NATIONAL SKILLS QUALIFICATION

LEVEL 5

TITLE:

Cloud Security Engineer

YEAR: 2024

NATIONAL SKILLS QUALIFICATION

NSQ LEVEL 5 Cloud Security Engineer

General Information

Qualification Purpose

The qualification is to equip individuals with advanced knowledge and technical expertise to design, implement, and manage secure cloud infrastructure, ensuring data protection, compliance, and risk mitigation in cloud environments while preparing them for leadership roles in cybersecurity operations.

Qualification Objectives

The learner should be able to:

i. Comply with relevant industry standards and organizational policies.
ii. Assess risks and vulnerabilities specific to cloud environments.
iii. Manage security architectures for cloud platforms.
iv. Investigate cloud-based threats, incidents, and mitigation strategies.
v. Advise stakeholders in cloud security design, governance, and decision-making processes.
vi. Supervise incident responses for cloud infrastructure, ensuring business continuity and recovery.

Mandatory Units

Unit No	Ref. Number	NOS Title	Credit Value	Learning Hours	Remark
Unit 01	IS/CS/01/L5	Occupational Health and Safety	2	20	Mandatory
Unit 02	IS/CS/02/L5	Communication in the Work Environment	2	20	Mandatory
Unit 03	IS/CS/03/L5	Teamwork	2	20	Mandatory
Unit 04	IS/CS/04/L5	Cloud Security Compliance and Governance	6	60	Mandatory
Unit 05	IS/CS/05/L5	Cloud Security Architecture and Design	6	60	Mandatory
Unit 06	IS/CS/06/L5	Cloud Threat Management and Monitoring	6	60	Mandatory
Unit 07	IS/CS/07/L5	Cloud Security Incident Response and Recovery	6	60	Mandatory
Unit 08	IS/CS/08/L5	Cloud Identity and Access Management (IAM)	6	60	Mandatory
Unit 09	IS/CS/09/L5	Cloud Data Security and Privacy	6	60	Mandatory
			42	**420**	

National Skills Qualification
Level 5 Cloud Security Engineer

Unit 01: Health, Safety and Environment

Unit Reference Number: IS/CS/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 Understand safety precautions in workplace	**1.1**	Dress properly to the work environment.								
	1.2	Comply 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 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 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 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								

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type				Ref. Page No			
		accidents should be reported to the 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 Cloud Security Engineer

Unit 02: Communication and Interpersonal Skill
Unit Reference Number: IS/CS/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 a given 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 Cloud Security Engineer

Unit 03: Teamwork
Unit Reference Number: IS/CS/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 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 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 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 Cloud Security Engineer

Unit 04: Cloud Security Compliance and Governance
Unit Reference Number: IS/CS/04/L5
NSQ Level: 5
Credit Value: 6
Guided Learning Hours: 60

Unit Purpose:
Learners will gain the skills to develop, implement, and monitor governance and compliance programs within cloud environments.

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: Cloud Security Compliance and Governance

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type					Ref. Page No			
LO1 **Ensure compliance with cloud security standards**	**1.1**	Demonstrate understanding of frameworks such as ISO 27017, ISO 27018, and CIS benchmarks for cloud security.									
	1.2	Analyse cloud service providers' (CSP) security policies for compliance.									
	1.3	Develop policies that align organizational requirements with cloud security frameworks.									
	1.4	Evaluate compliance reports and assess gaps in cloud security implementation.									
LO2 **Implement cloud security governance structures**	**2.1**	Develop governance models specific to cloud-based environments.									
	2.2	Implement cloud security governance tools to monitor compliance.									
	2.3	Advise stakeholders on legal and regulatory aspects of cloud security governance.									
	2.4	Supervise ongoing audits of cloud governance structures.									
LO3 **Assess and evaluate compliance risks in cloud environments**	**3.1**	Analyse risks associated with non-compliance in cloud deployments.									
	3.2	Evaluate risk management strategies to address compliance-related vulnerabilities.									
	3.3	Compare different risk management frameworks for cloud security.									
	3.4	Develop action plans to mitigate identified compliance risks.									
LO4 **Investigate and support compliance breach resolutions**	**4.1**	Investigate incidents of non-compliance and determine root causes.									
	4.2	Create reports detailing compliance breaches.									
	4.2	Suggest remediation strategies.									
	4.4	Support stakeholders in ensuring corrective actions are taken.									
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		

National Skills Qualification
Level 5 Cloud Security Engineer

Unit 05: Cloud Security Architecture and Design
Unit Reference Number: IS/CS/05/L5
NSQ Level: 5
Credit Value: 6
Guided Learning Hours: 60

Unit Purpose:
This unit equips learners with the knowledge and skills required to design secure cloud architectures that align with business needs. Learners will focus on developing scalable, secure, and resilient cloud 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: Cloud Security Architecture and Design

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type					Ref. Page No			
LO1 Develop secure cloud architectures	**1.1**	Ensure the cloud architecture incorporates security by design principles.									
	1.2	Develop cloud solutions that integrate with security frameworks (e.g., zero-trust models).									
	1.3	Plan secure configurations for multi-cloud and hybrid environments.									
	1.4	Assess the scalability and security of designed cloud architectures.									
LO2 Implement security controls within cloud infrastructures	**2.1**	Analyse the effectiveness of encryption techniques in cloud data storage and transmission.									
	2.2	Create automation for security control implementation across cloud services.									
	2.3	Inspect and compare various cloud security tools for managing configurations.									
LO3 Evaluate cloud security architectural solutions	**3.1**	Compare different cloud security architectures to assess performance and security effectiveness.									
	3.2	Evaluate the impact of architectural decisions on security postures.									
	3.3	Analyse risks associated with cloud security architecture configurations.									
	3.4	Interpret security assessment findings and propose improvements to cloud infrastructures.									
LO4 Supervise cloud architecture implementation and processes	**4.1**	Supervise cloud architecture deployment to ensure alignment with security best practices.									
	4.2	Review implementation progress of security compliance.									
	4.3	Initiate audits of cloud architecture after implementation.									
	4.4	Support continuous improvements based on architecture review.									

Learner's Signature	Date
Assessor's Signature	Date
IQA's Signature	Date
EQA's Signature	Date

National Skills Qualification
Level 5 Cloud Security Engineer

Unit 06: Cloud Threat Management and Monitoring
Unit Reference Number: IS/CS/06/L5
NSQ Level: 5
Credit Value: 6
Guided Learning Hours: 60

Unit Purpose:
This unit equips learners with the knowledge and skills required to operate cloud security monitoring systems and assess threat intelligence to protect cloud assets effectively.

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 06: Cloud Threat Management and Monitoring

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type					Ref. Page No			
LO1 Analyse cloud-specific security threats and risks	**1.1**	Investigate potential attack vectors targeting cloud environments.									
	1.2	Analyse vulnerabilities in cloud platforms and applications.									
	1.3	Evaluate the potential impact of cloud threats on business operations.									
	1.4	Compare historical threat patterns to predict future risks.									
LO2 Implement cloud-based threat detection systems	**2.1**	Develop and implement threat monitoring solutions within cloud services.									
	2.2	Select and integrate cloud-native tools for automated threat detection.									
	2.3	Plan strategies for monitoring cloud assets in real-time.									
	2.4	Operate threat intelligence platforms to detect emerging threats.									
LO3 Assess and evaluate cloud threat intelligence	**3.1**	Interpret threat intelligence reports to assess the organization's threat landscape.									
	3.2	Compare various cloud security intelligence feeds for accuracy and effectiveness.									
	3.3	Evaluate the effectiveness of threat detection systems within cloud environments.									
	3.4	Develop recommendations based on threat intelligence analysis.									
LO4 Support continuous threat management in cloud environments	**4.1**	Implement measures to improve cloud threat management processes.									
	4.2	Recommend to stakeholders on emerging threats and provide mitigation strategies.									
	4.3	Supervise the deployment of updated threat management protocols.									
	4.4	Support the continuous improvement of threat monitoring systems.									

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		

National Skills Qualification
Level 5 Cloud Security Engineer

Unit 07: Cloud Security Incident Response and Recovery
Unit Reference Number: IS/CS/07/L5
NSQ Level: 5
Credit Value: 6
Guided Learning Hours: 60

Unit Purpose:
This unit prepares learners to respond effectively to security incidents in cloud environments, handle forensic investigations, and manage recovery processes to minimize operational disruptions.

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: Cloud Security Incident Response and Recovery

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type					Ref. Page No			
LO1 **Plan cloud security incident response strategies**	**1.1**	Ensure that cloud incident response strategies align with organizational objectives.									
	1.2	Develop cloud-specific incident response protocols.									
	1.3	Create communication plans for incident reporting and escalation.									
	1.4	Initiate cloud incident response simulations to test readiness.									
LO2 **Respond to cloud security incidents**	**2.1**	Investigate the root cause of cloud security breaches.									
	2.2	Interpret forensic data to understand incident dynamics.									
	2.3	Support the isolation and containment of compromised cloud systems.									
	2.4	Develop detailed post-incident reports with recommended actions.									
LO3 **Implement recovery plans following cloud security breaches**	**3.1**	Plan the recovery and restoration of cloud services after security incidents.									
	3.2	**Explain** data integrity and continuity during cloud recovery processes.									
	3.3	Develop post-recovery plans to strengthen cloud security.									
	3.4	Evaluate the effectiveness of incident recovery efforts.									
LO4 **Supervise post-incident analysis and process improvements**	**4.1**	Supervise root cause analysis (RCA) processes for cloud security incidents.									
	4.2	Compare incident response outcomes to identify areas for improvement.									
	4.3	Support the revision of incident response plans based on lessons learned.									
	4.4	Implement continuous improvements for cloud incident response processes.									

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		

National Skills Qualification

Level 5 Cloud Security Engineer

Unit 08: Cloud Identity and Access Management (IAM)
Unit Reference Number: IS/CS/08/L5
NSQ Level: 5
Credit Value: 6
Guided Learning Hours: 60

Unit Purpose:
This unit equips learners with the knowledge to implement and manage secure identity and access management (IAM) systems in cloud environments, ensuring proper user access controls are in place.

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: Cloud Identity and Access Management (IAM)

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type					Ref. Page No			
LO1 Develop cloud-based IAM policies and frameworks	**1.1**	Create IAM policies aligned with cloud security requirements.									
	1.2	Ensure IAM solutions support principles of least privilege and role-based access control (RBAC).									
	1.3	Plan for integration of multi-factor authentication (MFA) in cloud services.									
	1.4	Evaluate the effectiveness of IAM policies.									
LO2 Implement IAM controls across cloud environments	**2.1**	Implement identity federation strategies across cloud services.									
	2.2	Configure IAM solutions for multiple cloud platforms.									
	2.3	Operate IAM tools for continuous access management and monitoring.									
	2.4	Support user lifecycle management, including access revocation.									
LO3 Assess and evaluate cloud IAM solutions	**3.1**	Evaluate IAM solutions for scalability, security, and compliance.									
	3.2	Compare different IAM vendors and their cloud offerings.									
	3.3	Assess the effectiveness of IAM in controlling access to sensitive cloud assets.									
	3.4	Create reports recommending IAM improvements.									
LO4 Supervise cloud IAM implementation and management	**4.1**	Supervise IAM policy enforcement across cloud platforms.									
	4.2	Observe and monitor access management practices to ensure security.									
	4.3	Plan and implement IAM audits to maintain access control compliance.									
	4.4	Initiate remediation processes for IAM-related security gaps.									

Learner's Signature	Date
Assessor's Signature	Date
IQA's Signature	Date
EQA's Signature	Date

National Skills Qualification

Level 5 Cloud Security Engineer

Unit 09: Cloud Data Security and Privacy
Unit Reference Number: IS/CS/09/L5
NSQ Level: 5
Credit Value: 6
Guided Learning Hours: 60

Unit Purpose:

This unit provides learners with the skills to protect data in cloud environments by applying encryption, privacy-enhancing technologies, and ensuring compliance with data privacy laws.

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 09: Cloud Data Security and Privacy

Learning Objective (LO)		Performance Criteria (PC)	Evidence Type					Ref. Page No			
LO1 **Ensure data protection compliance in cloud environments**	**1.1**	Explain to ensure cloud data protection practices comply with laws such as NDPR, GDPR and CCPA.									
	1.2	Develop cloud data governance frameworks to align with regulatory requirements.									
	1.3	Implement data residency and protection policies in multi-cloud environments.									
	1.4	Plan for regular audits of cloud data security practices.									
LO2 **Implement encryption and data protection solutions in the cloud**	**2.1**	Select and implement encryption technologies for cloud data storage and transfer.									
	2.2	Develop key management systems for cloud encryption solutions.									
	2.3	Utilize encryption and privacy tools to ensure data confidentiality in the cloud.									
	2.4	Support continuous encryption management across cloud platforms.									
LO3 **Assess and evaluate cloud data privacy controls**	**3.1**	Evaluate privacy-enhancing technologies (PET) used in cloud deployments.									
	3.2	Assess risks related to data privacy breaches in the cloud.									
	3.3	Compare data protection controls across different cloud service providers.									
	3.4	Inspect cloud privacy policies for compliance.									
LO4 **Supervise data security processes and privacy compliance**	**4.1**	Supervise the implementation of data privacy measures in cloud environments.									
	4.2	Plan for regular assessments of cloud data privacy compliance.									
	4.3	Support post-breach data recovery and privacy re-establishment.									
	4.4	Initiate processes for addressing data privacy violations in the cloud.									
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 08055900895
2	Frank Iheonu	Inits Limited 283 Herbert Macaulay Way, Yaba	iheonufrank@gmail.com 07036999294
3	Chibueze Princewill Okereke	Zenith Bank Group (Zenpay) 5 Roluga Street, Soluyi, Gbagada, Lagos	okerekeprincewill@hotmail.com 07025768487
4	Emmanuel C. Amadi	Federal University of Technology, Owerri	emmanuel.amadi@futo.edu.ng 08062142392
5	Engr. Lawal Abdullahi	Zenith Kad Ict Hub Kaduna	ocplawal@gmail.com 08035169089
6	Muhammad Musa	NBTE	muhammadwaziri@msn.com 08033671027
7	MUHAMMAD, BILYAMINU MUSA	NBTE	mahogany@gmail.com 09036071291
8	Muhammad Bello Aliyu	CPN	mbacaspet@gmail.com 08039176984
9	BENJAMIN, Prince Chukwudindu	CPN	pco.benjamin@gmail.com 08132850544
10	Amoo, Taofeek	CPN	taofeekamoo@gmail.com 08053370334
11	Olatunji Abibat	CPN	adehabb@gmail.com 08054263602
12	Linda Ngbeken	CPN	excel4all2000@yahoo.com 08128219274

VALIDATION TEA 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 09036071291
Muhammad Bello Aliyu		CPN	mbacaspet@gmail.com 08039176984
BENJAMIN, Prince Chukwudindu		CPN	pco.benjamin@gmail.com 08132850544