COMPETENCY STANDARD

FOR

Network and System Security

(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 **Network and System Security (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 guide

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

NSQF– National Skills Qualifications Framework

BNQF– Bangladesh National 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 Network and System Security (Cyber Security) 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	OUCyS012L5V1	Apply Network security Assessment	5	40
2	OUCyS015L5V1	Apply Cyber Security Risk Assessment	5	35
3	OUCyS019L5V1	Apply Social Engineering	5	15
4	OUCyS020L5V1	Apply Cloud security Concepts	5	30
5	OUCyS016L5V1	Interpret Cryptography	5	30
6	OUCyS010L5V1	Perform Pen Testing	5	60
7	OUCyS018L5V1	Apply Threat hunting concepts	5	50
8	OUCyS0023L5V1	Interpret IT Security Auditing	5	30
Total Nominal Learning Hours				**250**

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)
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
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
OUCyS020L5V1	Apply Cloud security Concepts	1. Interpret Cloud Computing concept and Roles 2. Identify Key Characteristics of Cloud Computing 3. Identify Building Block of Cloud Technologies 4. Identify Cloud Service Capabilities and Deployment Models 5. Practice cloud computing activities and services 6. Apply cloud security	30
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
OUCyS010L5V1	Perform Pen Testing	1. Identify Penetration Testing Tools 2. Perform Penetration Testing 3. Prepare VAPT report	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

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 Apply the Governance and Management of IT audit	30

The Generic Competencies

The Sector Specific Competencies

The Occupation Specific Competencies

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	6.1 **Management Security** is interpreted; 6.2 **Network devices** are interpreted; 6.3 Basic network **protocol** is identified; 6.4 Secure Network implementation process is interpreted by packet tracer; 6.5 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	3.1 Apply the concept of Cyber Security risk 3.2 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	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	OUCyS020L5V1: Apply Cloud Security Concepts
Nominal Hours	**30 Hours**
Unit Descriptor	This unit covers the knowledge, skills and attitudes required to Apply cloud security concepts. It specifically includes the tasks of Interpreting Cloud Computing concept and roles, Identifying Key Characteristics of Cloud Computing, Identifying Building Block of Cloud Technologies, Identifying Cloud Service Capabilities and Deployment Models, Practicing cloud computing activities and services and applying cloud security.
Elements of Competency	**Performance Criteria** **Bold and Underlined** terms are elaborated in the Range of Variables
1. Interpret Cloud Computing concept and Roles	1.1 Cloud computing concepts is interpreted 1.2 **Types of cloud** computing are identified 1.3 Types of cloud services are identified 1.4 Cloud service providers and their services are interpreted 1.5 **Cloud computing threats** are identified
2. Interpret Key Characteristics of Cloud Computing	2.1 On-Demand Self-Service is interpreted; 2.2 Easy Maintenance is identified; 2.3 Scalability and Rapid Elasticity is interpreted; 2.4 Measured And Reporting Service is interpreted; 2.5 Large Network Access is interpreted;
3. Identify Building Block of Cloud Technologies	3.1 Cloud Development Basics are interpreted; 3.2 Common Pitfalls are identified; 3.3 Common Cloud Vulnerabilities are interpreted; 3.4 Cloud Data Life Cycle Phases are interpreted; 3.5 Data Dispersion is defined; 3.6 Application capability types, platform capability types, infrastructure capability types are defined; 3.7 Cloud Service Categories are identified;
4. Identify Cloud Service Capabilities and Deployment Models	4.1 User provisioning and management are simplified; 4.2 Entitlements across platforms are synchronized 4.3 Enforcement of identity-based perimeter are identified; 4.4 Flexible customer access enablement is interpreted; 4.5 public, private, community, and hybrid deployment models are defined;
5. Practice cloud computing activities and services	5.1 Start with a high-value, tactical problem with a public cloud is solved; 5.2 Address and plan for cloud security upfront are interpreted; 5.3 Include as many people as you can in the review process is included;

6. Apply cloud security	6.1 Multi-Factor authentication (MFA) is deployed; 6.2 User Access to Improve Cloud Computing Security is managed; 6.3 Anti-Phishing Training for Employees on a regular basis is provided; 6.4 End User Activities with Automated Solution to Detect Intruders is monitored; 6.5 Cloud Security issues and threats are analyzed;
Range of Variables	
Variable	**Range** (may include but not limited to):
1. Types of cloud	1.1 Infrastructure as a Service (IaaS) 1.2 Platform as a Service (PaaS) 1.3 Serverlessand 1.4 Software as a Service (SaaS)
2. Cloud computing threats	2.1 Unauthorized Access. 2.2 Insecure Interfaces/APIs. 2.3 Hijacking of Accounts. 2.4 Lack of Visibility. 2.5 External Sharing of Data. 2.6 Malicious Insiders 2.7 Parameters tampering 2.8 Input validation
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 types of cloud computing; 1.2 Identified Cloud computing threats; 1.3 Identified Common Pitfalls; 1.4 Deployed Multi-Factor authentication (MFA);
2. Underpinning Knowledge	2.1. Cloud computing 2.2. Infrastructure as a Service (IaaS) 2.3. Platform as a Service (PaaS) 2.4. Serverlessand 2.5. Software as a Service (SaaS
3. Underpinning Skills	3.1 Applying concept of Cloud computing 3.2 Applying concept of Common Cloud Vulnerabilities

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	**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 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: 5.1 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