# NATIONAL SKILLS QUALIFICATION

# LEVEL 5

# TITLE:

**Cybersecurity Engineer**

# YEAR: 2024

## NATIONAL SKILLS QUALIFICATION

## NSQ LEVEL 5 Cybersecurity Engineer

# General Information

### Qualification Purpose

*This qualification is designed to develop professionals who possess the skills, knowledge, and capabilities to secure enterprise-level systems, networks, and data.*

### Qualification Objectives

The learner should be able to:

i. Comply with organizational policies, standards, and frameworks.
ii. Analyze risks and vulnerabilities in network, system, and application infrastructures.
iii. Implement robust cybersecurity strategies.
iv. Evaluate emerging cybersecurity threats and technologies.
v. Supervise incident responses, recovery, and forensic investigations.

## Mandatory Units

| Unit No | Ref. Number | NOS Title | Credit Value | Learning Hours | Remark |
|---|---|---|---|---|---|
| Unit 01 | IS/CCE/01/L5 | Occupational Health and Safety | 2 | 20 | Mandatory |
| Unit 02 | IS/CCE/02/L5 | Communication in the Work Environment | 2 | 20 | Mandatory |
| Unit 03 | IS/CCE/03/L5 | Teamwork | 2 | 20 | Mandatory |
| Unit 04 | IS/CCE/04/L5 | Cybersecurity Governance | 6 | 60 | Mandatory |
| Unit 05 | IS/CCE/05/L5 | Network Security Management | 6 | 60 | Mandatory |
| Unit 06 | IS/CCE/06/L5 | Information Security Management | 6 | 60 | Mandatory |
| Unit 07 | IS/CCE/07/L5 | Threat Intelligence and Monitoring | 6 | 60 | Mandatory |
| Unit 08 | IS/CCE/08/L5 | Incident Management and Forensic Investigation | 6 | 60 | Mandatory |
| | | | **36** | **360** | |

# National Skills Qualification
# Level 5 Cybersecurity Engineer

## Unit 01: Health, Safety and Environment
## Unit Reference Number: IS/CCE/01/L5
## NSQ Level: 5
## Credit Value: 2
## Guided Learning Hours: 20

## Unit Purpose:

*This unit covers the safe working practices and procedures to be observed when working in an ICT environment and the statutory requirement, risk assessment procedures and relevant requirements.*

## Unit Assessment Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out.

## Assessment Methods:

- Observation
- Professional Discussion
- Question and Answer
- Assignment (ASS), etc.

**Unit 01: Health, Safety and Environment**

| Learning Objective (LO) | | Performance Criteria (PC) | Evidence Type | | | | Ref. Page No | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Understand safety precautions in workplace** | **1.1** | Dress properly to the work environment. | | | | | | | | |
| | **1.2** | Always Work safely, complying with health and safety and other relevant regulations and guidelines. | | | | | | | | |
| | **1.3** | Get any cuts, grazes and wounds treated by the appropriate and qualified person. | | | | | | | | |
| | **1.4** | Report illness and infection promptly to the appropriate persons. | | | | | | | | |
| **LO2**<br>**Know how to maintain personal health and hygiene** | **2.1** | Summarise own responsibility under the Health and Safety Act as it relates to own occupation | | | | | | | | |
| | **2.2** | State general rules on hygiene that must be followed. | | | | | | | | |
| | **2.3** | Explain the importance of maintaining good personal hygiene. | | | | | | | | |
| | **2.4** | Describe how to deal with cuts, grazes and wounds and why it is important to do so | | | | | | | | |
| **LO3**<br>**Be able to help maintain a hygienic, safe and secure workplace.** | **3.1** | State the importance of working in a healthy, safe and hygienic workplace. | | | | | | | | |
| | **3.2** | Promote health, hygiene and safety procedures during work. | | | | | | | | |
| | **3.3** | Practice emergency procedures during work. | | | | | | | | |
| | **3.4** | Ensure that organizational security procedures are followed. | | | | | | | | |
| | **3.5** | Ensure the disposal of waste and pollution control with organic and inorganic waste disposal methods. | | | | | | | | |
| **LO4**<br>**Prevent hazards and maintain safe and secure workplace** | **4.1** | Supervise identification of any hazards or potential hazards and deal with these correctly. | | | | | | | | |
| | **4.2** | State where information about health and safety in your workplace can be obtained. | | | | | | | | |
| | **4.3** | Describe the type of hazards in the workplace that may occur and how to deal with them. | | | | | | | | |
| | **4.4** | Identify hazards that can be dealt with personally and those that should be reported to appropriate personnel. | | | | | | | | |
| | **4.5** | Follow organization procedures on how to warn other people about hazards and why this is important | | | | | | | | |
| | **4.6** | State why accidents and near accidents should be reported to the | | | | | | | | |

| **Learning Objective (LO)** | | **Performance Criteria (PC)** | **Evidence Type** | | | | **Ref. Page No** | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | appropriate personnel. | | | | | | | | |
| | **4.7** | Describe the type of emergencies that may happen in the workplace and how to deal with them. | | | | | | | | |
| | **4.8** | State where to find the first-aid equipment and locate the authorized personnel. | | | | | | | | |
| | **4.9** | Lift and handle materials in line with work environment procedure. | | | | | | | | |
| | **4.10** | State other ways of working safely that are relevant to own position responsibility and its importance. | | | | | | | | |
| | **4.11** | Describe organizational emergencies procedures, in particular fire, and how these should be followed. | | | | | | | | |
| | **4.12** | State the possible causes for fire in the workplace. | | | | | | | | |
| | **4.13** | Describe how to minimize the possibility of fire in the workplace. | | | | | | | | |
| | **4.14** | State where to find the alarms and how to set them up. | | | | | | | | |
| | **4.15** | State why a fire should never be approached unless it is safe to. | | | | | | | | |
| | **4.17** | Describe organizational security procedures and why these are important | | | | | | | | |
| | **4.18** | State the importance of reporting all usual or non-routine incidents to the appropriate personnel. | | | | | | | | |
| Learner's Signature | | | Date | | | | | | | |
| Assessor's Signature | | | Date | | | | | | | |
| IQA's Signature | | | Date | | | | | | | |
| EQA's Signature | | | Date | | | | | | | |

# National Skills Qualification
# Level 5 Cybersecurity Engineer

## Unit 02: Communication and Interpersonal Skill
## Unit Reference Number: IS/CCE/02/L5
## NSQ Level: 5
## Credit Value: 2
## Guided Learning Hours: 20

## Unit Purpose:

*This units seeks to develop the competency of the learner to be able to express oneself fluently in a well-defined manner understandable to the client with problems to solve and with group of colleagues.*

## Unit Assessment Requirements/Evidence Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

1. Direct Observation (DO)
2. Question and Answer (QA)
3. Witness Testimony (WT)
4. Reflective Journal (RJ)
5. Assignment (ASS)

## Unit 02: Communication and Interpersonal Skill

| Learning Objective (LO) | | Performance Criteria (PC) | Evidence Type | | | | | Ref. Page No | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1 Communicate with Client** | **1.1** | Notify client about new systems features to keep them up to date. | | | | | | | | | |
| | **1.2** | Notify client about new systems features to keep them up to date. | | | | | | | | | |
| | **1.3** | Communicate with the client about any changes on the website/application | | | | | | | | | |
| | **1.4** | Confirm that no request from client is pending. | | | | | | | | | |
| | **1.5** | Communicate to the team about the market trends to ensure that they are kept up to date. | | | | | | | | | |
| **LO2 Communicate with Peer/Team Members** | **2.1** | Check that all team members/peers are in line with the requirements | | | | | | | | | |
| | **2.2** | Give clear directions to team members/peers to follow | | | | | | | | | |
| | **2.3** | Check that a proper mechanism is in place to motivate all team members | | | | | | | | | |
| | **2.4** | Provide a suitable and comfortable work environment for peers and team members | | | | | | | | | |
| | **2.5** | Give report of team members activities | | | | | | | | | |
| **LO3 Communicate with Managers** | **3.1** | Provide a standard operating procedure for communication with the seniors. | | | | | | | | | |
| | **3.2** | Follow all instructions given by seniors in each job role. | | | | | | | | | |
| | **3.3** | Execute all instructions coming from the seniors using proper mechanism | | | | | | | | | |
| | **3.4** | Communicate all the emergencies and bugs/updates to the relevant Managers | | | | | | | | | |
| Learner’s Signature | | | | Date | | | | | | | |
| Assessor’s Signature | | | | Date | | | | | | | |
| IQA’s Signature | | | | Date | | | | | | | |
| EQA’s Signature | | | | Date | | | | | | | |

# National Skills Qualification

# Level 5 Cybersecurity Engineer

## Unit 03: Teamwork
## Unit Reference Number: IS/CCE/03/L5
## NSQ Level: 5
## Credit Value: 2
## Guided Learning Hours: 20

## Unit Purpose:

*The purpose for this unit is to impact into the learner the necessary skills, knowledge and understanding required to develop team spirit and positive working relationship with colleagues.*

## Unit Assessment Requirements/Evidence Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

1. Direct Observation (DO)
2. Question and Answer (QA)
3. Witness Testimony (WT)
4. Reflective Journal (RJ)
5. Assignment (ASS)

## Unit 03: Teamwork

| **Learning Objective (LO)** | | **Performance Criteria (PC)** | **Evidence Type** | | | | | **Ref. Page No** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Positive working relationship with colleagues** | **1.1** | Identify the need for developing positive working relationship with colleagues | | | | | | | | | |
| | **1.2** | Recognize the importance of relating with other people in a way that makes them feel valued and respected | | | | | | | | | |
| | **1.3** | Assist team members when required. | | | | | | | | | |
| | **1.4** | Report to the personnel when request for assistance fall outside area of responsibility | | | | | | | | | |
| | **1.5** | Communicate information to colleagues about own work that might affect others | | | | | | | | | |
| **LO2**<br>**Take responsibility within the team** | **2.1** | Recognize own role and responsibilities within team | | | | | | | | | |
| | **2.2** | Perform individual tasks in line with the team rules and regulations. | | | | | | | | | |
| | **2.3** | Participate effectively in teamwork | | | | | | | | | |
| **LO3**<br>**Compliance with policy of organisation** | **3.1** | Work in line with organizational standard | | | | | | | | | |
| | **3.2** | Use organizational code of practice | | | | | | | | | |
| | **3.3** | Explain organizational code of conduct | | | | | | | | | |
| Learner’s Signature | | | | Date | | | | | | | |
| Assessor’s Signature | | | | Date | | | | | | | |
| IQA’s Signature | | | | Date | | | | | | | |
| EQA’s Signature | | | | Date | | | | | | | |

## National Skills Qualification
## Level 5 Cybersecurity Engineer

**Unit 04: Cybersecurity Governance**
**Unit Reference Number: IS/CCE/04/L5**
**NSQ Level: 5**
**Credit Value: 6**
**Guided Learning Hours: 60**

### Unit Purpose:

*This unit aims to equip learner with knowledge, skills and capabilities to comply with standards and create security policies, while adhering to legal and industry cybersecurity mandates.*

### Unit Assessment Requirements/Evidence Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

1. Direct Observation (DO)
2. Question and Answer (QA)
3. Witness Testimony (WT)
4. Assignment (ASS)

## Unit 04: Cybersecurity Governance

| **Learning Objective (LO)** | | **Performance Criteria (PC)** | **Evidence Type** | | | | | **Ref. Page No** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Demonstrate understanding of security compliance frameworks** | **1.1** | Demonstrate understanding of cybersecurity frameworks like NIST 2.0, PCI DSS v4.0, CIS, CMMC, etc. | | | | | | | | | |
| | **1.2** | Analyse the role of cybersecurity governance within an organization. | | | | | | | | | |
| | **1.3** | Assess risk management policies and procedures. | | | | | | | | | |
| | **1.4** | Describe the impact of cybersecurity laws and regulations on business operations. | | | | | | | | | |
| | **1.5** | Advise stakeholders on implementing governance structures for security compliance. | | | | | | | | | |
| **LO2**<br>**Develop policies and strategies for security governance** | **2.1** | Create security policies that align with organizational objectives. | | | | | | | | | |
| | **2.2** | Evaluate the effectiveness of current security frameworks. | | | | | | | | | |
| | **2.3** | Implement security training programs to promote policy compliance **and awareness** | | | | | | | | | |
| | **2.4** | Support the creation of incident response plans in compliance with security governance. | | | | | | | | | |
| | **2.5** | Inspect policy effectiveness through internal audits. | | | | | | | | | |
| **LO3**<br>**Evaluate cybersecurity risk management frameworks** | **3.1** | **Identify and** Analyse potential risks related to cybersecurity threats. | | | | | | | | | |
| | **3.2** | Assess the likelihood and impact of security risks. | | | | | | | | | |
| | **3.3** | Develop risk mitigation strategies for identified threats. | | | | | | | | | |
| | **3.4** | Explain risk management tools and models. | | | | | | | | | |
| | **3.5** | Apply appropriate risk management model. | | | | | | | | | |
| | **3.6** | Evaluate the organization's risk tolerance and security posture. | | | | | | | | | |
| **LO4**<br>**Plan and develop compliance monitoring mechanisms** | **4.1** | Select appropriate tools to monitor cybersecurity compliance. | | | | | | | | | |
| | **4.2** | Create processes to audit and assess cybersecurity measures. | | | | | | | | | |
| | **4.3** | **Demonstrat your understanding** ongoing monitoring and adjustments to risk management procedures. | | | | | | | | | |
| | **4.4** | Compare different approaches to | | | | | | | | | |

| **Learning Objective (LO)** | | **Performance Criteria (PC)** | **Evidence Type** | | | | | **Ref. Page No** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | compliance monitoring. | | | | | | | | | |
| | **4.5** | Analyse monitoring  results and propose improvements. | | | | | | | | | |

| | |
|---|---|
| Learner’s Signature | Date |
| Assessor’s Signature | Date |
| IQA’s Signature | Date |
| EQA’s Signature | Date |

# National Skills Qualification
# Level 5 Cybersecurity Engineer

## Unit 05: Network Security Management
## Unit Reference Number: IS/CCE/05/L5
## NSQ Level: 5
## Credit Value: 6
## Guided Learning Hours: 60

## Unit Purpose:

*Learners will master the knowledge and skills to design, implement, and maintain secure network infrastructures.*

## Unit Assessment Requirements/Evidence Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

1. Direct Observation (DO)
2. Question and Answer (QA)
3. Witness Testimony (WT)
4. Assignment (ASS)

## Unit 05: Network Security Management

| Learning Objective (LO) | | Performance Criteria (PC) | Evidence Type | | | | | Ref. Page No | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Implement secure network architectures** | **1.1** | **Access** the integrity of network security protocols and firewalls. | | | | | | | | | |
| | **1.2** | Analyse network vulnerabilities and threat vectors. | | | | | | | | | |
| | **1.3** | Create a secure network architecture based on organizational requirements. | | | | | | | | | |
| | **1.4** | Inspect network traffic for suspicious activities and potential breaches. | | | | | | | | | |
| | **1.5** | **Reviwe** network configuration to enhance security measures. | | | | | | | | | |
| **LO2**<br>**Evaluate the effectiveness of network security controls** | **2.1** | **Access** network security breaches and suggest corrective actions. | | | | | | | | | |
| | **2.2** | Compare intrusion detection and prevention systems (IDPS). | | | | | | | | | |
| | **2.3** | Assess firewall and router configurations for gaps in security. | | | | | | | | | |
| | **2.4** | Analyse network segmentation to minimize threat impact. | | | | | | | | | |
| | **2.5** | Observe and interpret the performance of network security controls. | | | | | | | | | |
| **LO3**<br>**Implement secure access management** | **3.1** | Develop secure authentication and authorization mechanisms. | | | | | | | | | |
| | **3.2** | **Explain how to** adherence to least privilege access principles. | | | | | | | | | |
| | **3.3** | Investigate access control issues and take appropriate actions. | | | | | | | | | |
| | **3.4** | Implement multi-factor authentication (MFA) across network systems. | | | | | | | | | |
| | **3.5** | Support user awareness programs on secure access management. | | | | | | | | | |
| **LO4**<br>**Operate and maintain network security infrastructure** | **4.1** | Implement routine maintenance of network security tools. | | | | | | | | | |
| | **4.2** | **Implement** automated mechanisms for continuous monitoring of network health. | | | | | | | | | |
| | **4.3** | **Manage** the operation of VPNs, IDS, IPS, and firewalls. | | | | | | | | | |
| | **4.4** | Supervise network administrators to ensure compliance with security protocols. | | | | | | | | | |
| | **4.5** | Plan for the upgrade and renewal of network security systems. | | | | | | | | | |

Learner's Signature Date

| Learning Objective (LO) |  | Performance Criteria (PC) | Evidence Type |  | Ref. Page No |
|---|---|---|---|---|---|

|  |  |
|---|---|
| Assessor’s Signature | Date |
| IQA’s Signature | Date |
| EQA’s Signature | Date |

## National Skills Qualification
## Level 5 Cybersecurity Engineer

**Unit 06: Information Security Management**
**Unit Reference Number: IS/CCE/06/L5**
**NSQ Level: 5**
**Credit Value: 6**
**Guided Learning Hours: 60**

### Unit Purpose:

*Learners will acquire the skills to assess information security risks, design data protection systems, and respond to data breaches to maintain data integrity and confidentiality*

### Unit Assessment Requirements/Evidence Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

5. Direct Observation (DO)
6. Question and Answer (QA)
7. Witness Testimony (WT)
8. Assignment (ASS)

## Unit 06: Information Security Management

| Learning Objective (LO) | | Performance Criteria (PC) | Evidence Type | | | | | Ref. Page No | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Assess information security risks** | **1.1** | Analyse organizational data to identify potential risks. | | | | | | | | | |
| | **1.2** | Evaluate the impact of data breaches on operations, f**inancial impacts reputation, etc** | | | | | | | | | |
| | **1.3** | **Describe the process of data classification and prioritization.** | | | | | | | | | |
| | **1.4** | Support the organization in complying with **applicable** data protection laws. | | | | | | | | | |
| | **1.5** | **Develop risk mitigation strategies for data protection.** | | | | | | | | | |
| **LO2**<br>**Implement data protection measures** | **2.1** | ,Investigate data protection systems for weaknesses | | | | | | | | | |
| | **2.2** | Ensure the encryption of critical data assets. | | | | | | | | | |
| | **2.3** | **Semulute** policies to protect sensitive information. | | | | | | | | | |
| | **2.4** | Implement robust access control for sensitive data. | | | | | | | | | |
| | **2.5** | Plan incident response processes for data breaches. | | | | | | | | | |
| **LO3**<br>**Operate data protection systems** | **3.1** | Participate in data protection measures such as the maintenance, encryption of systems and backups. | | | | | | | | | |
| | **3.2** | Analyse the performance of data protection measures. | | | | | | | | | |
| | **3.3** | Compare different encryption algorithms and their effectiveness. | | | | | | | | | |
| | **3.4** | Implement measures to prevent data loss.( Policies and DLP etc) | | | | | | | | | |
| | **3.5** | Interpret reports from data protection monitoring systems. | | | | | | | | | |
| **LO4**<br>**Ensure compliance with data protection regulations** | **4.1** | Ensure alignment with GDPR, HIPAA, **NDPA or any other** local data laws. | | | | | | | | | |
| | **4.2** | Develop internal data protection audits and inspections **approches** | | | | | | | | | |
| | **4.3** | Evaluate the organization's compliance posture. | | | | | | | | | |
| | **4.4** | Implement necessary measures to address compliance gaps. | | | | | | | | | |
| | **4.5** | Advise stakeholders on the implications of data protection regulations. | | | | | | | | | |
| Learner’s Signature | | | | Date | | | | | | | |
| Assessor’s Signature | | | | Date | | | | | | | |

| Learning Objective (LO) |  | Performance Criteria (PC) | Evidence Type |  | Ref. Page No |
|---|---|---|---|---|---|
| IQA’s Signature |  |  | Date |  |  |
| EQA’s Signature |  |  | Date |  |  |

## National Skills Qualification

## Level 5 Cybersecurity Engineer

**Unit 07: Threat Intelligence and Monitoring**
**Unit Reference Number: IS/CCE/07/L5**
**NSQ Level: 5**
**Credit Value: 6**
**Guided Learning Hours: 60**

### Unit Purpose:

*The learner will gain an understanding of how to detect, monitor, and respond to emerging cybersecurity threats.*

### Unit Assessment Requirements/Evidence Requirements:

Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

1. Direct Observation (DO)
2. Question and Answer (QA)
3. Witness Testimony (WT)
4. Assignment (ASS)

## Unit 07: Threat Intelligence and Monitoring

| **Learning Objective (LO)** | | **Performance Criteria (PC)** | **Evidence Type** | | | | | **Ref. Page No** | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Analyse emerging cybersecurity threats** | **1.1** | Investigate new attack vectors and threat actors. | | | | | | | | | |
| | **1.2** | Compare emerging cybersecurity technologies. | | | | | | | | | |
| | **1.3** | Evaluate the potential impact of new threats on the organization. | | | | | | | | | |
| | **1.4** | Create threat models to understand potential vulnerabilities. | | | | | | | | | |
| | **1.5** | Support continuous threat monitoring efforts. | | | | | | | | | |
| **LO2**<br>**Implement threat detection systems** | **2.1** | Plan the integration of threat intelligence platforms (TIPs). | | | | | | | | | |
| | **2.2** | Implement automated threat detection mechanisms. | | | | | | | | | |
| | **2.3** | Compare and select intrusion detection systems. | | | | | | | | | |
| | **2.4** | Operate threat intelligence feeds for real-time monitoring. | | | | | | | | | |
| | **2.5** | Evaluate the effectiveness of implemented detection systems. | | | | | | | | | |
| **LO3**<br>**Response to cyber incidents** | **3.1** | Ensure proper incident response procedures are followed. | | | | | | | | | |
| | **3.2** | Analyse cyber incident reports for root causes. | | | | | | | | | |
| | **3.3** | Investigate compromised systems and contain threats. | | | | | | | | | |
| | **3.4** | Develop forensic investigation reports. | | | | | | | | | |
| | **3.5** | Support recovery efforts after incidents. | | | | | | | | | |
| **LO4**<br>**Supervise proactive threat hunting** | **4.1** | Plan proactive threat-hunting activities. | | | | | | | | | |
| | **4.2** | Investigate malicious activity (**systems for hidden** ). | | | | | | | | | |
| | **4.3** | Create strategies for continuous threat-hunting improvements. | | | | | | | | | |
| | **4.4** | Supervise junior security analysts during threat-hunting missions. | | | | | | | | | |
| | **4.5** | Evaluate and interpret the results of threat-hunting exercises. | | | | | | | | | |
| Learner's Signature | | | | Date | | | | | | | |
| Assessor's Signature | | | | Date | | | | | | | |
| IQA's Signature | | | | Date | | | | | | | |
| EQA's Signature | | | | Date | | | | | | | |

## National Skills Qualification
## Level 5 Cybersecurity Engineer

## Unit 08: Incident Management and Forensic Investigation
## Unit Reference Number: IS/CCE/08/L5
## NSQ Level: 5
## Credit Value: 6
## Guided Learning Hours: 60

### Unit Purpose:
*The learner will gain an understanding of incident management and digital forensics and acquire the skills to plan, develop, and execute incident response strategies,*

### Unit Assessment Requirements/Evidence Requirements:
Assessment must be carried out in real workplace environment in which learning and human development is carried out. Assessment methods to be used include:

1. Direct Observation (DO)
2. Question and Answer (QA)
3. Witness Testimony (WT)
4. Assignment (ASS)

## Unit 08: Incident Management and Forensic Investigation

| Learning Objective (LO) | | Performance Criteria (PC) | Evidence Type | | | | | Ref. Page No | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **LO1**<br>**Develop incident response procedures** | **1.1** | Create incident response protocols and escalation paths. | | | | | | | | | |
| | **1.2** | Ensure incident response plans comply with regulatory requirements. | | | | | | | | | |
| | **1.3** | Develop communication plans for stakeholders during incidents. | | | | | | | | | |
| | **1.4** | Select appropriate tools for incident management. | | | | | | | | | |
| | **1.5** | Initiate drills to test incident response readiness. | | | | | | | | | |
| **LO2**<br>**Investigate security incidents and breaches** | **2.1** | Examine logs and digital evidence for signs of compromise. | | | | | | | | | |
| | **2.2** | Develop root cause analysis reports. | | | | | | | | | |
| | **2.3** | Support collaboration with external cybersecurity teams during incidents. | | | | | | | | | |
| | **2.4** | **Obtained** fornensic evidence that complies with legal requirements. | | | | | | | | | |
| | **2.5** | Investigate the scope of data loss during breaches | | | | | | | | | |
| **LO3**<br>**Supervise post-incident recovery efforts** | **3.1** | Evaluate the organization’s readiness for post-incident recovery. | | | | | | | | | |
| | **3.2** | Create plans for restoring affected systems and services. | | | | | | | | | |
| | **3.3** | Ensure continuity and disaster recovery procedures are in place. | | | | | | | | | |
| | **3.4** | Supervise the implementation of lessons learned from incidents. | | | | | | | | | |
| | **3.5** | Support the update of incident response plans post-recovery. | | | | | | | | | |
| **LO4**<br>**Evaluate incident management processes** | **4.1** | Interpret post-incident reports to identify process improvements. | | | | | | | | | |
| | **4.2** | Compare different incident management frameworks. | | | | | | | | | |
| | **4.3** | Ensure alignment between incident management and organizational strategy. | | | | | | | | | |
| | **4.4** | Assess the effectiveness of current incident management procedures. | | | | | | | | | |
| | **4.5** | **Provied** recommendations for improving incident response capabilities. | | | | | | | | | |

| | |
|---|---|
| Learner’s Signature | Date |
| Assessor’s Signature | Date |
| IQA’s Signature | Date |

| Learning Objective (LO) |  | Performance Criteria (PC) | Evidence Type |  | Ref. Page No |
|---|---|---|---|---|---|
| EQA’s Signature |  |  | Date |  |  |

## CIRITIQUE TEAM LIST

| SN | NAME | ADDRESS | EMAIL AND PHONE |
|---|---|---|---|
| 1 | Ikechukwu Jacob Umesi | Mo Solicitors 4 Trinity Close Olodi Apapa, Lagos | iykejacob@gmail.com<br>08055900895 |
| 2 | Frank Iheonu | Inits Limited 283 Herbert Macaulay Way, Yaba | iheonufrank@gmail.com<br>07036999294 |
| 3 | Chibueze Princewill Okereke | Zenith Bank Group (Zenpay) 5 Roluga Street, Soluyi, Gbagada, Lagos | okerekeprincewill@hotmail.com<br>07025768487 |
| 4 | Emmanuel C. Amadi | Federal University of Technology, Owerri | emmanuel.amadi@futo.edu.ng<br>08062142392 |
| 5 | Engr. Lawal Abdullahi | Zenith Kad Ict Hub Kaduna | ocplawal@gmail.com<br>08035169089 |
| 6 | Muhammad Musa | NBTE | muhammadwaziri@msn.com<br>08033671027 |
| 7 | MUHAMMAD, BILYAMINU MUSA | NBTE | mahogany@gmail.com<br>09036071291 |
| 8 | Muhammad Bello Aliyu | CPN | mbacaspet@gmail.com<br>08039176984 |
| 9 | BENJAMIN, Prince Chukwudindu | CPN | pco.benjamin@gmail.com<br>08132850544 |
| 10 | Amoo, Taofeek | CPN | taofeekamoo@gmail.com<br>08053370334 |
| 11 | Olatunji Abibat | CPN | adehabb@gmail.com<br>08054263602 |
| 12 | Linda Ngbeken | CPN | excel4all2000@yahoo.com<br>08128219274 |

## VALIDATION TEAM LIST

| SN | NAME | ADDRESS | EMAIL AND PHONE |
|---|---|---|---|
| 1 | Dr. Musa Hatim Koko | NBTE | 08039606948 |
| 2 | Aliyu Imafidor Hassan | NBTE | 08065089233 |
| 3 | Oje Emmanuel | MINC | 07031350900 |
| 4 | Oluwafunmi Grace Akinda | Galaxy Backbone | 08182904573 |
| 5 | Fatai Akinsola | Galaxy Backbone | 08023220648 |
| 6 | Emmauel O. Okoi | NDC | 07036740799 |
| 7 | Remigius C. Okoro | NCC | |
| 8 | Kayode A. Oni | ONSA | 08034339128 |
| 9 | Pozing Zingman | NIMC | 07034612244 |
| 10 | Abbas Lawal | NGCERT | 08037007718 |
| 11 | Rani Mohammed | ONSA | 08068076158 |
| MUHAMMAD, BILYAMINU MUSA | | NBTE | mahogany@gmail.com<br>09036071291 |
| Muhammad Bello Aliyu | | CPN | mbacaspet@gmail.com<br>08039176984 |
| BENJAMIN, Prince Chukwudindu | | CPN | pco.benjamin@gmail.com<br>08132850544 |