according to the different environmental concerns
6. Implement specific environmental programs	6.1 Programs/Activities are identified according to organizations policies and guidelines. 6.2 Individual roles/responsibilities are determined and performed based on the activities identified. 6.3 Problems/constraints encountered are resolved in accordance with organizations' policies and guidelines 6.4 Stakeholders are consulted based on company guidelines
7. Monitor activities on Environmental protection/Programs	7.1 Activities are periodically monitored and Evaluated according to the objectives of the environmental program 7.2 Feedback from stakeholders are gathered and considered in Proposing enhancements to the program based on consultations 7.3 Data gathered are analyzed based on Evaluation requirements 7.4 Recommendations are submitted based on the findings 7.5 Management support systems are set/established to sustain and enhance the program 7.6 Environmental incidents are monitored and reported to

	7.7 concerned/proper authorities
8. Analyze resource use	8.1 All resource consuming processes are Identified as per the organizational work plan 8.2 Quantity and nature of resource consumed is determined based on processes 8.3 Resource flow is analyzed as per different parts of the process. 8.4 Wastes are classified according to NEMA regulations on waste management.
9. Develop resource Conservation plans	9.1. Efficiency of use/conversion of resources is determined according to industry protocol. 9.2. Causes of low efficiency of use of resources are Determined based on industry protocol. 9.3. Plans for increasing the efficiency of resource use are developed based on findings.

RANGE

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

Variable	**Range**
1. PPE may include but not limited to	• Mask • Gloves • Goggles • Safety hat • Overall • Hearing protector
2. Control measures may include but not limited to	• Methods for minimizing or stopping spread and ingestion of airborne particles • Methods for minimizing or stopping spread and ingestion of gases and fumes • Methods for minimizing or stopping spread and ingestion of liquid wastes

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Measuring
- Recording
- Analytical
- Monitoring
- Communication
- Writing

Required Knowledge

The individual needs to demonstrate knowledge of:

- PPEs
- Environmental regulations
- OSHS
- Pollution
- Waste management
- Principle of 3Rs
- Types of resources
- Techniques in measuring current usage of resources
- Environmental hazards
- Regulatory requirements

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Controlled environmental hazard 1.2 Controlled environmental pollution 1.3 Demonstrated sustainable resource use 1.4 Evaluated current practices in relation to resource usage 1.5 Demonstrated knowledge of environmental legislations and local ordinances according to the different environmental issues /concerns. 1.6 Described industrial standard environmental practices according to the different environmental issues/concerns. 1.7 Resolved problems/ constraints encountered based on management standard procedures 1.8 Implemented and monitored environmental practices on a periodic basis as per company guidelines 1.9 Recommended solutions for the improvement of the program 1.10 Monitored and reported to proper authorities any

	environmental incidents
2. Resource Implications	The following resources should be provided: 2.1 Workplace with storage facilities 2.2 Tools, materials and equipment relevant to the tasks (e.g. Cleaning tools, cleaning materials, trash bags) 2.3 PPE, manuals and references 2.4 Legislation, policies, procedures, protocols and local ordinances relating to environmental protection 2.5 Case studies/scenarios relating to environmental Protection
3 Methods of Assessment	Competency in this unit may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Written test 3.4 Portfolio of Evidence 3.5 Interview 3.6 Third party report
4 Context of Assessment	Competency may be assessed 4.1 On-the-job 4.2 Off-the –job 4.3 During Industrial attachment
5 Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

DEMONSTRATE OCCUPATIONAL SAFETY AND HEALTH PRACTICES

UNIT CODE: SES/OS/CS/BC/06/6/A

UNIT DESCRIPTION

This unit specifies the competencies required to demonstrate occupational health and safety practices. It involves identifying workplace hazards and risks, identifying and implementing appropriate control measures to hazards and risks and implementing OSH programs, procedures and policies/guidelines.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range***
1. Identify workplace hazards and risk	1.1 ***Hazards*** in the workplace are identified ***based their indicators*** 1.2 Risks and hazards are evaluated based on legal requirements. 1.3 ***OSH concerns*** raised by workers are addressed as per legal requirements.
2. Control OSH hazards	2.1 Hazard prevention ***and control measures*** are implemented as per legal requirement. 2.2 Risk assessment is conducted and a risk matrix developed based on likely impact. 2.3 ***Contingency measures***, including ***emergency procedures*** during workplace ***incidents and emergencies*** are recognized and established in accordance with organization procedures.
3. Implement OSH programs	3.1 Company OSH program are identified, evaluated and reviewed based on legal requirements. 3.2 Company OSH programs are implemented as per legal requirements. 3.3 Workers are capacity built on OSH standards and procedures as per legal requirements 3.4 ***OSH-related records*** are maintained as per legal requirements.

RANGE

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

Variable	Range
1. Hazards may include but not limited to:	• Physical hazards – impact, illumination, pressure, noise, • vibration, extreme temperature, radiation • Biological hazards- bacteria, viruses, plants, parasites, mites, molds, fungi, insects • Chemical hazards – dusts, fibers, mists, fumes, smoke, gasses, vapors • Ergonomics • Psychological factors – over exertion/ excessive force, awkward/static positions, fatigue, direct pressure, • varying metabolic cycles • Physiological factors – monotony, personal relationship, work out cycle • Safety hazards (unsafe workplace condition) – confined space, excavations, falling objects, gas leaks, electrical, poor storage of materials and waste, spillage, waste and debris • Unsafe workers' act (Smoking in off-limited areas, Substance and alcohol abuse at work)
2. Indicators may include but not limited to:	• Increased of incidents of accidents, injuries • Increased occurrence of sickness or health complaints/ symptoms • Common complaints of workers related to OSH • High absenteeism for work-related reasons
3. OSH concerns may include but not limited to:	• Workers' experience/observance on presence of work hazards • Unsafe/unhealthy administrative arrangements (prolonged work hours, no break time, constant overtime, scheduling of tasks) • Reasons for compliance/non-compliance to use of PPEs or other OSH procedures/policies/guidelines

4. Safety gears /PPE (Personal Protective Equipment) may include but not limited to:	• Arm/Hand guard, gloves • Eye protection (goggles, shield) • Hearing protection (ear muffs, ear plugs) • Hair Net/cap/bonnet • Hard hat • Face protection (mask, shield) • Apron/Gown/coverall/jump suit • Anti-static suits • High-visibility reflective vest
5. Appropriate risk controls may include but not limited to:	• Appropriate risk controls in order of impact are as follows: • Eliminate the hazard altogether (i.e., get rid of the dangerous machine) • Isolate the hazard from anyone who could be harmed (i.e., keep the machine in a closed room and operate it remotely; barricade an unsafe area off) • Substitute the hazard with a safer alternative (i.e., replace the machine with a safer one) • Use administrative controls to reduce the risk (i.e., train workers how to use equipment safely; train workers about the risks of harassment; issue signage) • Use engineering controls to reduce the risk (i.e., attach guards to the machine to protect users) • Use personal protective equipment (i.e., wear • gloves and goggles when using the machine)
6. Contingency measures may include but not limited to:	• Evacuation • Isolation • Decontamination • (Calling designed) emergency personnel
7. Incidents and emergencies may include but not limited to:	• Chemical spills • Equipment/vehicle accidents • Explosion • Fire • Gas leak • Injury to personnel • Structural collapse • Toxic and/or flammable vapors emission.

8. OSH-related Records may include but not limited to:	• Medical/Health records • Incident/accident reports • Sickness notifications/sick leave application • OSH-related trainings obtained

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Communication
- Interpersonal
- Presentation
- Risk assessment
- Evaluation
- Critical thinking
- Problem solving
- Negotiation

Required Knowledge

The individual needs to demonstrate knowledge of:

- General OSH Principles
- Occupational hazards/risks recognition
- OSH organizations providing services on OSH evaluation and/or work environment measurements (WEM)
- National OSH regulations; company OSH policies and protocols
- Systematic gathering of OSH issues and concerns
- General OSH principles
- National OSH regulations
- Company OSH and recording protocols, procedures and policies/guidelines
- Training and/or counseling methodologies and strategies

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Identified hazards in the workplace based their indicators 1.2 Evaluated workplace hazards based on legal requirements. 1.3 Addressed OSH concerns raised by workers as per legal requirements. 1.4 Implemented hazard prevention and control measures as per

	legal requirement. 1.5 Conducted risk assessment as per legal requirement. 1.6 Developed risk matrix based on likely impact. 1.7 Recognized and established contingency measures in accordance with organization procedures. 1.8 Identified, evaluated and reviewed company OSH program based on legal requirements. 1.9 Implemented company OSH programs as per legal requirements. 1.10 Capacity built workers on OSH standards and procedures as per legal requirements 1.11 Maintained OSH-related records as per legal requirements.
2. Resource Implications	The following resources should be provided: 2.3 Access to relevant workplace where assessment can take place 2.4 Appropriately simulated environment where assessment can take place
3. Methods of Assessment	Competency in this unit may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Written test 3.4 Portfolio of Evidence 3.5 Interview 3.6 Third party report
4. Context of Assessment	Competency may be assessed: 4.1 On-the-job 4.2 Off-the –job 4.3 During Industrial attachment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

COMMON UNITS OF COMPETENCY

DEMONSTRATE DIGITAL LITERACY

UNIT CODE: SEC/OS/CS/CC/01/6/A

UNIT DESCRIPTION

This unit covers the competencies required to demonstrate digital literacy. It involves identify appropriate computer software and hardware, applying security measures to data, hardware, and software in automated environment,computer software in solving tasks, internet and email in communication at workplace, desktop publishing in official assignments and preparing presentation packages.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace functions.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range***
1. Identify appropriate computer software and hardware.	1.1 Concepts of ICT are determined in accordance with computer equipment. 1.2 Classifications of computers are determined in accordance with manufacturer's specification. 1.3 Appropriate computer software is identified according to manufacturer's specification. 1.4 ***Appropriate computer hardware*** **is** identified according to manufacturer's specification. 1.5 Functions and commands of operating system are determined in accordance with manufacturer's specification.
2. Apply security measures to data, hardware, and software in automated environment.	2.1 ***Data security and privacy are classified*** in accordance with the prevailing technology. 2.2 ***Security threats*** are identified, ***and control measures*** are applied in accordance with laws governing protection of ICT. 2.3 Computer threats and crimes are detected. 2.4 Protection against computer crimes is undertaken in accordance with laws governing protection of ICT.
3. Apply computer software in solving tasks	3.1 ***Word processing concepts*** are applied in resolving workplace tasks, report writing and documentation. 3.2 Word processing utilities are applied in accordance with workplace procedures. 3.3 Worksheet layout is prepared in accordance with work procedures. 3.4 Worksheets are built, and data manipulated in the worksheets in accordance with workplace procedures. 3.5 Continuous data manipulated on worksheet is undertaken in accordance with work requirements 3.6 Database design and manipulation is undertaken in accordance with

ELEMENT These describe the key outcomes which make up workplace functions.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***Bold and italicized terms are elaborated in the Range***
	office procedures. 3.7 Data sorting, indexing, storage, retrieval and security is provided in accordance with workplace procedures.
4. Apply internet and email in communication at workplace.	4.1 Electronic mail addresses are opened and applied in workplace communication in accordance with organization ICT policy. 4.2 Office internet functions are defined and executed in accordance with office procedures. 4.3 Network configuration is determined in accordance with office operations procedures. 4.4 Security measures are put in place in line with the organization's ICT policy 4.5 Official World Wide Web is installed and managed according to workplace procedures.
5. Apply Desktop publishing in official assignments.	5.1 Desktop publishing functions and tools are identified in accordance with manufactures specifications. 5.2 Desktop publishing tools are developed in accordance with work requirements. 5.3 Desktop publishing tools are applied in accordance with workplace requirements. 5.4 Typeset work is enhanced in accordance with workplace standards.
6. Prepare presentation packages.	6.1 Types of presentation packages are identified in accordance with office requirements. 6.2 Slides are created and formulated in accordance with workplace procedures. 6.3 Slides are edited and run-in accordance with work procedures. 6.4 Slides and handouts are printed according to work requirements.

RANGE

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

Variable	Range
1. Appropriate computer Hardware may includes but not limited to:	• Computer case, monitor, keyboard, and mouse • hard disk drive • motherboard • video card.
2. Data security and privacy may includes but not limited to:	• Confidentiality of data. • Cloud computing. • Authenticity • Availability • Integrity • Non-repudiation • Integrity-but-curious data surfing.
3. Security and control measures may include but not limited to:	• Counter measures against cyber terrorism. • Risk reduction. • Cyber threat issues. • Risk management. • Pass-wording. • Authorization • Encryption
4. Security threats may includes but not limited to:	• Cyber terrorism. • Hacking.

REQUIRED SKILLS AND KNOWLEDGE

This section describes the skills and knowledge required for this unit of competency.

Required Skills

The individual needs to demonstrate the following skills:

- Analytical skills.
- Interpretation.
- Typing.
- Communication.
- Computing applying arithmetic operations.
- Basic ICT skills.

Required Knowledge

The individual needs to demonstrate knowledge of:

- Functions of computer software and hardware.
- Data security and privacy.
- Computer security threats and control measures.
- Technology underlying cyber-attacks and networks.
- Cyber terrorism and computer crimes.
- Detection and protection of computer crimes.
- Laws governing protection of ICT.
- Functions and concepts of word processing.
    - Documents and tables creation and manipulations.
    - Mail merging.
    - Word processing utilities.
- Spread sheets;
- Meaning, formulae, function and charts, uses and layout.
- Data formulation, manipulation and application to cells.
- Database;
- Database design, data manipulation, sorting, indexing, storage retrieval and security
- Desktop publishing;
- Designing and developing desktop publishing tools.
- Manipulation of desktop publishing tools.
- Enhancement of typeset work and printing documents.
- Presentation Packages;
- Types of presentation packages.
- Creating, formulating, running, editing, printing and presenting slides and handouts.
- Networking and Internet;
- Computer networking and internet.
- Electronic mail and World Wide Web.
- Emerging trends and issues in ICT;

- Identify and integrate emerging trends and issues in ICT.
- Challenges posed by emerging trends and issues.

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge and range.

1. Critical Aspects of Competency.	Assessment requires evidence that the candidate: 1.1 Identified and controlled security threats. 1.2 Detected and protected computer crimes. 1.3 Applied word processing in office tasks. 1.4 Designed, prepared work sheet and applied data to the cells in accordance to workplace procedures. 1.5 Opened electronic mail for office communication as per workplace procedure. 1.6 Installed internet and World Wide Web for office tasks in accordance with office procedures. 1.7 Integrated emerging issues in computer ICT applications. 1.8 Applied laws governing protection of ICT.
2. Resource Implications for competence assessment	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment.	Competency may be assessed through: 3.1 Written Test. 3.2 Demonstration. 3.3 Practical assignment. 3.4 Interview/Oral Questioning. 3.5 Demonstration.
4. Context of Assessment.	Competency may be assessed in an off and on the job setting.
5. Guidance information for assessment.	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

CORE UNITS OF COMPETENCY

PERFORM COMPUTER REPAIR AND MAINTENANCE

UNIT CODE: SEC/OS/CS/CR/01/6/A

UNIT DESCRIPTION

This unit covers the competencies required to perform computer repair and maintenance. It involves performing troubleshooting, dismantling faulty components, repairing/replacing faulty components, upgrading computer software/hardware, and preparing and documenting maintenance reports.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Perform troubleshooting	1.1 Performance issues in the machine are identified as per the workplace procedures 1.2 ***Hardware and software are*** diagnosed in line with the standard operating procedure 1.3 Testing and troubleshooting tools are established as pert the industry best practices
2. Dismantle faulty components	2.1 Components to be dismantled are identified 2.2 Components are dismantled in line with the manufacturer's manuals 2.3 Dismantling tools and components are established in standard operating procedures 2.4 Component handling is aligned to the standard operating procedures
3. Repair/Replace faulty components	3.1 Diagnostic tools and instruments are identified as per the workplace policy 3.2 Components functionality is tested as per the manufacturer's manuals 3.3 Test parameters are compared with the expected output in line with the manufacturer's manuals 3.4 Faulty components are identified and removed as per the standard operating procedure 3.5 Faulty components are repaired/replaced in line with manufacturers manuals 3.6 Repaired/replaced components are tested for their functionality according to standard operating procedure

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	3.7 Components are reassembled, and continuous monitoring performed as per the industries best practice
4. Upgrade computer hardware/software	4.1 Tools in managing software updates are established as per the industry best practice 4.2 Test environment is developed for hardware and software as per industry best practices 4.3 Licensed software and hardware are used in computer upgrades as per the organizations ICT policy 4.4 Schedule updates in lines with the organization policy 4.5 Upgraded computer hardware and software are tested in line with the organization policy
5. Prepare and document maintenance report	5.1 Maintenance report is prepared in line with the organizations approved format 5.2 Maintenance report is shared with the relevant parties 5.3 Prepared report is filed as per the organizations policy

RANGE

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

Variable	Range
1. Hardware may include but not limited to:	• Desktops • Central process unit (CPU) • Laptops • Mobile phones • Server boxes • Hard drives • Routers • Switches
2. Software may include but not limited to:	• Preventive • Detective

Variable	Range
	• Responsive

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

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

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:	
• Communications (verbal and written); • Time management; • Penetration Skills • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Diagnosed software and hardware in line with the standard operating procedure 1.2 Dismantled components in line with the manufacture's manuals 1.3 Tested components functionality as per the manufacturer's manuals 1.4 Tested repaired/replaced components functionality according to standard operating procedure 1.5 Monitoring reassembled components as per the industries best practice 1.6 Test environment was developed for hardware and software as per industry best practices 1.7 Prepared maintenance report in line with organizations

	approved format 1.8 Tested upgraded computer hardware and software were tested in line with the organization policy 1.9 Security threats were identified and classified as per the organization ICT policy 1.10 Security control measures were identified and categorized
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Practical test in conducting test 3.4 Demonstration of interpretation of test results
4. Context of Assessment	Competency may be assessed individually 4.1 In the actual workplace 4.2 Simulated environment of the work place
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

DEMONSTRATE UNDERSTANDING OF CYBER SECURITY LAWS, POLICIES AND REGULATIONS

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

UNIT DESCRIPTION

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

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
1. Demonstrate understanding of cyber security laws, polices and regulation	1.1 Different cyber security laws are identified based on the available world's legal systems. 1.2 Various types of cyber-crimes are identified based on the existing and emerging treaths 1.3 Cyber crime laws are identified based on the country's legal framework. 1.4 Cyber security laws are applied as per the country's legal system 1.5 Cyber security laws are complied with as per the organizations or country's legal framework. 1.6 Impacts of cyber crimes are identified according to country's social economic factors 1.7 Application of different cyber security policies are determined as per the industry best practice 1.8 Policies and regulation stakeholders are identified
2. Develop Cyber Security policy	2.1 ***Infrastructure and components*** for cyber security policy are identified and classified 2.2 Nature and operations of the business aligned to the policy is established 2.3 Draft cyber security policy is developed in line with the known industrial standards and the laws of the land 2.4 Review drafted cyber security policy in line with the industry best practice
3. Implement Cyber Security	3.1 Cyber security policy is adopted for implementation as per the organization requirements

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
policy and regulations	3.2 Cyber security policy implementation team is constituted in line with the organization requirements 3.3 Implementation schedule is prepared as per the organization requirement 3.4 Initiation of the cyber security policy implementation schedule is performed in line with organization policies 3.5 Cyber security policy implementation process is monitored in line with the established schedule 3.6 Cyber security policy and regulation implementation is verified as per the substantive law and organization policies
4. Evaluate Cyber security policy	4.1 Continuous review and updates of cyber security policy is performed in line with organization requirements 4.2 Cyber security policy is evaluated in line with the cyber security emerging trends
5. Evaluate compliance in Cyber security policy and regulations	5.1 ***Infrastructure landscape*** is audited in line with the organization Cyber security policy and regulations 5.2 Risk factors for non-compliance are calculate as per the industry best standards 5.3 Recommendation is reported on the compliance level as per the policy and regulations
6. Monitor effectiveness of Cyber security policy in an organization	6.1 Adoption levels are determined in line with organization requirements 6.2 Cyber security policy impact on technologies, process and people within the organization is monitored as per the organization policy. 6.3 Effectiveness of the Cyber security policy implemented is monitored in line with organization requirement

RANGE

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

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

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- Cyber security infrastructure auditing procedures
- Cyber security safety and precautious measures
- Cyber security prevention measures
- Performance monitoring techniques
- Cyber security policy
- Causes of hardware and software failure
- Components of cyber security infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Identified different types of cyber security policies and regulations 1.2 Determined application of different cyber security policies as per the industry best practice 1.3 Developed a draft of cyber security policy in line with the known industrial standards and the laws of the land 1.4 Prepared implementation schedule as per the organization requirement 1.5 Evaluated cyber security policy line with the cyber security trends 1.6 Calculated risk factors for non-compliance as per the industry best standards

	1.7 Reported recommendations on the compliance level as per the policy and regulations 1.8 Monitored Cyber security policy impact on technologies, process and people within the organization as per the organization policy 1.9 Monitored effectiveness of the Cyber security policy implementation in line with the organization requirement 1.10 Performed audit on existing cyber security components and infrastructure 1.11 Verified drafted cyber security policy in line with the standard operating procedure
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Written tests 3.3 Practical demonstration 3.4 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

PERFORM COMPUTER NETWORKING

UNIT CODE: SEC/OS/CS/CR/03/6 **/A**

UNIT DESCRIPTION

This unit covers the competencies required to perform computer networking activities. It involves identifying network types, configuring network devices, connecting network devices, monitoring network performance, documenting network report, training network users and maintaining of the network.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Identify network type	1.1. Site survey is conducted to determine the user needs and establish ***network topology*** 1.2. Network design is developed according to the site survey 1.3. ***Network components*** are identified according to the site survey 1.4. Network type is identified as per the client's requirements
2. Configure network devices	2.1.Network is installed and configured according to network installation manual. 2.2.IP addressing scheme, subnet masking and routing ***protocol*** configuration is performed 2.3.Network segmentation is determined as per the Network design. 2.4.Network privileges are allocated according to the network configuration. 2.5.***Network types*** are configured as per the type of connection
3. Connect network devices	3.1.Tools, materials and devices for network are identified according to the network type 3.2.Network connection is performed according to National and international communication standards and protocols 3.3.Stability and connectivity tests of cables and equipment is done as per the network type 3.4. Media management is performed as per the industry best practice

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
4. Monitor Network performance	4.1. Network ***monitoring tools*** are identified as per the type of tests to be carried out 4.2. Network monitoring tools are deployed as per the network connection type. 4.3. Network status is determined as per the monitoring report. 4.4. Network is monitored in line with its operation manual
5. Document network report	5.2 Networking report is prepared and filed in the approved format as per the organization policy 5.3 Networking report is shared with the relevant parties 5.4 Test results are document as per the organizations policy 5.5 Network reports are stored in the in the relevant department for reference purpose as per the organization policy
6. Train network users	6.1. Network user are trained on its operation in line with its installation manual 6.2. Users are identified as per the network coverage 6.3. Users are provided with the network operation manual 6.4. User training manuals are prepared according to network functionality 6.5. User training is done according to the user training manual
7. Maintain Network	7.1. Network is optimized between the network components and medium in line with the operation manual. 7.2. Network security is applied according to vulnerability of the Network. 7.3. Maintenance schedule is prepared as per the task to be carried out. 7.4. Network updates are scheduled as per the organization policy

RANGE

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

Variable	Range
1. Network topology includes but not limited to:	• Star • Ring • Mesh • Hybrid • Point to point
2. Network components includes but not limited to:	• Routers • Switches • Hub • RJ 45 connectors • Ports • Computers • Printers
3. Network protocols includes but not limited to:	• TCPIP • UDP • HTT
4. Network security Measures includes but not limited to:	• Intrusion detection systems • Patching and Updating • Port Scanners • Network Sniffers • Vulnerability scanners • Antiviruses
5. Network types includes but not limited to:	• WAN • LAN • PAN
6. Monitoring tools includes but not limited to:	• Ping • Tracert • Speed test
7. Network software includes but not limited to:	• NetFlow • Active Directory • Telnet • Wireshark

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Network Architecture
- Network programming languages
- Network Components and devices
- Network types
- Network security Measures
- Network Monitoring procedures
- Network testing techniques
- Network configuration techniques
- Network protocols
- Network security techniques and procedures
- Network testing procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:

- Communications (verbal and written);
- Proficient in ICT;
- Problem solving
- Decision Making
- Leadership
- Self-training

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Conducted site survey on determining the user needs and establishing of network topology 1.2 Developed network design in line with the site survey 1.3 Performed IP addressing scheme, subnet masking and routing protocol configuration of the network 1.4 Network privileges are allocated according to the network configuration. 1.5 Performed network connection according to the National and international communication standards 1.6 Identified network monitoring as per the type of tests that were to be carried out 1.7 Monitored network protocols in line with its operation manual 1.8 Prepared and filled network report in line with the approved format of the organization

	1.9 Prepared user training manuals according to the software functionality 1.10 Applied network security according to the vulnerability of the Network 1.11Components were identified during site survey
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Practical demonstration
4. Context of Assessment	Competency may be assessed individually in the actual workplace and simulated setting of the actual work place
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

BUILD SECURE NETWORK

UNIT CODE: SEC/OS/CS/CR/04/6/A

UNIT DESCRIPTION

This unit covers the competencies required in building secure network. It involves confirming user requirements and network equipment, reviewing security issues, analyzing network security protocols and features, designing and perimeters, installing and configuring perimeter solutions, configuring internal network devices, testing and verifying design performance and preparing network report.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
1. Confirm user requirements and network equipment	1.1 Network use is identified as per the organizations ICT policy and industry best practices 1.2 Equipment and network topology are established in line with workplace procedures 1.3 Network speed is established as per its source 1.4 Number of network users are determined in line with organization requirement 1.5 Perimeter type is identified as per the organization requirements 1.6 Security perimeters is established from the organization's objectives
2. Review security issues	2.1 Security threats in the organization are identified as per the its set up 2.2 Security issues are reviewed as per the industry best practices 2.3 Security control measures in the organization are identified in line with the ICT policy
3. Analyse network security protocols and features	3.1 Types of network security protocols are identified as per the industry best practice 3.2 Application of network security protocols are established in line with the industry best practice 3.3 Required network security protocols are established as per the client's requirements
4. Plan and design perimeter solution	4.1 Perimeter solution is designed as per the expected use and industry best practices 4.2 Perimeter schedule is designed in line with the organization ICT policy

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
	4.3 Perimeter design is approved as per the clients requirements 4.4 Perimeter design is tested for its functionality as per the expected objectives
5. Install and configure perimeter solutions	5.1 Perimeter solution system is acquired in line with the design 5.2 System is installed as per the design and the organization ICT policy 5.3 System is configured as per the manufacturers guidelines 5.4 Perimeter solution installed is tested as per the organization ICT policy 5.5 Parameters to be configured are identified as per the design
6. Configure internal network devices	6.1 Devices to be configured are identified from the system design 6.2 Internal devices compatibility are compared with the designed system 6.3 Internal network devices are configured as per manufacturers guidelines 6.4 Network devices are integrated to the security perimeter as per the organization ICT policy
7. Test and verify design performance	7.1 Types of tests are identified as per the systems efficiency 7.2 System performance test is conducted according to workplace procedures 7.3 Errors are checked and debugged as per the design 7.4 Threats are simulated in performance verification as per the work place procedures 7.5 Continuous monitoring of security perimeter performance is conducted as per the organization policy
8. Prepare network report	8.1 Network reports are prepared in line with the organizations approved format 8.2 Network reports are shared with relevant parties as per the organization policy 8.3 Network reports are documented and filled according organization filing system

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
	8.4 Network design recommendations are prepared and shared with the relevant parties

RANGE

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

Variable	Range
1. ICT components and infrastructure may include but not limited to:	• Software • Hardware • People • Data • Procedures • Information

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Identified perimeter type as per the organization requirements 1.2 Identified security threats in the organization as per its set up 1.3 Identified security control measures in the organization in line with the ICT policy 1.4 Types of network security protocols are identified as per the industry best practice 1.5 Designed perimeter solution with self-defensive mechanism 1.6 Tested perimeter design functionality as per the organization objectives 1.7 Configured the system as per the manufacturers guidelines 1.8 Installed perimeter solution was tested as per the organization ICT policy 1.9 Configured internal network devices as per manufacturers guidelines 1.10 Integrated network devices to the security perimeter as per the organization ICT policy
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of	Competency may be assessed individually in the actual

Assessment	workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

DEVELOP COMPUTER SOFTWARE

UNIT CODE: SEC/OS/CS/CR/05/6/A

UNIT DESCRIPTION

This unit covers the competencies required to develop computer software. It involves establishing software purpose, analysing software requirements, designing computer software, developing computer software, performing programme testing and maintenance.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Establish software purpose	1.1 Software are classified according to their functionality. 1.2 Software is determined in line with the scope of the work to be performed. 1.3 Criteria for selection of software is identified based on user requirements and functionality 1.4 ***Software acquisition methods*** are established as per the functionality
2. Analyse software requirement	2.1 ***Software specifications*** are determined as per their functionality. 2.2 Computer resource requirements are established in line with software requirements 2.3 Source of software installation files is determined according to the platform 2.4 User vendor agreements are identified according to the Installation manual.
3. Design computer software	3.1 Software is designed as per the client's requirement and industry best practice 3.2 Design is performed in line with the scope of the work and complexity of the software 3.3 Software security is considered in the design of the software in line with standard operating procedures 3.4 Software is designed in compatibility with the installation devices 3.5 Required ***software parameters*** are set as per the

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	software manual.
4. Develop computer software	4.1 Coding of the software is performed as per the design 4.2 Test and debugging of errors is performed as per the software performance 4.3 Software is developed as per the scope of the task to be handled.
5. Perform programme testing	5.1 Software performance is tested for its functionality as per standard operating procedures. 5.2 Software security test is performed as per the design manual 5.3 Software is tested, and errors debugged as per the standard operating procedure. 5.4 Software configuration is performed as per the set parameters 5.5 Test report is generated as per the test results obtained 5.6 Software auditing is performed for quality assurance in line with industry's best practice 5.7 Software implementation is performed as per the set parameters
6. Perform software maintenance	6.1 Software maintenance schedule is established in line with standard operating procedures 6.2 ***Software upgrades and modules patches*** are applied according to the developer's manual 6.3 Software revisions are performed to correspond with functionality changes in line with the organization requirements 6.4 Software monitoring is established in line with industry's best practices

RANGE

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

Variable	Range

Software acquisition methods may include but not limited to:	• In – house developed • Tailor made • Outsourced
Software specifications may includebut not limited to:	• Usually has the following characteristics: • Performance rate • Speed • Security • Complete. • Consistent. • Feasible. • Modifiable. • Unambiguous. • Testable

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Operating systems
- Types of operating systems
- Software security
- Software development life cycle
- Relevant organization ICT policy
- Software installation legal requirements
- Types of software installation
- Types of Software testing
- Software installation techniques
- Software Upgrading and Patching
- Software Acquisition Methods
- Software Maintenance Procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:
• Communications (verbal and written); • Troubleshooting • Problem solving; • Decision making; • Planning; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required knowledge and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Tested software functionality as per standard operating procedures. 1.2 Classified software according to their functionality. 1.3 Established computer resources in line with software requirements 1.4 Designed software as per the client's requirement and standard operating procedures 1.5 Considered software security in the its design 1.6 Performed software coding as per the design 1.7 Audited software quality assurance as per the industry's best practice 1.8 Configured software as per the set parameters and operation manufacturers manuals 1.9 Prepared software maintenance schedule in line with standard operating procedures 1.10 Performed software testing 1.11 User training manuals was prepared according to software functionality.
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Observation with the help of check list 3.2 Practical demonstrations 3.3 Oral Questioning
4. Context of Assessment	Competency may be assessed individually in the actual workplace or a simulated work place setting
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

SECURE SOFTWARE APPLICATION

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

UNIT DESCRIPTION

This unit covers the competencies required to secure software application. It involves identifying software to be secured, establishing tools for application security assessment, perform application security assessment, hardening software application, monitoring application security performance, performing application security configuration and preparation of reports on software security.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Identify software to be secured	1.1 Software is identified in line with manufacturers 1.2 Software use is established as per its applications 1.3 Software platform diversity is established according to manufactures user guides
2. Establish tools for application security assessment	2.1 Types of tools are identified according to the platform of use 2.2 Network communication is adhered to in tools identification 2.3 Tools are identified as per their availability and cost 2.4 Tools are identified as per the data size 2.5 Tools are identified according to the environment of use. 2.6 Tools identification is performed as per the nature of the software 2.7 Tools are established as per the type of hardware and software 2.8 Tools are selected as per the expected outcome of the application security assessment.
3. Perform application security assessment	3.1 Application assessment is performed in line with national and international standards 3.2 Application assessment is conducted as per the ISO 27001 3.3 Assessment is performed in line with NIST
4. Harden software application	4.1 Configuration is performed as per the manufacturers guide, ICT regulations and industries best practice 4.2 Security measures are put around the software

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	according ICT policy 4.3 Access control measures are set up in line organizations ICT policy 4.4 Valid licenses are installed in software as per the manufacturer's guides 4.5 Software is monitored continuously as per its operations 4.6 Security updates and patches are installed in line with manufacturers guidelines 4.7 Environment of software use is secured as per the organization policy
5. Monitor application security performance	5.1 Monitoring solution is implemented in line with organization policy 5.2 Logs are monitored as per the organization ICT policy 5.3 Continuous security assessment is conducted as per the industries best practice 5.4 Application security performance is measured in line with its uptime period
6. Prepare a report on software security	6.1 Software security reports are prepared in line with the organizations approved format 6.2 Software security reports are shared with relevant parties as per the organization policy 6.3 Software security reports are documented and filled according organization filing system 6.4 Software security risk mitigation recommendations are prepared and shared with the relevant parties

RANGE

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

Variable	Range

Variable	Range
ICT components and infrastructure may include but not limited to:	• Software • Hardware • People • Data • Procedures • Information

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects	Assessment requires evidence that the candidate:

of Competency	1.1 Software was identified in line with manufacturers 1.2 Software use was established as per its applications 1.3 Tool's identification was performed as per the nature of the software 1.4 Application assessment was performed in line with OWASP 1.5 Configuration was performed as per the manufactures guide, ICT regulations and industries best practice 1.6 Valid licenses were installed in software as per the manufacturer's guides 1.7 Security updates and patches were installed in line with manufacturers guidelines 1.8 SIEM solution was implemented in line with organization policy 1.9 Software security reports were shared with relevant parties as per the organization policy 1.10 Environment of software use is secured as per the organization policy
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

SECURE DATABASES

UNIT CODE: SEC/OS/CS/CR/07/6/A

UNIT DESCRIPTION

This unit covers the competencies required to secure databases. It involves identifying types of databases, identifying database threats and vulnerabilities, installing database patches, installing database security management system, monitoring database security, monitoring access control and managing database backups.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Identify types of databases	1.1 Database type is identified as per the types of data it holds 1.2 Database is established as per the amount of data it holds 1.3 Database is classified as per its distribution 1.4 Database type is determined in line with the number of users 1.5 Database is identified as per its operational model 1.6 Cost evaluation is adhered to in database type identification
2. Identify database threats and vulnerabilities	2.1 Database tests are performed as per the manufacturers manual 2.2 Security vulnerabilities and exposures updates are assessed as per the standard operation procedures 2.3 Database is checked for misconfiguration as per the manufacturers guide
3. Install databases patches	3.1 Required patches are identified and acquired as per manufacturers guidelines 3.2 Required patches are verified as per the manufacture's guidelines 3.3 Database patches are deployed in a test environment as per the organization quality assurance policy. 3.4 Database patches are monitored as per the ICT policy 3.5 Database patches are deployed in the production environment as per the organization policy.
4. Install database security	4.1 Type of database security management system is established as per the client's requirements

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
management systems	4.2 Security management system is established in line with the deployment model 4.3 Hardware sizing is performed in line with database to be secured 4.4 Security management system is installed and configured according to manufacturer's manual 4.5 Security management system is verified as per the guidelines in database security management system set up. 4.6 System integration is performed as per the manufacturers manual and client's requirement
5. Monitor database security	5.1 Logs are collected and analysed as per the standard operating procedure 5.2 Failed log in attempts is monitored as per system operation 5.3 Database firewall is configured as per the database expected operation 5.4 Remote access is monitored as per database operation 5.5 Odd hours database access monitored as per the its operation 5.6 Change in user access patterns is monitored in with the operation of the database 5.7 Random change in size of the database is monitored as per its normal size. 5.8 File configuration changes are monitored as per database operation.
6. Manage access control	6.1 Failed log in attempts is identified as per the system operation 6.2 Privilege account abuse is checked as per the access control policy 6.3 Users access control is managed in line with the least privileged principle 6.4 Active directory rules are adhered to in database access 6.5 Database is accessed by allowed devices as per the organizations policy 6.6 Obfuscation is adhered to in database access

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	6.7 Database auditing system is established as per the nature of the data to be secured
7. Manage database backups	7.1 Automatic backups are scheduled as per the ICT policy and regulations 7.2 Backups are managed in line with the organization ICT policy and industry best practice 7.3 Database backups are updated as per the ICT policy 7.4 Backups are stored as per the organization set up and industry best practice 7.5 Backups are regularly checked in line with the ICT policy 7.6 Identify and manage backup solutions in line with the organization policy

RANGE

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

Variable	Range
Cyber security components and infrastructure includes but not limited to:	• Software • Hardware • People • Data • Procedures • Information
Distribution includes but not limited to:	• Open source • Closed source

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures

• ICT safety and precautious measures • ICT Prevention measures • Performance monitoring techniques • ICT policy • Causes of hardware and software failure • Components of ICT Infrastructure • User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Faults troubleshooting • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Database was established as per amount of data it holds 1.2 Database was identified as per its operation model 1.3 Cost evaluation was performed in database type identification 1.4 Database was checked for misconfiguration in line with the manufacturers guide 1.5 Database patches were deployed in a test environment as per the organization quality assurance policy. 1.6 Database patches were monitored as per the ICT policy 1.7 Hardware sizing was performed in line with database to be secured 1.8 Database firewall was configured as per the database expected operation

	1.9 Automatic backups were scheduled as per the ICT policy and regulations 1.10 Backups were managed in line with the organization ICT policy and industry best practice 1.11 Backups were stored as per the organization set up and industry best practice
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

INSTALL CYBER SECURITY SYSTEM

UNIT CODE: SEC/OS/CS/CR/08/6/A

UNIT DESCRIPTION

This unit covers the competencies required to Install cyber security system. It involves identifying and analysing information to be protected, establishing systems to be installed, assessing system compatibility, installing established systems, performing system testing and debugging, monitoring system performance, documenting system installation report, establishing a cyber security backup and restoration plan and conducting training of the system users.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
1. Identify and analyze information to be protected	1.1 Platform of the information location is established as per the organization policy 1.2 Information attributes of the organization is determined in line with the organization policy 1.3 Technology used in information storage is established as per the organization policy 1.4 Information access control is established in line with organization policy 1.5 Information or data to be protected is analyzed in line with the Cyber security policy and regulations
2. Establish systems to be installed	2.1 System is established as per the scope of the information to be protected 2.2 Existing ***threats*** and trends are considered in establishing the security system to be installed as per the industry best practice 2.3 Hardware and software requirements are established in line with the system to be installed
3. Asses system's compatibility	3.1 Cyber security system is assessed for compatibility with the cyber security devices and equipment 3.2 Component's specification are checked in line with the entire cyber security system 3.3 System is assessed in line with the manufacturers manual and organizations objectives
4. Install established systems	4.1 ***Security system*** is acquired in line with the specification and compatibility established 4.2 Relevant installation tools and equipment are

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
	identified as per the industry best practice 4.3 **System** installation schedule is prepared as per the nature of the job 4.4 System installation and configuration is performed as per the manufacturers manual 4.5 System is configured in line with the organizations cyber security policy
5. Perform systems testing and debugging	5.1 Types of test on the system are established as per the standard operating procedure 5.2 System is tested as per the organization policy 5.3 Errors identified during system testing are troubleshooted
6. Monitor system performance	6.1 System effectiveness is monitored periodically in line with the operation manual and cyber security policy 6.2 Simulations are performed during system monitoring period as per the organization policy 6.3 Logs are continuously analysed and reported as per the organization cyber security policy 6.4 System security updates and patches are installed according to manufacturer's manuals and organization cyber security policy
7. Document system installation report	7.1 Installation and operation report are prepared and shared with the relevant parties 7.2 Prepared report is filled as per the organizations cyber security policy
8. Establish a cyber security back up and restoration plan	8.1 Location for the backup is identified as per the organization policy and industry best practice 8.2 Information to be backed up is established as per the organization cyber security policy 8.3 Back up platform is established in line with the organization policy 8.4 Performance validation of the backups is performed as per the organization cyber security policy 8.5 Measures on creating backup schedules are developed in line with the industry best practice
9. Conduct training of system users	9.1 Users of the Installed security system are trained on the performance of the system

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements ***(Bold and italicised terms are elaborated in the Range)***
	9.2 Training manual is prepared and shared with the system users 9.3 Operation manuals are strategically filed for easier access by the system users

RANGE

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

Variable	Range
1. Security threats may include but not limited to:	• Malicious hackers • Industrial espionage • Employee sabotage • Fraud and theft • Loss of physical and infrastructure support • Errors and Omissions
2. Security control measure may include but not limited to:	• Preventive • Detective • Responsive
3. Cyber Security system may include but not limited to:	• Knowledge management system • Firewall's instruction detection system

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Cyber Security risk management techniques and procedures

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

FOUNDATION SKILLS

The individual needs to demonstrate the following foundation skills:	
• Communications (verbal and written); • Time management; • Penetration Skills • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1 Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Considered existing threats and trends in establishing the security system to be installed 1.2 System to be installed was established with self-defensive mechanism 1.3 Components specification were checked in line with the entire cyber security system 1.4 System was installed and configured as per the manufacturers manual 1.5 Established testing types as per the standard operating procedure 1.6 Performed simulations during system monitoring period as per the organization policy 1.7 Continuously analysed logs and reported as per the organization cyber security policy 1.8 Establish back up platforms in line with the organization policy 1.9 Performed validation of the backups as per the organization ICT policy 1.10 Developed back up schedule as per the organization cyber

	security policy 1.11 Training manual was prepared and shared with the system users
2 Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3 Methods of Assessment	Competency may be assessed through: 3.1 Observation 3.2 Oral questioning 3.3 Practical test in conducting test 3.4 Demonstration of interpretation of test results
4 Context of Assessment	Competency may be assessed individually 4.1 In the actual workplace 4.2 Simulated environment of the work place
5 Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

MANAGE CYBER SECURITY RISKS

UNIT CODE: SEC/OS/CS/CR/09/6/A

UNIT DESCRIPTION

This unit covers the competencies required to manage cyber security risks. It involves establishing risk context, identify risk factors, implementing contingency plans, monitoring and updating risk profiles and reporting of risk profiles.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Establish Risk context	1.1 ***Infrastructure*** is identified as per the organizations network scope 1.2 Types of assets used in the organization are established in line with the size of the organization 1.3 Organization's security awareness is established in line with its staff 1.4 Risk context is established as per the organizations cyber security policies
2. Identify Risk factors	2.1 Risk factors are identified as per the organization cyber security policy 2.2 Risk factors are assessed in line with the manufacturer's manuals 2.3 Risk factors are identified as per the organizations ICT policy and cyber security related equipment 2.4 Risk factors are classified as per their impact 2.5 Information access is assessed as per the organization policy 2.6 Risk factors are identified according to National and international standards
3. Implement contingency plans	3.1 ***Contingency plans*** are implemented as per the systems operation manuals 3.2 Back up measures are implemented as per the organization policy 3.3 Data loss prevention measures are implemented according to organization policy and rules and regulation 3.4 Communication contingency plans are adhered to in sharing of the information within and outside the

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	organization 3.5 Intrusion detection and prevention measures are implemented according to organization best practices. 3.6 Contingency plans are simulated in adherence to the expected efficiency
4. Monitor and update risk profile	4.1 Risk calculation is performed as per the standard operating procedures 4.2 Automated security operation centres and monitor the risk factors as per the standard operating procedures 4.3 System users are continuously trained on trends in cyber security issues in line with the organizations policy 4.4 Risk profile is updated in line with simulated risk factors 4.5 Risk monitoring and updates are performed according to systems manufacturer's security updates
5. Report risk profile	5.1 Risk reports are prepared in line with the organizations approved format 5.2 Risk reports are shared with relevant parties as per the organization policy 5.3 Risk reports are documented and filled according organization filing system 5.4 Risk mitigation recommendations are prepared and shared with the relevant parties

RANGE

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

Variable	Range
1. infrastructure may	• People • Data

Variable	Range
include but not limited to:	• Procedures • Information
2. Contingency plans may include but not limited to:	• Incidence response • Cyber threats intelligence • Business continuity plans • Disaster recovery plans • Back up stratey

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures
- Government ICT policies and regulations
- Government policies and regulation
- Applicable laws and regulations

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Faults troubleshooting • Problem solving; • Planning;	• Decision making; • Report writing; • Creativity • Self-driven

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Risk assets established as per the organizations cyber security policy 1.2 Organization security awareness established as per its staff 1.3 Risk assets assessed in line with manufacturers manual 1.4 Information access is assessed as per the organization policy 1.5 Contingency plans implemented as per system operating manual 1.6 Implemented back up measures as per the organization policy 1.7 Implemented data loss prevention measures according to organization policy and rules and regulation 1.8 Performed risk calculations as per the standard operating procedures 1.9 Updated risk profile in line with simulated risk factors 1.10 Risk reports are documented risk reports and filled according to organization filing system
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

CONDUCT CYBER SECURITY ASSESSMENT AND TESTING

UNIT CODE: SEC/OS/CS/CR/10/6/A

UNIT DESCRIPTION

This unit covers the competencies required to conduct security assessment and testing. It involves gathering information about organization and its systems, scan and mapping of network, enumerating network resources, exploiting known vulnerabilities, performing social engineering and preparing security assessment and testing report.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Gather information about organization and its systems	1.1 Types of information required is established according line with the industry best practice 1.2 The nature of the target is determined in line with the information required 1.3 Search engines are considered in information gathering 1.4 Information gathering is conducted in adherence to the target social engineering 1.5 Information gathering is conducted in line with manufacturers guide of the source of the information 1.6 Organization operation platform is established in line industry best practice
2. Scan and map the network	2.1 Live hosts are identified as per the standard operation procedure 2.2 Network topology is drawn based on industry best practice 2.3 Services running on the live hosts are identified in line industry best practices 2.4 Vulnerable points are identified as per the services on the host
3. Enumerate target resources	3.1 Users are identified as per the standard operating procedure 3.2 Authorization credentials are established as per the organization ICT policy 3.3 Enumeration in services are established based on the organization policy

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	3.4 Protocols enumeration is performed as per the standard operating procedure 3.5 Work groups are established in line with the network and active directory 3.6 Database is enumerated in line with industry best practice 3.7 Rainbow tables are designed based on industry best practice
4. Exploit known vulnerabilities	4.1 Exploits are deployed in line with industry best practice 4.2 Payloads are prepared and deployed in line with the environment and industry best practice and ethics 4.3 Deploying methods are established in line with the expected target 4.4 Access to remote host is maintained per standard operating procedure 4.5 Exploitation proof of concept is generated in line with the standard operating procedure
5. Perform social engineering	5.1 Methods of manipulating human emotion are exercised as per workplace procedures 5.2 System users are manipulated using the system as per the industry best practice 5.3 System is manipulated using third party vendors in line with industry best practice
6. Prepare security assessment and testing report	6.1 Security assessment and testing reports are prepared in line with the organizations approved format 6.2 Security assessment and testing reports are shared with relevant parties as per the organization policy 6.3 Security assessment and testing reports are documented and filled according organization filing system 6.4 Security assessment and testing risk mitigation recommendations are prepared and shared with the relevant parties

RANGE

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

Variable	Range
	•

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:	
• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Faults troubleshooting • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects	Assessment requires evidence that the candidate:

of Competency	1.1 Targets nature was determined in line with the information required 1.2 Types of information required was established according line with the industry best practice 1.3 Organization operation platform was established in line industry best practice 1.4 Network topology was drawn based on industry best practice 1.5 Vulnerable points were identified as per the services on the host 1.6 Protocol's enumeration was performed as per the standard operating procedure 1.7 Authorization credentials were established as per the organization ICT policy 1.8 Payloads were prepared and deployed in line with industry best practice and ethics 1.9 Exploitation proof of concept was generated in line with the standard operating procedure 1.10 System users were manipulated using the system as per the industry best practice
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.

MANAGE SECURITY OPERATIONS

UNIT CODE: SEC/OS/CS/CR/11/6/A

UNIT DESCRIPTION

This unit covers the competencies required to manage security operations. It involves gathering information asset inventory, implementing a security management solution, establishing threats landscape, responding to established threats, monitoring events in the landscape and generating security operation report.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT These describe the key outcomes which make up workplace function.	**PERFORMANCE CRITERIA** These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
1. Gather information asset inventory	1.1 Capacity of the organization is established as per the information required 1.2 Assets in the organization are established in line with industry best practice 1.3 Assets are classified according to organization ICT policy
2. Implement a security management solution	2.1 Security management solution is acquired according to the context of the information gathered 2.2 Security management solution is deployed as per manufacturers guides 2.3 Security management solution is set up and configured in line with the organization ICT policy 2.4 Configuration are verified and hardened as per the industry best practices 2.5 Workspaces and dashboards are set up in line with the manufacturers guide and industry best practices
3. Establish threats landscape	3.1 Common threats are established in line with the installed dashboards 3.2 Reasons for presence of the threats identified are analysed as per the workplace procedures 3.3 Mitigation measures of the threats identified are implemented as per the organization ICT policy and industry best practice.
4. Respond to identified threats	4.1 Share the established threats with CIRT/CERT as per the organization ICT policy 4.2 Quarantine or removal of the established threats is performed in line with workplace procedures 4.3 System is kept live as per the organization ICT

ELEMENT These describe the key outcomes which make up workplace function.	PERFORMANCE CRITERIA These are assessable statements which specify the required level of performance for each of the elements. ***(Bold and italicised terms are elaborated in the Range)***
	policy 4.4 Participate in creation and implementation of business continuity plan in line with the organization policy
5. Monitor events in the landscape	5.1 Continuous monitoring of events is performed as per the implemented security management system 5.2 System user awareness is conducted in line with the organization policy 5.3 Security system, hardware and software are kept up to date as per the organization policy 5.4 Simulation of threats is performed on the system and response monitored as per the organization policy
6. Generate security operations report	6.1 Security operation reports are prepared in line with the organizations approved format 6.2 Security operation reports are shared with relevant parties as per the organization policy 6.3 Security operation reports are documented and filled according organization filing system 6.4 Security operation risk mitigation recommendations are prepared and shared with the relevant parties

RANGE

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

Variable	Range

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Troubleshooting techniques
- ICT Infrastructure auditing procedures
- ICT safety and precautious measures
- ICT Prevention measures
- Performance monitoring techniques
- ICT policy
- Causes of hardware and software failure
- Components of ICT Infrastructure
- User training procedures

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

• Communications (verbal and written); • Proficient in ICT; • Time management; • Analytical • Faults troubleshooting • Problem solving; • Planning;	• Decision making; • Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 Security management solutions were deployed as per manufacturers guides 1.2 Security management solutions were set up and configured in line with the organization ICT policy 1.3 Configuration were verified and hardened as per the industry best practices 1.4 Mitigation measures of the threats identified were implemented as per the organization ICT policy and industry best practice. 1.5 Established threats were shared with CIRT/CERT as per the

	organization ICT policy 1.6 Quarantine or removal of the established threats was performed in line with workplace procedures 1.7 Security system, hardware and software were kept up to date as per the organization policy 1.8 Simulation of threats was performed on the system and response monitored as per the organization policy 1.9 Security operation reports were shared with relevant parties as per the organization policy
2. Resource Implications for competence certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	4.1 Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	5.1 Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.