COMPETENCY STANDARD

FOR

Hacking Forensic Investigation

(Cyber Security)

ICT Sector

Level: 5

Competency Standard Code: ICTCS0004L5V1

National Skills Development Authority
Prime Minister's Office, Bangladesh

Contents

Introduction 2
Overview 3
List of Abbreviations 5
Approval of Competency Standard 6
Course Structure 7
Units & Elements at a Glance 8
The Generic Competencies 11
The Sector Specific Competencies 12
The Occupation Specific Competencies 13
OUCyS001L4V1: Interpret Information Security Concepts 3
OUCyS002L4V1: Apply Operating Systems Administration Concepts 6
OUCyS012L5V1: Apply Network security Assessment 8
OUCyS005L4V1: Apply Mobile Application Security 11
OUCyS011L5V1: Apply Identity &Access Management 14
OUCyS003L4V1: Analyze Malicious Code 16
OUCyS017L5V1: Perform Digital Forensic 19
OUCyS018L5V1: Apply Threat Hunting Concepts 22
OUCyS019L5V1: Apply Social Engineering 26
Unit Title and Unit Code 29
OUCyS0023L5V1: Interpret IT Security Auditing 29

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 **Hacking Forensic Investigation (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 Hacking Forensic Investigation 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	OUCyS001L5V1	Interpret Information Security Concepts	5	20
2	OUCyS002L5V1	Apply Operating Systems Administration Concepts	5	25
3	OUCyS012L5V1	Apply Network security Assessment	5	40
4	OUCyS005L5V1	Apply Mobile Application Security	5	40
5	OUCyS011L5V1	Apply Identity & access management	5	15
6	OUCyS003L5V1	Analyze malicious code	5	30
7	OUCyS017L5V1	Perform Digital Forensic	5	60
8	OUCyS018L5V1	Apply Threat hunting concepts	5	50
9	OUCyS019L5V1	Apply Social Engineering	5	15
10	OUCyS0023L5V1	Interpret IT Security Auditing	5	30
Total Nominal Learning Hours				**325**

Units & Elements at a Glance

The Generic Competencies

The Sector Specific Competencies

The Occupation Specific Competencies

Code	Unit of Competency	Elements of Competency	Duration (Hours)
OUCyS001L5V1	Interpret Information Security Concepts	1. Interpret Information Security System 2. Interpret Hacking Techniques 3. Identify types of Attacks 4. Categorize Security Threats & Control 5. Interpret Cyber Law	20
OUCyS002L5V1	Apply Operating Systems Administration Concepts	1. Install Virtual machine 2. Install OS 3. Perform Hacking using hacking tool	25
OUCyS012L5V1	Apply Network security Assessment	1. Interpret Network security concepts. 2. 2.Implement Network Security 3. Assess Network security	40
OUCyS005L5V1	Apply Mobile Application Security	1. Interpret Mobile Application Security 2. Perform Mobile application penetration testing 3. Perform web application countermeasures	40
OUCyS011L5V1	Apply Identity & access management	1. Interpret identity & access probation life cycle 2. Apply access control management Identification and Authentication devices	15
OUCyS003L5V1	Analyze malicious code	1. Install Virtual machine 2. Install OS 3. Perform Hacking using hacking tool	30
OUCyS017L5V1	Perform Digital Forensic	1. Perform OS forensics 2. Perform Mobile Forensics 3. Perform Graphics Forensics 4. Perform Cloud Forensics 5. Perform E-mail Forensics	60
OUCyS018L5V1	Apply Threat hunting concepts	1. Identify Cyber Threat Hunting and articulate its value to an organization 2. Interpret Cyber threat hunting methodologies and techniques 3. Analyze Cyber Threat hunting 4. Follow Incident Response and Incident Handling	50
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
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	30

		4. Interpreted Information Systems Acquisition, Development and Implementation 5. Interpret the protection of information assets 6. Apply the Governance and Management of IT audit	

The Generic Competencies

The Sector Specific Competencies

The Occupation Specific Competencies

Unit Code and Title	OUCyS001L4V1: Interpret Information Security Concepts
Nominal Hours	**20 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to interpret information security concepts in the workplace. It specifically includes the tasks of interpreting information security system, hacking techniques, identifying types of attacks, categorizing security threats & control and interpreting cyber law.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret Information Security System	1.1 Information Security is interpreted; 1.2 Information **Security Principles** are stated; 1.3 Information Security Policy is interpreted; 1.4 Information **security framework** are listed;
2. Interpret Hacking Techniques	2.1 Hacking is Interpreted; 2.2 **Types of hackers** is identified; 2.3 Hacking Techniques is Interpreted;
3. Identify types of Attacks	3.1 Step of hacking is interpreted; 3.2 **Types of Attacks** are identified;
4. Categorize Security Threats & Control	4.1 Necessity of awareness about cyber security threats is interpreted; 4.2 Anti-Virus Software is Installed; 4.3 Updated patch is ensured; 4.4 Firewall is used to protect networks; 4.5 Internet Downloads are scanned; 4.6 Regular backups of critical data are ensured;
5. Interpret emerging technology	5.1 Artificial Intelligence is interpreted; 5.2 Big Data is interpreted; 5.3 Data Science is interpreted; 5.4 Machine Learning is interpreted; 5.5 Machine vision is interpreted;
6. Interpret Cyber Law	6.1 Cyber Law is stated; 6.2 Cyber Law Global Impact is interpreted 6.3 Cyber Law in Bangladesh is interpreted
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Security Principles	1.1 Confidentiality 1.2 Integrity 1.3 Availability 1.4 Authentication 1.5 Non-Repudiation
2. Security framework	2.1 NIST cyber security framework (CSF) 2.2 ISO/IEC 27001/2 2.3 COBIT 5

	2.4 ITIL 2.5 General Data Protection Regulation (GDPR)
3. Types of hackers	3.1 Cyber terrorist 3.2 Black Hat' Hackers 3.3 White Hat' Hackers 3.4 Grey Hat' Hackers 3.5 Hacktivist 3.6 Script kiddies
4. Types of Attacks	4.1 Malware Attack 4.2 Phishing 4.3 SQL Injection Attack 4.4 Cross-Site Scripting (XSS) 4.5 Denial of Service (DoS) 4.6 Session Hijacking and Man-in-the-Middle Attacks 4.7 Credential Reuse 4.8 OWASP top 10

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 Interpreted global impact of Cyber Law 1.2 Interpreted Cyber Law in Bangladesh 1.3 Identified types of attacks 1.4 Identified types of hackers;
2. Underpinning Knowledge	2.1 Security Principles 2.2 types of Attacks 2.3 Hacking 2.4 Types of hackers 2.5 Hacking Techniques 2.6 Step of hacking 2.7 types of Attacks 2.8 Cyber Law Global Impact 2.9 Cyber Law in Bangladesh
3. Underpinning Skills	3.1 Installing Anti-Virus Software 3.2 Ensuring Updated Anti-virus software 3.3 Installing Firewall 3.4 Scanning Internet Downloads 3.5 Checking data backups 3.6 Performing folder management
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	**OUCyS002L4V1: Apply Operating Systems Administration Concepts**
Nominal Hours	**25 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply operating systems administration concepts. It specifically includes the tasks of installing virtual machine, installing OS and performing hacking using hacking tool.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Install Virtual machine	1.1 Concept is virtualized; 1.2 **VM** is Selected and collected; 1.3 VM is Installed following SOP; 1.4 VM is configured following SOP;
2. Install OS	2.1 Basic operating system concepts is interpreted; 2.2 **OS** is selected and collected; 2.3 OS is Installed following SOP; 2.4 Basic **command** is interpreted; 2.5 Internet and network connectivity is checked; 2.6 OS packages with dependency are updated and upgraded;
3. Perform Hacking using hacking tool	3.1 **Hacking tools** are identified as per requirement; 3.2 Hacking tools are installed; 3.3 Hacking tools with dependency are updated and upgraded;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. VM	1.1 Virtual Machine 1.2 Oracle virtual Box 1.3 VM ware
2. OS	2.1 Windows 2.2 Kali Linux 2.3 Ubuntu 2.4 MAC 2.5 Parrot OS
3. Hacking tools	3.1 The harvester 3.2 Nmap 3.3 Wire shirk 3.4 John the ripper 3.5 Responder 3.6 Hashcat 3.7 Metasploit 3.8 Burpsuite

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 Configured VM 1.2 Installed OS 1.3 Installed hacking tools
2. Underpinning Knowledge	2.1 Internet 2.2 Basic networking 2.3 NAT 2.4 Local host 2.5 Bridge 2.6 Virtual Machine
3. Underpinning Skills	3.1 Installing OS 3.2 Connecting OS with network 3.3 Checking network connectivity
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	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	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	**OUCyS011L5V1: Apply Identity &Access Management**
Nominal Hours	**15 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply identity & access management. It specifically includes the tasks interpreting identity & access probation life cycle and applying access control management identification and authentication devices.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret identity & access probation life cycle	1. 1 Access control management system is interpreted 1. 2 Control physical and logical access to assets is interpreted 1. 3 Implement and manage **authorization mechanisms** is interpreted 1. 4 identity and access provisioning lifecycle is interpreted
2. Apply access control management Identification and Authentication devices	2.1 Access controls are applied for **information systems** 2.2 **Authentication mechanisms** are applied.
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Authorization mechanisms	2.1 Role Based Access Control (RBAC) 2.2 Rule-based access control 2.3 Mandatory Access Control (MAC) 2.4 Discretionary Access Control (DAC) 2.5 Attribute Based Access Control (ABAC)
2. Information systems	3.1 People 3.2 Devices 3.3 Network 3.4 Work load 3.5 Data
3. Authentication mechanisms	4.1 multi-factor authentication 4.2 Accountability
	4.3 Personal Information server security 4.4 802.1x (Radious, TACACS+ Server)
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 Interpreted identity and access provisioning lifecycle; 1.2 Applied access controls for information systems; 1.3 Applied authentication mechanisms;
1. Underpinning Knowledge	2.1 Access control management system 2.2 Authorization mechanisms 2.3 Access control management Identification and authentication devices
2. Underpinning Skills	3.1 Apply the concept of identity & access probation life cycle; 3.2 Apply the concept of authentication devices
3. 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
4. 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.
5. 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
6. 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	OUCyS003L4V1: Analyze Malicious Code
Nominal Hours	**30 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to analyze malicious code. It specifically includes the tasks of interpreting malicious code, identifying malwares, analyzing malicious code using tools and counter measuring for malware infections.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret Malicious Code	1.1 **Malware** is defined; 1.2 Threatens of Malicious Code is explained; 1.3 Process to Avoid Malicious Code is interpreted; 1.4 Malware propagation techniques is interpreted;
2. Create malwares	2.1 Virus Tools are Selected; 2.2 Program is unzipped as required; 2.3 **Process of malwares infection** is identified; 2.4 Malwares are created using required **tools;** 2.5 Malwares are detected using required tools;
3. Analyze Malicious Code using Tools	3.1 Infected systems is analyzed; 3.2 Malicious code is analyzed using required tools;
4. Implement countermeasures for Malware infections	4.1 Anti-malware is used to prevent malware; 4.2 Countermeasures for Malware infections are selected; 4.3 Selected countermeasures are implemented; 4.4 Malware is removed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Malware	1.1 Trojans 1.2 Trojan and Backdoors 1.3 Ransomware 1.4 Addware 1.5 Spyware 1.6 Virus 1.7 Worms 1.8 Rootkit
2. Process of malwares infection	2.1 Email attachment 2.2 Drive by download 2.3 Social media
3. Tools	Creation Tools: 3.1 Metasploit 3.2 Poison virus 3.3 Prorat 3.4 SMS-Flooder 3.5 IM-Flooder

	Detection Tools: 3.1 MALWARE CORPORA 3.2 Virustotal.com 3.3 ID serve 3.4 Telosintelligence.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 Identified process of malwares infection; 1.2 Detected Malwares by using required tools 1.1 Used Anti-malware to prevent malware 1.2 Implemented selected countermeasures
2. Underpinning Knowledge	2.4. Malware 2.5. Anti-malware 2.6. Phishing 2.7. Vishing 2.8. Smhishing 2.9. Social Engineering
3. Underpinning Skills	3.3 Installing Anti malware tools 3.4 Installing Malware detection 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	OUCyS017L5V1: Perform Digital Forensic
Nominal Hours	**60 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to perform digital forensic. It specifically include the tasks of interpreting digital forensic, interpreting Digital Evidence First Responders (DEFR) responsibility, performing OS forensics, Mobile Forensics, Graphics Forensics, Cloud Forensics and Email Forensics.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret Digital Forensic	1.1 Digital Forensic is interpreted; 1.2 Types of **Forensic** is identified; 1.3 Anti-forensic techniques are interpreted; 1.4 Chain of custody is interpreted; 1.5 Responsibilities of forensic Investigator are identified;
2. Interpret Digital Evidence First Responders (DEFR) responsibility	2.1 DEFR responsibilities are interpreted; 2.2 Data acquisition steps are interpreted; 2.3 Data acquisition steps are practiced;
3. Perform OS forensics	3.1 OS storage Disk is attached; 3.2 **OS Forensics Tools** are installed;
4. Perform Mobile Forensics	4.1 Mobile is connected; 4.2 **Mobile Forensics Tools** are identified as per requirement; 4.3 Mobile Forensics Tools are installed;
5. Perform Graphics Forensics	5.1 Image is selected; 5.2 Steganography is interpreted; 5.3 **Graphics Forensics Tools** are identified as per requirement; 5.4 Graphics Forensics Tools are installed;
6. Perform Cloud Forensics	6.1 Targeted Cloud is connected; 6.2 **Cloud Forensics Tools** are identified as per requirement; 6.3 Cloud Forensics Tools are installed;
7. Perform Email Forensics	7.1 Targeted E-mail server is connected; 7.2 **Email Forensics Tools** are identified as per requirement; 7.3 Email Forensics Tools are installed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Forensic	1.1 Web forensic 1.2 Network forensic 1.3 Database forensic

	1.4 IoT forensic
2. VM	1.5 Oracle Virtual Box 1.6 VmWare
3. OS Forensics Tools:	2.1 ProDiscover Basic 2.2 Autopsy 2.3 AccessData 2.4 FTK Imager
4. Mobile Forensics Tools	3.1 Andriller 3.2 Linux memory extractor (LIME)
5. Graphics Forensics Tool	4.1 Meta data analysis 4.2 Photo forensics 4.3 WaveSurfer 4.4 Steganalysis 4.5 AccessData FTK Imager
6. Cloud Forensics Tools	5.1 ThreatResponse (AWS) 5.2 FROST 5.3 SANSSIFT
7. Email Forensics Tools	6.1 MXToolbox 6.2 MailXaminer 6.3 ActiveInbox

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 Interpreted Digital Forensic 1.2 Performing OS forensics 1.3 Performing Mobile Forensics 1.4 Performing Graphics Forensics 1.5 Performing Cloud Forensics 1.6 Performing Cloud Forensics
2. Underpinning Knowledge	2.1 File systems of Storage Devices 2.2 Windows Registry 2.3 Image Header 2.4 Cloud infrastructure 2.5 Email Header
3. Underpinning Skills	2.6 Applying skills Paladin Portable OS 3.1 Applying skills solving problem of Hexadecimal Number System 3.2 Applying skills of File systems of Storage Devices 3.3 Applying skills of Windows Registry 3.4 Skills of prepare image header 3.5 Skills of prepare Email Header

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	OUCyS018L5V1: Apply Threat Hunting Concepts
Nominal Hours	**50 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to apply threat hunting concepts. It specifically includes the tasks of identifying Cyber Threat Hunting and articulate its value to an organization, interpreting Cyber threat hunting methodologies and techniques, analyzing Cyber Threat hunting, following Incident Response and Incident Handling and Incident Response, Interpreting Incident Handling, performing Incident Handling and performing Disaster Recovery.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Identify Cyber Threat Hunting and articulate its value to an organization	1.1 Cyber Threat Hunting Concepts are identified; 1.2 Threat Hunting Values to the Organizations are identified; 1.3 Threat Hunting Values to the Organizations are articulated;
2. Interpret Cyber threat hunting methodologies and techniques	2.1 Threat Hunting Methodologies are interpreted; 2.2 Threat Hunting Techniques are identified; 2.3 Threat Hunting Lifecycles are identified; 2.4 Threat Hunting Capabilities identified;
3. Analyze Cyber Threat hunting	3.1 Network Devices are identified; 3.2 Logs are collected; 3.3 Vulnerable Protocols are identified; 3.4 collected traffic are analyzed; 3.5 Threat Hunting for host-based cyber threat is analyzed; 3.6 Threat Hunting for Incident Handling is analyzed; 3.7 Cyber Threat hunting for Web Application is analyzed; 3.8 Brief Introduction to IOC/IOA are interpreted; 3.9 Types of IOC/IOA are identified;
4. Follow Incident Response and Incident Handling	4.1 Incident Response steps are identified using SOP; 4.2 Incidents are correlated; 4.3 **SIEM Components** are identified using **SIEM tools;** 4.4 Open source SIEM are installed using SOP; 4.5 SIEM Implementation phases are identified;
5. Interpret Incident Handling	5.1 Incident Handling is defined 5.2 Concept of Identification, Overview and Preparation of Incident Handling are interpreted 5.3 Incident Response **Cert Team** is interpreted

6. Perform Incident Handling	6.1 **Phases of Incident Handling** is explained 6.2 **Incident Elements Handling process** are classified 6.3 Incident handling is performed
7. Perform Disaster Recovery	7.1 Disaster Recovery is defined 7.2 Disaster Recovery Strategy and Policy is reviewed 7.3 **Disaster Recovery Steps** are explained 7.4 Disaster recovery is performed
Range of Variables	
Variable	**Range** (may include but not limited to):
1. SIEM Component	1.1 Report generation 1.2 Dashboard 1.3 rule setup 1.4 log collection 1.5 correlate
2. SIEM tools	2.1 AlienVault 2.2 Splunk 2.3 Logrythm 2.4 IBM qradar 2.5 RSA
3. Tools:	3.1 ARP 3.2 ICMP 3.3 TCP 3.4 DHCP 3.5 DNS 3.6 HTTPS 3.7 Mitre Attack 3.8 Cyber Kill Chain 3.9 SSH 3.10 SIP 3.11 RTP & 3.12 20 plus protocols detailed analysis
4. Cert Team	4.1 CSIRT 4.2 Bdcert 4.3 BGD e-govcirt 4.4 APCERT 4.5 OIC-CERT
5. Phases of Incident Handling	5.1 Acknowledgement and Planning 5.2 Risk Assessment 5.3 Containment 5.4 Eradication 5.5 Recovery 5.6 Lessons Learned 5.7 Report Writing

6. Incident Elements Handling process	6.1 Email Security Incidents 6.2 Web Application and server Incidents 6.3 Network Security Incidents 6.4 Malware Incidents 6.5 Cloud security Incident 6.6 Insider threats
7. Disaster Recovery Steps	7.1 Identify the Risk 7.2 Identify Critical Business Processes and Vital Applications 7.3 Create a Disaster Recovery Team and workstations 7.4 Determine the RPO and RTO 7.5 Designate Maximum Tolerable Downtime (MTD) 7.6 Implement Backup & Data Recovery Strategy 7.7 Perform a Business Impact Analysis (BIA) 7.8 Business Continuity Plan 7.9 Report Generation for Future reference

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 Cyber Threat Hunting 1.2 Identified Threat Hunting Techniques 1.3 Identified Vulnerable Protocols 1.4 Installed Open source SIEM using SOP
2. Underpinning Knowledge	2.1 Cyber Threat Hunting Concepts 2.2 Threat Hunting Methodologies 2.3 Vulnerable Protocols 2.4 Incident Response 2.5 Incident Handling
3. Underpinning Skills	3.1 Applying concept of Cyber Threat Hunting 3.2 Applying concept of Vulnerable Protocols 3.3 Applying concept of Incident Response
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	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 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