COMPETENCY STANDARD

FOR

Penetration Testing

(Cyber Security)

ICT Sector

Level: 5

Competency Standard Code: ICTCS0004L5V1

National Skills Development Authority
Prime Minister's Office, Bangladesh

Contents

Introduction

The National Skills Development Authority (NSDA) aims to enhance an individual's employability by certifying completeness with skills. NSDA works to expand the skilling capacity of identified public and private training providers qualitatively and quantitatively. It also aims to establish and operationalize a responsive skill ecosystem and delivery mechanism through a combination of well-defined set of mechanisms and necessary technical supports.

Key priority economic growth sectors identified by the government have been targeted by NSDA to improve current job skills along with existing workforce to ensure required skills to industry standards. Training providers are encouraged and supported to work with industry to address identified skills and knowledge to enable industry growth and increased employment through the provision of market responsive inclusive skills training program **Penetration Testing (Cyber Security)** is selected as one of the priority occupations of **Information and Communication Technology** Sector. This standard is developed to adopt a demand driven approach to training with effective inputs from Industry Skills Councils (ISC's), employer associations and employers.

Generally, a competency standard informs curriculum, learning materials, assessment and certification of students enrolled in TVET. Students who successfully pass the assessment will receive a qualification in the National Skills Qualification Framework (NSQF) and will be listed on the NSDA's online portal.

This competency standard is developed to improve skills and knowledge in accordance with the job roles, duties and tasks of the occupation and ensure that the required skills and knowledge are aligned to industry requirements. A series of stakeholder consultations, workshops were held to develop this document.

The document also details the format, sequencing, wording and layout of the Competency Standard for an occupation which is comprised of Units of Competence and its corresponding Elements.

Overview

A **competency standard** is a written specification of the knowledge, skills and attitudes required for the performance of an occupation, trade or job corresponding to the industry standard of performance required in the workplace.

The purpose of a competency standards is to:

- provide a consistent and reliable set of components for training, recognising and assessing people's skills, and may also have optional support materials
- enable industry recognised qualifications to be awarded through direct assessment of workplace competencies
- encourage the development and delivery of flexible training which suits individual and industry requirements
- encourage learning and assessment in a work-related environment which leads to verifiable workplace outcomes

Competency standards are developed by a working group comprised of representative from NSDA, Key Institutions, ISC, and industry experts to identify the competencies required of an occupation in **Information and Communication Technology** sector.

Competency standards describe the skills, knowledge and attitude needed to perform effectively in the workplace. CS acknowledge that people can achieve technical and vocational competency in many ways by emphasizing what the learner can do, not how or where they learned to do it.

With competency standards, training and assessment may be conducted at the workplace or at training institute or any combination of these.

Competency standards consist of a number of units of competency. A unit of competency describes a distinct work activity that would normally be undertaken by one person in accordance with industry standards.

Units of competency are documented in a standard format that comprises of:

- unit title
- nominal duration
- unit code
- unit descriptor
- elements and performance criteria
- variables and range statement
- curricular content guide
- assessment evidence guides

Together, all the parts of a unit of competency:

- describe a work activity
- guide the assessor to determine whether the candidate is competent or not yet competent

The ensuing sections of this document comprise of a description of the relevant occupation, trade or job with all the key components of a unit of competency, including:

- a chart with an overview of all Units of Competency for the relevant occupation, trade or job including the Unit Codes and the Unit of Competency titles and corresponding Elements
- the Competency Standard that includes the Unit of Competency, Unit Descriptor, Elements and Performance Criteria, Range of Variables, Curricular Content Guide and Assessment Evidence Guide

Level descriptors of NTVQF/ NSQF (BNQF 1-6)

Level & Job classification	Knowledge Domain	Skills Domain	Responsibility Domain
6 Mid-Level Manager/ Sub Assistant Engineer	Comprehensive actual and theoretical knowledge within a specific work or study area with an awareness of the validity and limits of that knowledge, able to analyze, compare, relate and evaluate.	Specialised and wider range of cognitive and practical skills required to provide leadership in the development of creative solutions to defined problems. Communicate professional issues and solutions to the team and to external partners/users.	Work under broad guidance and self-motivation to execute strategic and operational plan/s. Lead lower-level management. Diagnose and resolve problems within and among work groups.
5 Supervisor	Broad knowledge of the underlying, concepts, principles, and processes in a specific work or study area, able to scrutinize and break information into parts by identifying motives or causes.	Broad range of cognitive and practical skills required to generate solutions to specific problems in one or more work or study areas. Communicate practice-related problems and possible solutions to external partners.	Work under guidance of management and self-direction to resolve specific issues. Lead and take responsibility for the work and actions of group/team members. Bridge between management.
4 Highly Skilled Worker	Broader knowledge of the underlying, concepts, principles, and processes in a specific work or study area, able to solve problems to new situations by comparing and applying acquired knowledge.	A range of cognitive and practical skills required to accomplish tasks and solve problems by selecting and applying the full range of methods, tools, materials and information. Communicate using technical terminology and IT technology with partners and users as per workplace requirements.	Work under minimal supervision in specific contexts in response to workplace requirements. Resolve technical issues in response to workplace requirements and lead/guide a team/ group.
3 Skilled Worker	Moderately broad knowledge in a specific work or study area, able to perceive ideas and abstract from drawing and design according to workplace requirements.	Basic cognitive and practical skills required to use relevant information in order to carry out tasks and to solve routine problems using simple rules and tools. Communicate with his team and limited external partners upholding the values, nature and culture of the workplace	Work or study under supervision with considerable autonomy. Participate in teams and responsible for group coordination.
2 Semi-Skilled Worker	Basic understanding of underpinning knowledge in a specific work or study area, able to interpret and apply common occupational terms and instructions.	Skills required to carry out simple tasks, communicate with his team in the workplace presenting and discussing results of his work with required clarity.	Work or study under supervision in a structured context with limited scope of manipulation
1 Basic Skilled Worker	Elementary understanding of ability to interpret the underpinning knowledge in a specific study area, able to interpret common occupational terms and instructions.	Specific Basic skills required to carry out simple tasks. Interpret occupational terms and present the results of own work within guided work environment/ under supervision.	Work under direct supervision in a structured context with limited range of responsibilities.

List of Abbreviations

General

NSDA - National Skills Development Authority

CS – Competency Standard

ILO – International Labor Organization

ISC – Industry Skills Council

BNQF– Bangladesh National Qualifications Framework

NSQF– National Skills Qualifications Framework

NTVQF – National Technical and Vocational Qualifications Framework

SCVC – Standards and Curriculum Validation Committee

TVET – Technical Vocational Education and Training

UoC – Unit of Competency

Occupation Specific Abbreviations

MSDS – Material Safety Data Sheet

OSH – Occupational Safety and Health

PPE – Personal Protective Equipment

SOP – Standard Operating Procedures

Approval of Competency Standard

Members of the Approval Committee:

Member	Signature
Dulal Krishna Saha Executive Chairman (Secretary) National Skills Development Authority (NSDA)	21.06.21
Md. Nurul Amin Member (Admin & Finance) And Member (Registration & Certification) Joint Secretary National Skills Development Authority (NSDA)	21.06.21
Alif Rudaba Member (Planning & Skills Standard) Joint Secretary National Skills Development Authority (NSDA)	

21.06.21

Dulal Krishna Saha

Executive Chairman (Secretary)

National Skills Development Authority (NSDA)

Competency Standards for National Skill Certificate –5 in Penetration Testing in ICT Sector

Course Structure

SL	Unit Code and Title		UoC Level	Nominal Duration (Hours)
The Generic Competencies				
The Sector Specific Competencies				
The Occupation Specific Competencies				
1	OUCyS014L5V1	Apply Python Programming	5	50
2	OUCyS005L5V1	Apply Mobile Application Security	5	40
3	OUCyS019L5V1	Apply Social Engineering	5	15
4	OUCyS006L5V1	Apply advance Web Application Security	5	50
5	OUCyS012L5V1	Apply Network security Assessment	5	40
6	OUCyS015L5V1	Apply Cyber Security Risk Assessment	5	35
7	OUCyS016L5V1	Interpret Cryptography	5	30
8	OUCyS021L5V1	Interpret IoT Concepts	5	20
9	OUCyS010L5V1	Perform Pen Testing	5	60
10	OUCyS0023L5V1	Interpret IT Security Auditing	5	30
Total Nominal Learning Hours				**370**

Units & Elements at Glance

The Generic Competencies

The Sector Specific Competencies

The Occupation Specific Competencies

Code	Unit of Competency	Elements of Competency	Duration (Hours)
OUCyS014L5V1	Apply Python Programming	1. Interpret python programming structure 2. Practice with sequential structure 3. Practice with decisions making structure 4. Practice with Loop structure 5. Apply Functions and scripts 6. Maintain Error Handling	50
OUCyS005L5V1	Apply Mobile Application Security	1. Interpret Mobile Application Security 2. Perform Mobile application penetration testing 3. Perform web application countermeasures	40
OUCyS019L5V1	Apply Social Engineering	1. Interpret the social engineering concepts 2. Identify the social engineering threats 3. Identify Social engineering tools 4. Analyze the social engineering attacks	15
OUCyS006L5V1	Apply advance Web Application Security	1. Perform SQL injection 2. Interpret Misconfiguration & data expose 3. Perform XSS & CSRF 4. Apply access control	50
OUCyS012L5V1	Apply Network security Assessment	1. Interpret Network security concepts. 2. Implement Network Security 3. Assess Network security	40
OUCyS015L5V1	Apply Cyber Security Risk Assessment	1. Interpret Cyber Security Risk Assessment 2. Assess IT Risk 3. Analyze Risk performance 4. Prepare Risk Assessment Report	35
OUCyS016L5V1	Interpret Cryptography	1. Interpret Security Service goals 2. Classify classic Encryption technique 3. Categorize PKI component 4. Interpret Digital Certification workflow 5. Interpret cryptography algorithm 6. Perform Steganography	30

OUCyS021L5V1	Interpret IoT Concepts	1. Interpret IOT concepts and IOT Standards 2. Interpret IOT Applications 3. Identify Challenges in IOT implementation	20
OUCyS010L5V1	Perform Pen Testing	1. Identify Penetration Testing Tools 2. Perform Penetration Testing 3. Prepare VAPT report	60
OUCyS0023L5V1	Interpret IT Security Auditing	1. Interpret IT Security Audit 2. Interpret Auditing Information System 3. Use of Information Systems Operations Maintenance and Service Management 4. Interpreted Information Systems Acquisition, Development and Implementation 5. Interpret the protection of information assets 6. Apply the Governance and Management of IT audit	30

The Generic Competencies

The Sector Specific Competencies

The Occupation Specific Competencies

Unit Code and Title	OUCyS014L5V1: Apply Python Programming
Nominal Hours	**50 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply python programming. It specifically includes the tasks of interpreting python programming structure, practicing with sequential structure, practicing with decisions making structure, practicing with loop structure, applying functions and script and maintaining error handling.
Elements of Competency	**Performance Criteria** **<u>Bold and Underlined</u>** terms are elaborated in the Range of Variables
1. Interpret python programming structure	1. 1 Features of Python Language are stated 1. 2 Structure of Python Program is explained 1. 3 **<u>Variables</u>** of Python Language are identified 1. 4 Application of Python in cyber security is interpreted
2. Practice with sequential structure	2.1 Sequential structured problems are identified 2.2 Algorithm for sequential structured programs is prepared 2.3 Flow chart of sequential structure programs are created 2.4 Code is written to implementing the sequential structured programs.
3. Practice with decisions making structure	3.1. **<u>Selective structured</u>** problems are identified 3.2. Algorithm for selective structured programs is prepared 3.3. Flow chart of selective structure programs are created 3.4. Code is written to implementing the selective structured programs.
4. Practice with Loop structure	4.1 **<u>Repetitive structured</u>** problems are identified 4.2 Algorithm for repetitive structured programs is prepared 4.3 Flow chart of repetitive structure programs are created 4.4 Code is written to implementing the Repetitive structured programs.
5. Apply Functions and script	5.1 Remote Management system is interpreted 5.2 Function program problems are identified 5.3 Code is written to implementing the function programs with **<u>various function activities</u>**
6. Maintain Error Handling	6.1 **<u>Standard Errors</u>** are interpreted 6.2 New bugs are identified 6.3 New bugs are fixup 6.4 New or changed requirements are implemented without breaking existing functionality. 6.5 Extensibility are provided flexibility; 6.6 Enables a high level of reusability is developed for code base. 6.7 Efficiently discovering bugs and untested code
Range of Variables	

Variable	**Range** (may include but not limited to):
1. Variables	1.1 Integer 1.2 Float 1.3 String 1.4 Boolean
2. Selective structure	2.1 if 2.2 if else 2.3 if else if
3. Repetitive structure	3.1 For loop 3.2 While loop
4. Various function activities	4.1 with argument(s) 4.2 return zero 4.3 return value 4.4 with global & local variable
5. Standard Error	5.1 Application Error 5.2 Validation Error 5.3 Response Error 5.4 Required Error 5.5 Unique field Error 5.6 Bad Request Error 5.7 Unauthorized Error.

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Code is written to implementing basic selective & repetitive structure program in python. 1.2 Maintained error handling properly
2. Underpinning Knowledge	2.1. Sequential structured problems 2.2. Algorithm for selective structured 2.3. Algorithm for repetitive structured 2.4. Flowchart of repetitive structure 2.5. Function program problems 2.6. Standard Errors
3. Underpinning Skills	3.1 Applying concept of algorithm 3.2 Applying concept of flowchart 3.3 Applying the concept of sequential structure

4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS005L4V1: Apply Mobile Application Security**
Nominal Hours	**40 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to applying mobile application security. It specifically includes the tasks of interpreting mobile application security, performing mobile application penetration testing and performing web application countermeasures.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Mobile Application Security	1.1 Mobile application security is interpreted;
	1.2 **Mobile OS** is interpreted;
	1.3 Mobile Application Security **Best Practices** is interpreted;
	1.4 **Mobile Apps threats** are identified;

2. Perform Mobile application penetration testing	2.1 **Penetration testing steps** are interpreted;
	2.2 Penetration testing is performed using **tools;**
	2.3 Report is prepared;

3. Perform web application countermeasures	3.1 Start with thought like an attacker; 3.2 Mobile application security is performed using required **Solutions;** 3.3 Web application countermeasures are performed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Mobile OS	1.1 Android 1.2 IOS
2. Best practices	2.1 Enact Digital Security Training 2.2 Proactively Monitor for Rogue Apps 2.3 Only Download from Trusted Sources 2.4 Improve Data Security 2.5 Avoid Saving Passwords 2.6 Force User Session End 2.7 Go Beyond Anti-Malware
3. Mobile Apps threats	2.1 Login credentials being stolen 2.2 Credit card details stolen and resold 2.3 Giving hackers access to their business networks 2.4 Wholesale identity theft 2.5 Their device being used to spread malware to uninfected devices 2.6 Having TXT or SMS messages copied and scanned for private info 2.7 Other malicious applications

4. Penetration testing steps	3.1. Information gathering 3.2. Scanning 3.3. Enumeration 3.4. Vulnerability Assessment 3.5. Penetrate the application vulnerabilities
5. Tools	4.1 MobSF 4.2 kingoRoot 4.3 Cydia 4.4 Apktool 4.5 Appcrack 4.6 Burp Proxy 4.7 Wireshark 4.8 Metasploit
6. Solutions	5.1 Patching 5.2 Anti-malware protection

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Identified mobile apps threats; 1.2 Performed penetration testing is using tools
2. Underpinning Knowledge	2.1. Mobile Application Security 2.2. Mobile application penetration testing 2.3. Web application countermeasures
3. Underpinning Skills	3.1 Applying concept of mobile application security 3.2 Applying concept of penetration testing 3.3 Applying concept of countermeasures
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.

6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS019L5V1: Apply Social Engineering**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply social engineering. It specifically includes the tasks of interpreting the social engineering concepts, identifying the social engineering threats, identifying social engineering tools and analyzing the social engineering attacks.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret the social engineering concepts	1.1 Social Engineering and **Social networks** are interpreted;
	1.2 Social Engineering in Cyber Security is identified;
	1.3 Social Engineering in Law is identified;

2. Identify the social engineering threats	2.1 Threats of Social Engineering are identified;
	2.2 Types of **Social Engineering Threats** are listed;
	2.3 Review Social Engineering case studies and methods of manipulation are comprehended;
	2.4 Prevention tricks against Social Engineering Threats are identified;

3. Identify Social engineering tools	3.1 **Social Engineering tools** are identified as per requirement; 3.2 Social Engineering tools are installed; 3.3 Social Engineering tools are updated and upgraded with dependency;
4. Analyze the social engineering attacks	4.1 Social Engineering attacks are categorized for computer, mobile and physical entity; 4.2 Social Engineering tools are selected as per requirement; 4.3 Social Engineering attacks are analyzed following SOP; 4.4 Standard report is prepared as per requirement;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Social Network	1.1. Facebook 1.2. Linkedin 1.3. Email messenger 1.4. Instagram 1.5. whatsapp
2. Social engineering Threats	2.1. Shoulder surfing 2.2. Dumpster diving 2.3. Tailgating, Impersonation 2.4. Hoaxes 2.5. Whaling 2.6. Insider threat 2.7. Phishing

	2.8. Vishing 2.9. CSRF 2.10. XSS
3. Social Engineering tools	3.1 **Ohphish** 3.2 Skiphish 3.3 Computer Based Tools: • Maltego • Social Engineer Toolkit (SET) 3.4 Phone based Tools: • Burner Phones • Caller ID Spoofing • True Call Id 3.5 Physical Tools : • Cameras • GPS Trackers • Lock Picking • Recording Devices 3.6 OSIRT tools

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Identified Social Engineering in Law; 1.2 Identified Threats of Social Engineering 1.3 Installed Social Engineering tools 1.4 Prepared Standard report is as per requirement
2. Underpinning Knowledge	2.1 OS 2.2 Social network 2.3 Computer 2.4 Mobile (Android, Apple)
3. Underpinning Skills	3.1 Operating OS 3.2 Operating Social network 3.3 Operating Mobile (Android, Apple)
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace

5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS006L4V1: Apply advance Web Application Security**
Nominal Hours	**50 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply advance web application security. It specifically includes the tasks performing SQL injection, interpreting misconfiguration and data expose, performing advance web attack and applying access control.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Perform SQL injection	1.1 Down blow database is collected;
	1.2 Finding Vulnerable Website is identified;
	1.3 Vulnerable columns are displayed;
	1.4 Admin Panel is identified;
	1.5 Web application **tools** are identified;

2. Interpret Misconfiguration and data expose	2.1 Misconfiguration concepts are interpreted; 2.2 Application behavior to mitigate the risk of misconfiguration is performed; 2.3 Risk of **Security misconfiguration** is limited; 2.4 NIST 25 critical controls are interpreted; 2.5 Software testing is interpreted;

3. Perform advance web attack	3.1 **Cross site scripting** is performed;
	3.2 **Cross-Site Forgery (CSRF) attacks** are prevented;
	3.3 **CSRF token** are validated depends on request method;
	3.4 Buffer overflow is performed;
	3.5 Local File Inclusion (LFI) is performed;
	3.6 Remote file inclusion (RFI) is performed;
	3.7 Parameter Tampering is performed;
	3.8 OS command injection is performed;

4. Apply access control	4.1 Access control is interpreted; 4.2 **Accesses** are controlled following SOP;

Range of Variables

Variable	**Range** (may include but not limited to):
1. Tools	1.1 Burp suite 1.2 Acunetix 1.3 Nessus 1.4 Vega 1.5 Metasploit 1.6 Medusa 1.7 Nmap 1.8 BeeF framework 1.9 DVWA

2. Security Misconfiguration	2.1. Creating policy 2.2. Reducing attack surface 2.3. Remaining adaptable despite granular policy 2.4. Managing networks 2.5. Enforcing (both the network and process level)
3. Cross site scripting	3.1. Hijack an account 3.2. Spread web worms 3.3. Access browser history and clipboard contents 3.4. Control the browser remotely 3.5. Scan and exploit intranet appliances and applications
4. Persistent Cross site scripting	4.1 Input coming into web applications is not validated 4.2 Output to the browser is not HTML encoded
5. Cross-Site Forgery (CSRF) attacks	5.1 Unpredictable with high entropy, as for session tokens in general. 5.2 Tied to the user's session. 5.3 Strictly validated in every case before the relevant action is executed
6. Accesses	6.1 Mandatory access control (MAC) 6.2 Discretionary access control (DAC) 6.3 Role-based access control (RBAC) 6.4 Rule-based access control (RBAC)

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Performed application behavior to mitigate the risk of misconfiguration; 1.2 Performed cross site scripting; 1.3 Controlled the accesses by following SOP;
2. Underpinning Knowledge	2.1 SQL injection 2.2 Misconfiguration & data expose 2.3 XSS & CSRF
3. Underpinning Skills	3.1 Apply the concept of SQL injection 3.2 Apply the concept of misconfiguration and data expose 3.3 Apply the concept of XSS & CSRF
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace

5. Resource Implications	The following resources must be provided: 5.3 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.4 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.5. Written Test 6.6. Demonstration 6.7. Oral Questioning 6.8. Portfolio
7. Context of Assessment	7.3. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.4. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS012L5V1: Apply Network security Assessment**
Nominal Hours	**40 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply network security assessment. It specifically includes the tasks of interpreting network security concepts, performing common network attack and vulnerabilities, implementing network security and assessing network security.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret Network security concepts	1.1 **Management Security** is interpreted;
	1.2 **Network devices** are interpreted;
	1.3 Basic network **protocol** is identified;
	1.4 Secure Network implementation process is interpreted by packet tracer;
	1.5 Network Topologies and Architecture are interpreted;

2. Perform common network attack and vulnerabilities	2.1 Major network **intrusion** is identified;
	2.2 Network attacks **tools** are performed;

3. Implement Network Security	3.1 **Network Security Solutions and devices** are identified;
	2.3 Network Security Solutions and devices are selected as per job requirements;
	2.4 Network Security Solutions are implemented;

4. Assess Network security	3.2 Network Security vulnerabilities are identified; 3.3 Network Security vulnerabilities are assessed; 3.4 Network Security vulnerabilities are penetrated; 3.5 Report is prepared following standard format;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Management Security	1.1 Operational Security 1.2 Physical Security
2. Network Devices:	2.1 Hub 2.2 Repeater 2.3 Switch 2.4 Router 2.5 Wireless AP 2.6 Load Balancer
3. Protocol	3.1 TCP/IP 3.2 IPv4 3.3 IPv6
4. Intrusion	4.1 DOS and DDOS 4.2 DNS cache poisoning 4.3 Session hijacking 4.4 IP Spoofing

	4.5 Sniffing 4.6 MITM
5. Tools	a. LOIC/HOIC b. SSLstrip c. Wireshark d. Nmap e. Router scan f. Wifite2 g. Wireless network watcher
6. Network Security Solutions and Devices:	a. Firewall b. IPS / IDS c. Threat Protection d. ANTI APT e. Sandbox

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Implemented Network Security Solutions 1.2 Penetrated Network Security vulnerabilities 1.3 Prepared Report following standard format.
2. Underpinning Knowledge	2.1. Topology 2.2. Operational Security. 2.3. Physical Security 2.4. Network Security Solutions and devices 2.5. Network Security vulnerabilities
3. Underpinning Skills	3.1 Applying the concept of Topology 3.2 Applying the concept of Operational Security 3.3 Applying the concept of Physical Security
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.

6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS015L5V1: Apply Cyber Security Risk Assessment**
Nominal Hours	**35 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply cyber security risk assessment. It specifically includes the tasks of interpreting cyber security risk assessment, assessing IT risk, analyzing risk performance and preparing risk assessment report.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret Cyber Security Risk Assessment	1. 1 Risk Assessment is interpreted; 1. 2 Risk management strategy is interpreted; 1. 3 Risk treatment is interpreted;

2. Assess IT Risk	2.1. **Risk Assessment** is performed;
	2.2. Risk Management Control is designed;
	2.3. Risk Management Control is implemented;
	2.4. Risk Management Control is assessed;

3. Analyze Risk performance	3.1 **Risk performance** is interpreted; 3.2 KPI is Applied to identify the performance; 3.3 KRI is Applied to identify the Risk; 3.4 RTO and RPO are defined; 3.5 RTO and RPO are analyzed; 3.6 Risk capacity are interpreted; 3.7 Risk appetite are interpreted; 3.8 Risk tolerance are interpreted;
4. Prepare Risk Assessment Report	4.1 Risk Assessment report is prepared 4.2 Recommendations are prepared.
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Risk Assessment	1.1 People 1.2 Process 1.3 Technology 1.4 Governance
2. Risk performance	2.1. KPI 2.2. KRI
Evidence Guide The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency	

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1.1 Performed risk assessment 1.2 Applied KPI to identify the performance 1.3 Applied KRI to identify the Risk
2. Underpinning Knowledge	2.1. IT Risk Assessment Process 2.2. Distinguish Risk, threats and vulnerabilities 2.3. Risk Assessment 2.4. Security Policy, Standards, Procedures 2.5. Risk Assessment Report 2.6. Good Practices in Enterprise IT Risk Management
3. Underpinning Skills	3.4 Apply the concept of Cyber Security risk 3.5 Apply the concept of Cyber Security risk assessment
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS016L5V1: Interpret Cryptography**
Nominal Hours	**30 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to interpret Cryptography. It specifically includes the tasks of interpreting security service goals, classifying classic Encryption techniques, categorizing PKI component, interpreting digital certification workflow, interpreting cryptography algorithm and performing Steganography.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret Security Service goals	1.1 Security service **goals** are defined; 1.2 Security service mechanism is interpreted;

2. Classify classic Encryption technique	2.1. **Encryption Technique** is classified;
	2.2. Multiplicative inverse is interpreted;
	2.3. Additive inverse is interpreted;
	2.4. GCD is interpreted;

3. Categorize PKI component	3.1. PKI infrastructure is Illustrated;
	3.2. **PKI component** is Identified;

4. Interpret Digital Certification workflow	4.1 Digital Certificate workflow is explained; 4.2 Steps of achieve Digital certificate is interpreted;

5. Interpret cryptography algorithm	5.1 Cryptography Algorithm is interpreted;
	5.2 **Cryptography Algorithm** is Illustrated;
	5.3 **Hashing algorithm** is illustrated;

6. Perform Steganography	6.1 Steganography tools are identified as per requirement; 6.2 **Steganography Tools** are installed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Goals	1.1 Confidentiality 1.2 Integrity 1.3 Availability
2. Encryption technique	2.1 Playfair 2.2 Rotor 2.3 Caeser 2.4 Substitution 2.5 Transposition
3. PKI component	3.1. RA 3.2. CIA 3.3. CRL 3.4. OCSP
4. Cryptography algorithm	4.1 RSA 4.2 Elliptic Curve

	4.3 DH 4.4 DES/AES 4.5 RC4 4.6 Isakamp/IKE
5. Hashing algorithm	4.7 SHA-1/SHA-2 etc 4.8 MD5 4.9 RC4
6. Steganography Tools	5.1 Xiao Stenography 5.2 S-Tools

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate:
	1.1 Classified Encryption techniques;
	1.2 Illustrated PKI infrastructure;
	1.3 Interpreted Cryptography Algorithm;
	1.1 Installed Steganography Tools;

2. Underpinning Knowledge	2.1. Security service mechanism 2.2. Encryption Technique 2.3. PKI component 2.4. Cryptography Algorithm 2.5. Steganography tools
3. Underpinning Skills	3.1 Apply the concept of Cryptography 3.2 Apply the concept of Steganography tools
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio

7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS021L5V1: Interpret IoT Concepts**
Nominal Hours	**20 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to interpret IoT concepts. It specifically includes the tasks of interpreting IOT concepts and IOT standards, interpreting IOT applications and identifying challenges in IOT implementation.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables

1. Interpret IOT concepts and IOT Standards	1.1 **Components of IOT** System are identified;
	1.2 Working Process of IOT are examined;
	1.3 IOT Architecture is interpreted;
	1.4 **Stages of IOT architecture** are identified;
	1.5 IOT Application Areas are identified;

2. Interpret IOT Applications	2.1 IOT technologies and Protocols are identified;
	2.2 IOT communication Models are identified;

3. Identify Challenges in IOT implementation	3.1. Challenges in IOT are identified;
	3.2. IOT security Problems are identified;
	3.3. IOT Vulnerabilities are identified;
	3.4. IOT Attack Surface Area are identified;
	3.5. **Threats for IOT** are identified;

Range of Variables	
Variable	**Range** (may include but not limited to):
1. Components of IOT	1.1 Connected devices 1.2 Central Control Hardware. 1.3 Networks and protocols 1.4 Data Cloud 1.5 User interface 1.6 Network Interconnection 1.7 System Security 1.8 Data Analytics
2. Threats for IOT	2.1. Botnets 2.2. Denial of service 2.3. Man-in-the-Middle 2.4. Identity and data theft 2.5. Social engineering 2.6. Advanced persistent threats 2.7. Ransomware 2.8. Remote recording

3. Stages of IOT architecture	3.1 Sensors and actuators. 3.2 Internet gateways and Data Acquisition Systems 3.3 Edge IT Data Processing. 3.4 Datacenter and cloud.

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate: 1. 1 Identified components of IOT System; 1. 2 Identified IOT security Problems 1. 3 Identified Threats for IOT
2. Underpinning Knowledge	2.1. Sensors and actuators. 2.2. Internet gateways and Data Acquisition Systems 2.3. Edge IT Data Processing. 2.4. Datacenter and cloud
3. Underpinning Skills	3.1 Apply the concept of components of IOT 3.2 Apply the concept of Threats for IOT 3.3 Apply the concept of Stages of IOT architecture
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Code and Title	**OUCyS010L5V1: Perform Pen Testing**
Nominal Hours	**60 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to perform pen testing. It specifically includes the tasks of identifying penetration testing tools, performing penetration testing, preparing VAPT report.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Identify Penetration Testing Tools	1.1 Penetration testing is interpreted; 1.2 **Penetration Testing Tools** are identified and selected;
2. Perform Penetration Testing	2.1 Vulnerabilities/potential problem areas are listed; 2.2 List of items is ranked in the order of priority/criticality; 2.3 Access data/network/server/website is unauthorized; 2.4 Re-run until the problem area is fixed;
3. Prepare VAPT report	3.1 Information is scanned; 3.2 Information is identified for targeting; 3.3 Results from the scanning is prepared; 3.4 Services are identified; 3.5 Scanned information are confirmed; 3.6 Vulnerabilities are assessed and documented;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Penetration Testing Tools	1.1 Kali Linux or Parrot security OS • Netsparker • Acunetix • Metasploit • Wireshark • Hydra • Hping 2/3 • w3af • Nessus • Burpsuite • Zed Attack Proxy (ZAP) • John The Ripper • Sqlmap • Nmap • BeEF • Probely • Mozilla observatory • Pentest-tools.com

Evidence Guide

The evidence must be authentic, valid, sufficient, reliable, consistent and recent and meet the requirements of the current version of the Unit of Competency

1. Critical Aspects of Competency	Assessment required evidence that the candidate:
	1.1 Selected Penetration Testing Tools;
	1.2 Listed vulnerabilities/potential problem areas;
	1.3 Prepared results from the scanning;
	1.4 Assessed and documented Vulnerabilities;

2. Underpinning Knowledge	2.1. Penetration testing 2.2. Vulnerabilities/potential problem areas 2.3. Re-run until the problem area
3. Underpinning Skills	3.1. Apply the concept of penetration testing 3.2. Apply the concept of vulnerabilities/potential problem areas 3.3. Apply the concept of scanned information
4. Required Attitudes	4.1 Commitment to occupational health and safety 4.2 Promptness in carrying out activities 4.3 Sincere and honest to duties 4.4 Environmental concerns 4.5 Eagerness to learn 4.6 Tidiness and timeliness 4.7 Respect for rights of peers and seniors in workplace 4.8 Communication with peers and seniors in workplace
5. Resource Implications	The following resources must be provided: 5.1 Relevant tools, Equipment, software and facilities needed to perform the activities. 5.2 Required learning materials.
6. Methods of Assessment	Methods of assessment may include but not limited to: 6.1. Written Test 6.2. Demonstration 6.3. Oral Questioning 6.4. Portfolio
7. Context of Assessment	7.1. Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2. Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA.

Unit Title and Unit Code	OUCyS0023L5V1: **Interpret IT Security Auditing**
Unit Descriptor	This unit covers the knowledge, skills and attitude required to interpret IT security auditing. It includes interpreting concept of IT security auditing, auditing information system, Using of Information Systems, Operations Maintenance & Service Management, Acquisition, Development, Implementation, protection of information assets and applying the Governance and Management of IT audit.
Nominal Hours	**30 Hours**
Elements of Competency	**Performance Criteria** **Bold and underline** terms are elaborated in the range of variables

1. Interpret IT Security Audit	1.1 The Process of Auditing Information Systems is defined;
	1.2 **Control objectives** of IT Security Audit are Interpreted;
	1.3 **Risk management** of IT Security Audits are Interpreted;
	1.4 Self-Control Assessment Auditing is interpreted;

2. Interpret Auditing Information System	2.1 **Types of IT Audit** are explained;
	2.2 Processes of IT Audit are interpreted;
	2.3 IT Risk Assessment procedure is interpreted;
	2.4 IT Audit Sampling Methodology is explained;
	2.5 IT Audit Reporting is explained;

3. Use of Information Systems Operations Maintenance and Service Management	3.1. IT Inventory is interpreted;
	3.2. IT Service Management is explained;
	3.3. IT Change Management is explained;
	3.4. IT Upgrade/Patch Management is performed;
	3.5. IT Systems Hardening is explained;
	3.6. IT Backup & Restore is used;
	3.7. Firewall & Router Access List is identified;

4. Interpreted Information Systems Acquisition, Development and Implementation	4.1 Software Development Life Cycle (SDLC) is interpreted;
	4.2 Version/Release Management is interpreted;
	4.3 Configuration Management is interpreted;
	4.4 Vendor/Service Provider Management is interpreted;

5. Interpret the protection of information assets	5.1 Protection of Information Assets is defined
	5.2 Information Assets are interpreted;
	5.3 Information Security Awareness Program is interpreted;
	5.4 Physical and Logical Security Controls are explained
	5.5 Fraud Risk Management is interpreted;
	5.6 Encryption and Public Key Infrastructure (PKI) is interpreted;

6. Apply the Governance and Management of IT audit	6.1 Segregation of Duties (SoD) are interpreted; 6.2 Implementation of IT Security Policy is interpreted; 6.3 Business Impact Analysis (BIA) is performed 6.4 Business Continuity Plan (BCP) is prepared and used. 6.5 IT Audit is performed according to IT governance and management practices
Range of Variables	
Variable	**Range** (May include but not limited to:)

1. Control objectives	1.1 Preventive Control 1.2 Detective Control 1.3 Corrective Control
2. Risk management	2.1 Accept 2.2 Avoid 2.3 Mitigate 2.4 Transfer
3. Types of IT Audit	3.1. Internal IT Audit 3.2. External IT Audit 3.3. Risk Based IT Audit 3.4. Compliance Audit 3.5. Operational Audit

Evidence Guide

The evidence guide provides advice on assessment and must be read together with the performance criteria, required skills and knowledge and range of variable. Evidence must be gathered in the workplace wherever possible. Where no workplace is available, a simulated workplace must be provided.

To achieve competency in this unit, a trainee must be able to provide evidence in the form of the following:

1.Critical Aspects	The assessment required evidence that the candidate: 1.1 interpreted IT Audit Process 1.2 Interpreted IT Risk Assessment, 1.3 Interpreted Risk Based IT Audit 1.4 Interpreted Separation of Duties (SoD) 1.5 Interpreted IT Risk Register 1.6 Interpreted Business Impact Analysis (BIA) 1.7 Interpreted Business Continuity Plan (BCP)
2.Underpinning knowledge	2.1 IT Audit Process 2.2 IT Risk Assessment, 2.3 Concept of Risk Based IT Audit 2.4 Separation of Duties (SoD) 2.5 IT Risk Register 2.6 Business Impact Analysis (BIA) 2.7 Business Continuity Plan (BCP)
3.Underpinning Skills	3.1 Developing IT Security Audit Checklist 3.2 Developing Network Security Audit Checklist 3.3 Developing Operating System Security Audit Checklist 3.4 Developing Database Security Audit Checklist 3.5 Developing Access Control Audit Checklist 3.6 Developing Physical Security Audit Checklist
4.Required Attitude	4.1 Commitment to occupational safety and health 4.2 Environmental concerns 4.3 Tidiness and timeliness 4.4 Respect for rights of peers and seniors in workplace 4.5 Eagerness to learn 4.6 Promptness in carrying out activities

	4.7 Sincere and honest to duties and responsibilities 4.8 Communication with peers, sub-ordinates and seniors in workplace
5.Resource Implication	The following resources must be provided: 5.1 required Tools & equipment's, real workplace or simulated workplace, facilities and relevant accessories of the construction sector Consumables materials to perform activities 5.2 required teaching aids 5.3 learning Materials
6.Methods of Assessment	6.1 Written test 6.2 Demonstration 6.3 Oral questioning 6.4 Portfolio
7.Context of Assessment	7.1 Competency assessment must be done in a training center or in an actual or simulated work place after completion of the training module 7.2 Assessment should be done by NSDA certified assessor

Accreditation Requirements

Training Providers must be accredited by National Skills Development Authority (NSDA), the National Quality Assurance Body, or a body with delegated authority for quality assurance to conduct training and assessment against this unit of competency for credit towards the award of any NTVQF qualification. Accredited providers assessing against this unit of competency must meet the quality assurance requirements set by NSDA

Copyright

This document is available from:

National Skills Development Authority (NSDA)
423-428 Tejgaon Industrial Area, Dhaka-1215
Phone: +880 2 8891091; Fax: +880 2 8891092; E-mail: ecnsda@nsda.gov.bd
Website: www.nsda.gov.bd