CENTRAL BANK OF NIGERIA
Financial Policy and Regulation Department
Central Business District
P.M.B. 0187
Garki, Abuja.

Tel: 09-46237401
E-mail:fprd@cbn.gov.ng

Ref: FPR/DIR/PUB/CIR/001/042 **April 25, 2022**

Circular to all Other Financial Institutions

GUIDANCE NOTE ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) REGULATIONS FOR OTHER FINANCIAL INSTITUTIONS

The Central Bank of Nigeria in carrying out its supervisory activities observed that Other Financial Institutions (OFIs) have uneven challenges in the implementation of effective risk-based approach to AML/CFT programme that meets the standard of regulatory requirements.

As part of efforts to address the challenges, the CBN has developed a **GUIDANCE NOTE ON AML/CFT REGULATIONS FOR OTHER FINANCIAL INSTITUTIONS** to assist the sub-sector in the identification, assessment as well as mitigation of ML/TF risks in their operations.

Consequently, the Guidance Note is hereby released for immediate compliance by all OFIs.

CHIBUZO A. EFOBI
DIRECTOR, FINANCIAL POLICY AND REGULATION DEPARTMENT

GUIDANCE NOTE ON ANTI-MONEY LAUNDERING AND COMBATING FINANCING OF TERRORISM REGULATIONS FOR OTHER FINANCIAL INSTITUTIONS

CENTRAL BANK OF NIGERIA

APRIL, 22 (VERSION 1.0)

TABLE OF CONTENTS

Preface

The CBN in exercise of its powers and responsibilities under the CBN AML/CFT Regulations, 2013 (as amended) and in compliance with the Financial Action Task Force (FATF) Recommendation 1, hereby issues this document titled "Guidance Note on AML/CFT Regulations and Assessment of ML/TF Risks for Other Financial Institutions in Nigeria in line with the relevant provisions of Money Laundering Prohibition Act (MLPA) 2011 (as amended), and Terrorism Prevention Act (TPA) 2011 (as amended), and Section 66(2) of BOFIA, 2020.

This Guidance Note will provide the basic ideas of complying with the AML/CFT Regulations, identifying, assessing and mitigating ML/TF risks that Other Financial Institutions (OFIs) may encounter in conducting their businesses. These risks may arise from customers, product and services, business practices or delivery methods and jurisdictions or geographical presence.

This Note shall be a minimum guide for OFIs on AML/CFT programme in identifying and assessing ML/TF risks in their operations. The application of the Guidance Note is expected to assist the institutions take appropriate measures to review, monitor and mitigate the identified risk. OFIs could use more stringent tools to identify and assess ML/TF risks in their institutions. However, irrespective of the method adopted, the risk assessment should be updated regularly.

List of Abbreviations

AML/CFT	Anti-Money Laundering & Combating the Financing of Terrorism
CDD	Customer Due Diligence
CCO	Chief Compliance Officer
CRT	Currency Transaction Report
EDD	Enhanced Due Diligence
EFTs	Electronic Funds Transfers
FATF	Financial Actions Task Force
HOC	Head of Compliance
KYC	Know Your Customer
ML/TF	Money Laundering and Terrorism Financing
MIS	Management Information System
MLPA	Money Laundering Prohibition Act
NFIU	Nigeria Financial Intelligence Unit
OFIs	Other Financial Institutions
PEPs	Politically Exposed Persons
STR	Suspicious Transaction Report
TF	Terrorist Financing

INTRODUCTION

The determination of criminals and criminal organizations to use other financial institutions (OFIs) to launder funds and finance terrorist activities poses threats to the financial system globally. This threat continues to be a source of concern to the Central Bank of Nigeria (CBN).

Over the years, there have been extensive efforts in many countries to come up with appropriate measures to combat money laundering and financing of terrorism.

One of the core mandates of the CBN is to promote the safety and soundness of the financial system and, by extension, formulating appropriate policies and procedures designed to mitigate AML/CFT risks to promote financial system stability.

In furtherance of the above mandate, the CBN has developed this Guidance Note on AML/CFT Regulations and Assessment of ML/TF Risks to assist the OFIs in identifying risks associated with money laundering and terrorist financing that will help them in designing effective AML/CFT compliance programme.

The Guidance Note (herein referred to as The Guidance) has been aligned with the preventative measures set out in the CBN AML/CFT Regulations 2013 (as amended - hereafter referred to as AML/CFT Regulations). The Guidance Note identified relevant risk management procedures that would lessen the susceptibility of OFIs as a fertile ground for money laundering, terrorist financing and proliferation financing.

1.1 Compliance with this Guidance Note

OFIs understand their business better and thus, are best placed to identify and determine the inherent risks their business faces from money laundering (ML) and terrorism financing (TF). They are therefore, expected to develop appropriate strategies to manage, mitigate and control these risks.

This Guidance Note does not constitute secondary regulation or new regulatory requirement. It is intended to assist OFIs to comply with measures contained in the CBN AML/CFT Regulations, 2013 (as amended) and other relevant AML/CFT laws. It aims to further guide OFIs to meet the CBN's governance and control expectations. It should be noted that the Guidance Note does not override any legal or regulatory requirements. In the event of any discrepancy between the Guidance Note and relevant AML/CFT laws and regulations, the provisions of the latter will apply. The Guidance Note is not exhaustive and do not set limitations on steps to be taken by OFIs to meet their statutory obligations.

Similarly, where the Guidance Note has provided little or no information on a specific Regulation of the CBN AML/CFT Regulations, it is assumed that the relevant Regulations already provides clear and detailed information on the obligations of OFIs. The OFIs are therefore reminded that the Guidance Note is not a checklist of the activities they must do or should not do in order to mitigate their ML/TF risk.

However, it is important to note that effective control over ML/TF risks and related regulatory, operational and reputation risks is essential for the operations of OFIs. OFIs, are therefore, expected to adopt the AML/CFT approaches that take into account the nature, scope, complexity and risk profile of their institutions.

1.2 Scope

The Guidance, to the extent possible, covers the requirements prescribed in the MLPA 2011 (as amended), TPA 2011 (as amended) and CBN AML/CFT Regulations.

OFIs should bear in mind that other competent authority such as the NFIU also issue directives/Guidance Note that would improve their AML/CFT compliance programme.

It should be noted that the Guidance Note does not provide an express or implied assurance that the CBN would not exercise its regulatory powers where a suspected breach of relevant AML/CFT Laws and Regulations is brought to its attention.

It should be further noted that this Guidance Note is subject to periodic review by the Central Bank of Nigeria.

1.3 AML/CFT Extant Laws and Regulations in Nigeria

The relevant extant laws and regulations governing AML/CFT in Nigeria include but not limited the following:

- Money Laundering (Prohibition) Act 2011 (as amended);
- Terrorism Financing (Prevention) Act 2011 (as amended);
- Nigeria Financial Intelligence Unit Act, 2018;
- Economic and Financial Crime Commission Act 2004;
- Independent Corrupt Practices and Other Related Offences Commission (ICPC) Act, 2000
- National Drug Law Enforcement Agency (NDLEA) Act 1989;
- Advance Fee Fraud and Other Related Offences Act (AFF) 2006;
- CBN AML/CFT Regulations, 2013 (as amended);
- Terrorism Prevention (Freezing of International Terrorists Funds and Other Related Measures) Regulation 2011; and
- CBN AML/CFT (Administrative Sanctions) Regulations, 2018.

1. AML/CFT COMPLIANCE PROGRAMME

2.1 Scope of the AML/CFT Compliance Programme

OFIs should develop and administer AML/CFT programme that is commensurate with their size, complexity of operations and the requirements of extant AML/CFT Laws and Regulations in Nigeria.

2.2 Principal Elements

OFIs are required to develop an AML/CFT programme, which at the minimum should contain the following:

1. Board and Senior management oversight;
2. Risk Management;
3. Policies and Procedures;
4. Monitoring and Suspicious Transaction Report;
5. Internal Control;
6. Compliance Function; and
7. Training.

2.3 Corporate Governance (Board of Directors and Senior Management)

2.3.1 Board of Directors

The ultimate responsibility for AML/CFT compliance is placed on the OFI's Board of Directors and Senior Management.

Board of Directors shall:

a) establishes an AML/CFT programme that is consistent with the AML/CFT legislations and regulations
b) approves written AML/CFT policies and procedures
c) designates any of its members to be responsible for AML/CFT issues or establish an AML/CFT Committee.
d) receives reports on AML/CFT programme periodically
e) provides timely feedback/decisions on reports it receives

f) issues specific risk management policies and procedures with respect to ML/TF risks.
g) formulates and communicates a code of conduct/ethics that include AML/CFT issues

2.3.2 Senior management oversight

Senior Management is responsible and accountable for day-to-day implementation of the AML/CFT programme. They should ensure that the programme is adequate to mitigate ML/TF risks and complies with the extant AML/CFT laws, regulations, guidelines and relevant circulars.

Senior Management shall:

a. on a regular basis, identify where the business is vulnerable to money laundering and terrorist financing;
b. based on the risk assessment, develop internal policies, procedures, and controls to combat money laundering and the financing of terrorism;
c. ensure staff effectively implement the internal policies, procedures, and controls and receive appropriate training;
d. ensure that regulatory returns are rendered to relevant regulatory agencies; and
e. monitor the implementation of policies, procedures, and controls and make improvements where required on the basis of changes to the OFI's money laundering and terrorist financing risk assessment or as recommended by the supervisory agency and/or the Financial Intelligence Unit.

2.4 Policies and Procedures

OFI shall:

1. have a written and Board approved policies and procedures for CDD/KYC principles appropriate to its size and type of business.

2. disseminate policies and procedures to all its employees and management.
3. implement CDD measures for customer identification and verification with respect to:
    a. Individuals
    b. Legal entities: companies, etc.
    c. PEPs
    d. Beneficiaries
    e. High risk customers
    f. Any other customer
4. have an account opening procedure that specify the means of identification to be obtained from each customer as part of its CDD.
5. implement the AML/CFT policies and procedures in all branches/subsidiaries.
6. have a system for testing compliance of the CDD policies and procedures with the extant AML/CFT laws and regulations.
7. have CDD policies and procedures that provide for:
    a. Customer Acceptance and Rejection.
    b. Simplified due diligence for low-risk customers.
    c. Enhanced CDD for higher risk clients, products, transactions, etc.
    d. Monitoring of customer accounts and transactions (including enhanced monitoring for higher risk clients).
    e. Reporting of suspicious transactions.
    f. Record keeping policy.
8. have AML/CFT CDD policies and procedures that requires:
    a. identification and verification of identity of ultimate beneficiaries.
    b. identification of all third parties that pay or provide funds for investments for or on behalf of the client.

c. recording of information on the purpose and intended nature of the business relationship/transaction.
d. specific CDD procedures for PEPs (domestic and foreign) and other high-risk customers and transactions, etc.
e. a designated top management staff to be responsible for approving and handling PEPs and high-risk client accounts and transactions.
f. updating customer profile records.
g. maintaining CDD and transaction records.

9. require the following information on the beneficial owner in the event that a prospective customer is an intermediary or authorized representative for another party, including but not limited to:
    a. similar information as per the procedure for acceptance of individual customers.
    b. legal relationship and authority, such as evidence of assignment, power of attorney, resolution and similar mandates.
    c. information on the source of funds/wealth of the ultimate beneficial owner.
    d. identity of management and principal owners/controllers of a company being represented.
10. have identification and verification procedures for all new customers that include the following:
    a) examination of documents for authenticity.
    b) face-to-face meeting with prospective customers.
    c) crosscheck information provided by customers with information from independent sources.
    d) conduct stricter verification for customers classified as high risk, linked to high risk business, and/or from high risk countries.
    e) in the case of companies, obtain information on line of business, location, financial statements, expected transaction profile, etc.

11. have CDD policy that include checking of clients against high risk customers in official country lists or lists issued by international organizations e.g. UN terrorism lists.
12. have record retention of customer identification, transactions, suspicious activity reports, etc.
13. have policies and procedures for whistleblowing, staff training and tipping-off.

2.5 Risk Management

OFIs shall establish:

a) a Risk Management function/unit that includes ML/TF risks assessment
b) an ML/TF risk classification system.
c) specific types or categories of products, and clients identified as high risk.
d) categories of customers that are prohibited from doing business with the institution based on their ML/TF risks.
e) a screening mechanism for PEPs, UN sanctioned persons/entities list, other official lists, or internally generated lists of high-risk customers.
f) system and procedures for screening of high-risk customers.
g) a process that considers ML/TF risks in approving expansion of business e.g. new branches, and markets (domestic and foreign) and high-risk locations where it conducts businesses, etc.
h) policies and procedures for assessing ML/TF risks in the development of new products/services.
i) a mechanism for communicating to Board and senior management of changing ML/TF risk levels.

2.6 Monitoring and Suspicious Transaction Reporting

OFIs shall have:

a) an internal system for detecting and reporting unusual and suspicious activities
b) specific monitoring systems for terrorism financing
c) a system for monitoring unusual and suspicious activity on a group-wide basis from branches and subsidiaries
d) designation of persons responsible for identifying, researching and reporting suspicious activities
e) reports from the operational units analysed by the AML Compliance officer/unit
f) security measures to prevent information about unusual and suspicious activities from being disclosed to unauthorized parties, intentionally or unintentionally (e.g oath of confidentiality, integrity checks, employee screening).
g) specific monitoring mechanisms for PEPs
h) suspicious activities reported to the NFIU.
i) a policy to protect the employees, if they report suspicious transactions, in good faith.
j) administrative sanctions for employees that do not adhere to the monitoring and reporting policies and procedures of the OFI.

2.7 Internal Control

OFIs shall have:

a) an Internal Audit Department/function
b) internal Audit to review and test the AML/CFT programme, CDD/KYC policies and procedures amongst others
c) a specific AML/CFT audit plan

d) Board of Directors or a designated Board Committee to receive audit reports that include AML/CFT issues
e) internal audit to review the Compliance function
f) internal audit function with respect to AML/CFT that is risk-based
g) internal audit staff with the right professional qualifications, experience and competence
h) an external audit function that reviews AML/CFT issues

2.8 Compliance Function

OFIs shall:

1. establish a compliance function and approve a compliance policy that covers all significant business lines and processes of the institution
2. appoint an AML/CFT compliance officer at the management/senior level;
3. allocate resources to the compliance function;
4. a compliance officer or AML/CFT officer at each office, branch, or subsidiary;
5. ensure there is no conflict of interest between the AML/CFT compliance function and other duties assigned to the AML/CFT Officer; and
6. specify the role of the AML/CFT compliance officer in (a) monitoring and reporting of suspicious activities; (b) training; (c) development of risk systems and controls.

And the Board of Directors shall:

1. designate a person or persons to be responsible for the overall AML/CFT compliance programme;
2. ensure the CCO/HCO has the necessary authority and resources to effectively execute all the duties assigned to him/her;
3. ensure the CCO/HCO and his/her staff have the necessary competencies;

4. ensure the AML/CFT compliance function is sufficiently staffed for the institution's overall risk level based on products, services, customers, geographic locations, size and compliance needs; and
5. ensure that no conflict of interest exists and that the staff are given adequate time to execute their duties.

2.9 Training

The AML/CFT Regulation 33(4)(b) requires financial institutions to develop on-going employee training programme to ensure that employees are kept informed of new developments, including information on current ML/TF techniques, methods and trends.

OFIs should ensure that written AML/CFT training programme are developed and maintained. Appropriate training should be considered for directors, senior management, employees, agents and any other persons who may be responsible for control activity, outcomes or oversight, or who are authorized to act on the OFI's behalf. Nature and content should be appropriate to the AML/CFT responsibilities of all category of staff in the OFI. In particular, training should be tailored to provide information and skills that are necessary for the effective performance of the AML/CFT function in each case.

Training programme should provide sufficient briefing concerning risks and controls.

Having well trained staff who are familiar with the ML/TF risks is critical in the detection and prevention of money laundering and terrorist financing. OFIs should ensure that all employees, directors and agents are aware of the risks of money laundering and terrorist financing relevant to the business, the applicable legislation and their obligations and responsibilities.

OFIs should provide appropriate and adequate trainings, which are tailored to the nature, scale, complexity and proportionate to the level of ML/TF risk faced by the institution.

OFIs should ensure that all employees, directors and agents are:

- trained in the institution's AML/CFT Business Risk Assessment and how it affects their daily work;
- trained on the institution's AML/CFT policy, which should be drafted in clear and unambiguous language;
- trained in the institution's procedures to recognize and address potential instances of money laundering or terrorist financing;
- made aware of the institution's internal reporting procedures and responsibilities of the institution's Head of Compliance (HoC) in respect of STRs, PEPs, CDD, etc.
- trained on individual and institution's obligations under the CBN AML/CFT Regulations and AML/CFT Risk-Based Frameworks as well as those of the OFIs.

Regulation 37 of the AML/CFT Regulations also requires financial institutions to ensure that employees are trained on the laws relating to money laundering and terrorist financing, CDD etc. This Regulation further requires conduct of ongoing training on identifying a transaction or other activity that may be related to money laundering or terrorist financing, and on how to proceed once such a transaction or activity is identified.

In summary, OFIs shall have:

1. an AML/CFT training programme approved by the Board of Directors in place for employees.
2. annual budget for AML/CFT training.
3. the Board and senior management participate in AML/CFT training.

4. the compliance officer attend professional training regarding ML/TF methods and typologies, CDD, suspicious activity monitoring and reporting, record keeping, etc.
5. a mechanism of ensuring that every employee requested to attend training actually attends the training.
6. different types of AML/CFT training programmes e.g. for new and existing employees and by type of business activities, etc.
7. a mechanism for communicating new AML/CFT related laws or changes to existing AML/CFT related policies or practices to its employees.
8. records of its training sessions including attendance records and relevant training materials used and retain them in line with regulatory requirements.
9. sanctions for employee that fail to attend assigned training programmes.

2. CUSTOMER DUE DILIGENCE

CDD involves customer identification, information gathering, and monitoring. These components must comply with applicable regulatory requirements and should be enhanced for higher risk customers/transactions.

As a general principle, a business relationship should only be entered into or maintained, with a customer if the OFI is satisfied that the information gathered demonstrates sufficient knowledge about the customer (i.e. the customer has disclosed his or her true identity and a legitimate purpose for entering or maintaining the business relationship with the OFI).

OFIs should assess the appropriateness and comprehensiveness of its CDD policies, procedures and processes for obtaining customer information, which should assist in detecting, monitoring and reporting suspicious transactions.

Furthermore, OFIs shall:

a. ensure its CDD policies, procedures, and processes are commensurate with the institution's risk profile and allow for changes to a customer's risk profiling;

b. assign person(s) to be responsible for reviewing or approving such changes in customer risk profiling;

c. ensure there are processes in place for obtaining information at account opening (onboarding), in addition to ensuring current customer information is maintained;

d. have enhanced due diligence (EDD) procedures and processes to identify customers that may pose higher risk of money laundering or terrorist financing; and

e. provide Guidance Note for documenting analysis associated with the due diligence process, including Guidance Note procedures in respect

of Customer Due Diligence for resolving issues when insufficient information or inaccurate information is obtained.

The prescribed rules comprising CDD requirements do not permit OFIs to establish anonymous accounts for customers. If OFIs provide services (such as account numbering or coding services) that effectively shield the identity of a customer for business reasons (for instance, in a corporate acquisition where the premature circulation of information could jeopardize the transaction), or where customer's identity is withheld for proprietary reasons, OFIs must ensure that they have appropriately ascertained the identity of the customer and that this information is accessible by the HOC.

Where the regulatory requirements prescribe a determination of the status of a customer, for example, whether a customer is a PEP, OFIs should ensure that the determination is made based on an assessment of the information received.

3.1 Nature and Amount

At a minimum, CDD measures must comply with the requirements of the CBN AML/CFT Regulation 2013 (as amended). CDD standards should provide that, where there are doubts about the veracity or adequacy of previously obtained customer identification and verification data, enhanced CDD must be performed.

3.2 Customer Identification and Ascertaining Identity

OFIs may have customers already on boarded whose identities have not been ascertained in accordance with the AML/CFT Regulations. These customers should be subjected to appropriate customer identification measures.

Regulation 14 and Schedule II of the AML/CFT Regulations specifies the originals of prescribed valid documents that may be inspected to ascertain the identity of individuals and the existence of corporate entities. A CDD policy should

provide clear direction that complies with the CBN AML/CFT Regulation, (where applicable) on:

- when a customer's identity must be ascertained (timing);
- how to ascertain the identity of the customer, when the customer is present or not present; and
- which original and valid identification documents should be used to ascertain identification and what information is to be recorded from them.

While identification and verification standards and policies must meet the minimum prescribed requirements, OFIs may consider that the assessment of inherent risk justifies the application of additional identification requirements to some categories of customers. The CBN permits the acceptance of identity cards issued by the National Identity Management Commission, Independent National Electoral Commission, the Federal Road Safety Commission, Nigerian Immigration Service and National Commission for Refugees, Migrant and IDPs.

If these are not available, other credible evidence should be used in supporting the identity of the customer as specified by Know Your Customers (KYC) principles as may be issued by the CBN from time to time.

Identifying a corporate customer or other entity may involve collection of substantial information in some cases. In addition to confirming the existence of the entity, OFIs must take reasonable measures to obtain names, addresses and occupations of its directors, and individuals who are the ultimate beneficial owners of the entity. Reasonable measures to obtain this information could include:

- requesting directly from the entity;
- consulting credible public database; or
- a combination of both.

Where an OFI is required to obtain details of occupation of a person (for example, a director of a corporate entity), the OFI should ensure that the occupation

obtained is the person's principal occupation and not merely the person's title in the entity.

OFIs must also ascertain the identity of every person who signs a signature card in respect of corporate accounts.

In addition, OFIs must take reasonable measures prescribed in the AML/CFT Regulations, to determine whether an individual customer is acting for or on behalf of a third party.

3.3 Sources of Accumulated Funds or Wealth

OFIs should satisfy themselves that, in appropriate circumstances, customers' accumulated funds or wealth appears to be reasonable and consistent with the information provided. Doubts about the origin of such funds or wealth should be satisfied before proceeding with the relationship or permitting transactions to occur.

Reasonable measures to implement this requirement could include:

- obtaining and evaluating more detailed information from the customer; and
- verifying information obtained from other financial institutions or references.

In cases where a customer is assessed as high risk and the source of accumulated funds or wealth does not appear to be reasonable or is inconsistent with the information provided after taking reasonable measures to resolve the inconsistency, the OFI should consider declining to enter the business relationship, or terminating it, and file a suspicious transaction report.

3.4 Monitoring

3.4.1 Standard

OFIs must be able to identify suspicious transactions and report these to the NFIU. An OFI must take reasonable measures to ascertain the identity of every person

with whom the institution conducts a transaction that is identified to be suspicious. These obligations imply that the activities of all customers, regardless of their risk ranking, must be subject to some form of ongoing monitoring to detect potentially suspicious transactions.

Reasonable measures for such monitoring could include:

- Identification and review of types of transactions or attempted transactions (defined by size, frequency, geographical location, delivery channel, business relationship or other factors) that appear to be inconsistent with the intended purpose of the account or the circumstances; and
- Changes in transaction activity that may on their own or in conjunction with recorded changes in customer information, be indicative of a change in the nature of a customer's business or intended use of the account.

Monitoring should identify information, transactions that are unusual or potentially suspicious and require further analysis. Monitoring criteria should cover all relevant indicators.

Relevant indicators could include:

- frequent and unexplained movement of accounts to different financial institutions;
- frequent and unexplained movement of funds between different financial institutions in various geographic locations;
- customer information on the source of transaction funds or accumulated wealth that is not reasonable or credible;
- structured/complex or unusually large transactions relative to the size and business of the customer or the geographical location of the transaction;
- transactions or patterns of transactions that is inconsistent with the purpose of the account or the business of the customer; and
- transactions that have no apparent economic or visible lawful purpose.

3.4.2 Enhanced

Where an OFI determines ML/TF risks to be high, it must take prescribed special measures for identifying customers, keeping records and monitoring financial transactions in respect of the activities that pose the high risk. The prescribed special measures should include: reasonable measures to determine whether the high risk customer is a PEP; maintain customer identification information; file a suspicious transaction report and generally mitigate the high risk.

OFIs should consider creating more than one category of higher risk customers, and more than one category of enhanced due diligence, if the nature, scope, complexity and risk profile of the financial institution merits such action. Each level of enhanced monitoring should reflect the assessed level of risk appropriately.

Reasonable measures for applying enhanced monitoring could include:

- Frequent reviews of customer activity;
- Frequent updates or reviews of customer information;
- The application of additional customer identification measures;
- The gathering of information from public or open sources such as commercial databases;
- Frequent flagging of unusual transactions or other information;
- Referral of customer activity and transactions to a more senior officer in the OFI for review.

Additional measures that could be taken to strengthen the monitoring of high risk activities include:

- Review of business reports, including exceptions reports, generated by management information systems (for example, anti-fraud systems), for possible indicators of unusual or suspicious activity; and

- Analysis of STR information for trends and other indicators of suspicious activity to aid the development of appropriate risk-base controls in businesses that indicate such activity.

3. HIGHER RISK CUSTOMERS

OFIs should develop appropriate measures in respect of enhanced due diligence and related controls applicable to areas of identified higher risk. Regulation 16 of the AML/CFT Regulations, specified the customers/circumstances where enhanced due diligence should be applied to include non-resident customers, private banking, trust and other companies that are asset holding entities, PEPs, cross border banking and business relationships, companies with nominee shareholding, etc.

4.1 Intermediaries and Third Parties

OFIs may rely on intermediaries or other third parties for customer information gathering and verification purposes (Regulation 28 of AML/CFT Regulations), which could include the use of solicitors, brokers etc.

ML/TF risk mitigation can be compromised where OFIs do not ensure that appropriate customer identification standards are applied by the intermediaries or other third parties. Consequently, accountability for identifying and obtaining information of the customer remains with the OFIs when third parties are engaged (Regulation 28(5) of the AML/CFT Regulations). In respect of this accountability, OFIs must have an agreement or arrangement in writing with the agent if such person is to be responsible for customer identification and verification.

The provisions of this arrangement or agreement must conform with the requirements of Regulation 28(2) of the AML/CFT Regulations and it should also obligate the agent to:

- apply customer identification procedures that include viewing original identification documents;

- ensure that, where the customer is not present at the time customer identification is ascertained, the agent applies prescribed non-person-to-person identification requirements;
- provide the customer identification information to the OFI promptly after obtaining it;
- ensure that if the agent is responsible for collecting the information required to make a third party determination or a PEP determination, these responsibilities are also documented;
- ensure they receive customer identification information within the required timeframes; and
- periodically review the quality of customer information gathered and documented to ensure that it meets OFI's requirements.

Documentation of relationships and communications with agents and intermediaries as well as customer due diligence work done should be complete.

OFIs should consider terminating relationships with agents or intermediaries that do not comply with agreed customer identification responsibilities or provide the requisite customer information on a timely basis. Contracts with agents should be reviewed and updated (as necessary) to ensure compliance with the extant AML/CFT laws and regulations regarding the use of agents and intermediaries.

Bureaux-de-Change (BDCs) that are directly involved in the purchases and sales of foreign currencies should note that the BDCs may be easily used for laundering the proceeds of frauds/crimes and financing of terrorism. They should, therefore, adopt enhanced due diligence to maintain adequate records of customers for easy reference.

4.2 Politically Exposed Persons (PEPs)

The FATF Recommendations state that PEPs are potentially more susceptible to financial crime than other customers of financial institutions. In Nigeria, the

AML/CFT Regulations, requires OFIs to determine whether they are dealing with PEPs and prescribes mandatory enhanced due diligence measures and on-going monitoring of relationship with PEPs.

PEPs are defined in Regulation 18 of the AML/CFT Regulations as individuals who are or have been entrusted with prominent public function in Nigeria or foreign countries and people or entities associated with them. Also, PEPs are extended to include persons who are or had been entrusted with a prominent function by an international organization, including members of senior management, directors, deputy directors, assistant directors and members of a board or equivalent function other than middle-ranking or more junior individuals.

Once the determination is made, prescribed actions must be taken by OFIs. OFIs should take "reasonable measures" to determine the status of PEPs when;

- an account is opened (onboarding);
- an existing customer becomes a PEP.

The Reasonable measures could include:

- asking the individual for information that could indicate PEP status;
- screening the individual's name and other personal information against a commercially or publicly available database to gather more information about the individual; or
- establish the source of wealth
- a combination of all.

4.2.1 Asking the Customer:

If OFIs choose to ask the individual for information, the institutions should keep in mind that customers are not expected to know the criteria that determine whether they are PEPs. OFIs should also note that there is no obligation imposed

on them to disclose to a customer that a determination must be made, or needs to be made.

A reasonable approach would be to ask customers if they have ever had a prescribed connection to a federal, state, local government, military or judiciary. The questions could be expanded to cover family members with any similar connections. If the responses are not clear or inconclusive, additional assessment or due diligence may be necessary before finalizing the determination. The additional measures could range from asking the applicant for more information, or do internet searches, to running the individual(s) name(s) against a public database.

OFIs may assign responsibility for collecting the information necessary to determine if the customer is a PEP, but the OFI, not the agent, is responsible for making the determination and applying the prescribed measures accordingly. OFIs should ensure that where agents or intermediaries are responsible for gathering the information, the agents understand what is required to be done and the OFI satisfies itself that its agents are doing what is required.

4.2.2 What Happens after a PEP Determination is made

Once a customer is identified as a PEP, this may not be changed, except for correction of errors in the information provided.

After it is established that a customer is a PEP, an OFI must:

- take reasonable measures to establish the source of acquired funds;
- obtain the approval of senior management (who has the authority to make this decision) to keep the account operational; and
- conduct enhanced ongoing monitoring of the PEP's account to identify potentially suspicious transactions.

Reasonable measures should be put in place for enhanced and ongoing monitoring of PEPs' accounts and may involve manual or automated processes, or a combination of both depending on resources and needs. This could include:

- ensuring that the system for monitoring and reporting PEPs for suspicious activities are adequate given the OFIs size, complexity, location and types of customer relationships;
- developing reports or performing a frequent review of PEP account activity, and flagging activities that deviate from expectations and elevate concerns as necessary;
- setting up a management committee to regularly review all identified PEPs and their transactions; and
- frequent review of transactions against red flags.

OFIs should ensure that their methodology for PEP determination does not preclude individuals merely because they are not Nigerian citizens or residents.

4.4 Mortgage Loans and other Products

OFIs should ensure their customer acceptance and due diligence processes address the risk of use of proceeds crimes for acquiring property. OFIs should take reasonable measures to address the risk, which could include:

- applying enhanced customer identification measures such as viewing a second piece of identification, or viewing government-issued photo identification;
- having an agent or intermediary apply enhanced non-face-to-face customer identification measures;
- ensuring that legal and/or beneficial ownership of property or business is identified and documented;

- satisfying themselves that the amount of customers' accumulated funds or wealth appears to be reasonable and consistent with the information provided;
- training of staff or agents to recognize valid identification and signs of falsified documents;
- obtaining corroboration of information in employer letters, references, pay stubs or credit records, as appropriate; and
- corroborating the existence and value of stated assets.

Primary Mortgage Banks and other relevant OFIs should ensure that mortgage loans are subject to the AML/CFT programme.

4. TRANSACTION REPORTING

OFIs should ensure that internal reporting processes are designed to ensure compliance with regulatory reporting requirements as they relate to transaction reporting systems. Systemic compliance issues should be documented, escalated to the HOC and brought to the Board and Senior Management or the regulatory authorities as the case may be. Control measures should include the identification of remedial action designed to eliminate compliance issues.

5.1 Currency Transaction Reporting

OFIs are required to render Currency Transaction Report (CTR) to NFIU for each transaction in cash (deposit, withdrawal, exchange or other payment or transfer) of N5,000,000 and above or N10,000,000 and above for individuals or corporate bodies respectively. All types of currency transactions are to be reported, there are no exempt persons.

A completed CTR is required to be rendered (manually or electronically) to the NFIU within 7 days after the date of the transaction. If an OFI fails to file CTRs on reportable transactions as a result of unforeseen circumstances. The OFI must retain copies of CTRs for five years from the date of the report.

5.2 Suspicious Transactions Reporting (STRs)

Suspicious transactions are defined as those transactions in respect of which there are reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of an ML or FT offence. It should be noted that there is no monetary threshold applicable to suspicious transactions.

Transactions that the OFIs reasonably suspect are related to money laundering offences must be reported to the NFIU. Property in the possession or control of OFIs

that is known or believed to be owned or controlled by or on behalf of a terrorist or terrorist groups, must also be reported to NFIU. This includes information about any transaction or proposed transaction relating to that property.

Suspicious transactions should be identified by OFIs from unusual activity or transactions. Procedures to identify unusual activities should capture the background and purpose of the transaction(s), who was involved, when and where it occurred, what products or services were involved and how the transaction was structured and should be recorded.

STRs must be filed promptly in compliance with the regulatory requirements. Supporting documentation must be retained as prescribed and made available to assist law enforcement authorities within prescribed deadlines.

OFIs must ensure that information concerning STRs, including the fact that there is a suspicion and/or an STR, is kept strictly confidential. The customer(s) involved must not be tipped off and information within the OFI must be strictly limited to the HOC and others on a "need to know" basis.

The obligation on financial institutions to report suspicious transactions applies to whether the transactions are completed or not (Regulation 31 (4)), thus an attempted suspicious transaction is also subject to reporting to the NFIU.

Regulation 31 of the AML/CFT Regulations provides what constitute a suspicious transaction, the obligation to and timing of reporting to the NFIU. Regulation 31 (3) specified that a financial institution shall report to the NFIU not later than 24 hours, any suspicious transaction, stating clearly the reasons for the suspicion and the actions taken, the identity of the principal and any other relevant information.

Except where the identity has been previously ascertained in accordance with the Regulations, OFIs should take reasonable measures to ascertain the identity of every person with whom a suspicious transaction or suspicious attempted transaction is conducted. While reasonable measures may include normal

customer identification practices, care must be taken to ensure that such practices, if used, do not tip off the customer.

In summary the OFIs policies, procedures and processes for identifying, investigating and reporting suspicious transaction should include the following:

i. Lines of communication for the referral of unusual activity to appropriate personnel;
ii. Designation of individual(s) responsible for identifying, researching and reporting suspicious activities;
iii. Monitoring systems used to identify unusual activity; and
iv. Procedures for reviewing and evaluating transaction activity reported to law enforcement agencies. OFIs should also evaluate the policies, procedures and processes for:

    (a) responding to LEA's requests;

    (b) evaluating the account of the target for suspicious transactions;

    (c) filing of STRs, if necessary; and

    (d) handling account closures.

5.2.1 STR Decision Making

The financial institution's policies, procedures and processes should include procedures for:

(i) documenting decisions not to file a STR;

(ii) issues identified as the result of STR filings on accounts; and

(iii) closing accounts as a result of continuous suspicious transaction.

5.2.2 STR Completion and Filing

The financial institution's policies, procedures and processes provide for:

(i) completing, filing and retaining STRs and their supporting documentation;

(ii) reporting STRs to the board of directors, or a committee thereof and informing senior management; and

(iii) sharing STRs with head offices and controlling companies, as necessary.

5. OVERVIEW OF ML/TF RISKS

6.1 Introduction

The success of the AML/CFT programme depends on effective assessment of related threat and vulnerability and having necessary controls for combating ML/TF risks.

The purpose of this section is to:

a. provide general information about ML/TF risks related to products, services, delivery channels and geographical location;
b. assist OFIs in assessing their ML/TF risks;
c. enable OFIs implement an AML/CFT programme appropriate to their size, nature and complexity;
d. enhance the OFI's understanding of its vulnerability to ML/TF risks; and
e. assist OFIs to allocate resources efficiently to mitigate the ML/TF risks.

6.2 Obligation for ML/TF Risk Assessment and Management

Regulation 5 of the AML/CFT Regulations requires institutions under the purview of the CBN to take appropriate steps to identify, assess and understand the ML/TF risk of their customers, geographic areas of operations, products, services and delivery channels.

It further requires institutions to document their risk assessment and consider all relevant risk factors before determining the overall level of risk and mitigation to be applied.

Regulation 40(1) of the AML/CFT Regulations also requires OFIs to identify and record areas of potential money laundering risks not covered by the Regulations and report to the CBN and NFIU as appropriate.

It is therefore obligatory for OFIs to conduct periodic risk assessment of their ML/TF risks in line with the aforementioned provisions.

6.3 Assessing Risk

There is no single prescribed methodology for ML/TF risk assessment in OFIs. However, the methods used should be sufficient in assessing the ML/TF risks.

Measures to be applied should take into consideration the following:

- the business lines and other operations;
- cross-border and international operations, if any, and linkages among others;
- any other relevant information.

6. RISK MANAGEMENT

OFIs are required to have policies, controls and procedures that enable them to effectively manage and mitigate the ML/TF risks that have been identified. They are also required to monitor the implementation of those controls and enhance them, where necessary. The policies, controls and procedures must be approved by senior management, and the measures taken to manage and mitigate the risks (whether higher or lower) should be consistent with regulatory requirements.

7.1 Risk Identification

The OFIs should identify sources of risk, areas of impacts, events (including changes in circumstances), causes and their potential consequences. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

OFIs must consider the risk posed by any element or any combination of the elements listed below:

- Customers
- Products and services
- Delivery channels
- Geographic location (jurisdictions).

- **Customers:** The followings are some indicators to identify ML/TF risk arising from customers:
  - a new customer
  - a new customer who wants to carry out a large transaction

- a customer or a group of customers making lot of transactions and/or maintaining several accounts in the same name or group
- a customer who has a business which involves large amounts of cash
- a customer whose identification is difficult to check
- customers conducting their business relationship or transactions in unusual circumstances, such as:
    - significant and unexplained geographic distance between the institution and the location of the customer.
    - frequent and unexplained movement of accounts to different institutions.
    - frequent and unexplained movement of funds between institutions in various geographic locations.
- a non- resident customer
- a corporate customer whose ownership structure is unusual and excessively complex
- customers that are politically exposed persons (PEPs) or influential persons (IPs) or head of international organizations and their family members and close associates
- customers submits account documentation showing an unclear ownership structure
- customer opens account in the name of his/her family member who intends to credit large amount of deposits not consistent with the known sources of legitimate family income
- a customer comes with premature liquidation of fixed deposit
- a customer who wants to settle his loan early
- government employee having several large amounts of fixed deposit accounts

- **Products and services:**
    - prioritized or privileged financial service
    - credit card
    - syndicate financing
    - anonymous transaction
    - non face to face business relationship or transaction
    - payment received from unknown or unrelated third parties
    - receivable financing
    - home equity and loan against deposits
    - sale and lease back facility
    - any new product & service developed
- **Delivery channels:**
    - direct to the customer (face-to-face)
    - online/internet
    - mobile banking
    - USSD
    - electronic wallet
    - email
    - third-party, agent or broker
- **Geographic location (Jurisdiction):**
    i. any country which is identified by credible sources as having significant level of corruption and criminal activity
    ii. any country subject to economic or trade sanctions
    iii. any country known to be a tax haven and identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country
    iv. any country identified by FATF/GIABA as not having adequate AML/CFT system

v. any country identified as destination of illicit financial flow

vi. branch in any land port, seaport city or any border area

- **Regulatory risk**

This risk is the probability of not meeting the requirements of extant laws and regulations governing AML/CFT in Nigeria. Examples of some of these risks are:

- customer/beneficial owner identification and verification (KYC) not properly done
- failure to keep record
- failure to train staff on AML/CFT
- absence of board approved AML/CFT policies/frameworks
- failure to report suspicious transactions or activities
- non rendition of AML/CFT returns to CBN
- not having an AML/CFT Compliance Officer
- failure to conduct Enhanced Due Diligence (EDD) for high risk customers (i.e, PEPs, IPs)
- not complying with any order for freezing or suspension of transaction issued by CBN or NFIU
- not submitting accurate information or statement requested by the CBN and other competent authorities.

7.2 Risk Assessment

The risk associated with an event is a combination of the likelihood and severity of occurrence. The likelihood of occurrence is the possibility of the risk occurring while the impact/severity represents the amount of loss or damage suffered by the institution. Having identified the ML/TF risks, OFIs need to assess the likelihood of occurrence and the severity/impact, if the risks crystalized.

Therefore, to measure the identified risks, OFIs should apply the risk rating scales for likelihood and impact in *Tables 1* and *2, respectively*.

LIKELIHOOD	X	IMPACT	=	RISK LEVEL/SCORE

- **Likelihood scale**

Three levels of risk are shown in Table 1, however, the OFIs can have as many as practicable. This likelihood can be ascertained based on the available information, group consultation or by applying subjective judgment.

Table 1: Likelihood scale

Frequency	Likelihood of an ML/TF risk
Very likely	Almost certain: it will probably occur
Likely	High probability it will happen
Unlikely	Unlikely, but not impossible

- **Impact scale**

The impact of an ML/TF risk, depending on the nature of business, should be rated from the following point of view:

- how the business would be affected if the OFI suffers a financial loss from either a crime or as a result of fines;
- the risk that a particular transaction may result in the loss of life or property through a terrorist act;
- the risk that a particular transaction may be involved in funds generated from any of the predicate offences;
- the risk that a particular transaction may be involved in financing of terrorism;

- reputational risk which could occur if an OFI is found to have (unknowingly) aided an illegal act;
- the OFI becoming part of legal proceedings as a result of litigation arising from being used as a channel for ML/TF;

Table 2: Impact scale

Consequence	Impact of an ML/TF risk
Major	**Huge consequences – major damage or effect. Serious terrorist act or large-scale money laundering.**
Moderate	**Moderate level of money laundering or terrorism financing impact.**
Minor	**Minor or negligible consequences or effects.**

- **Risk matrix and risk score**

The risk matrix combines LIKELIHOOD and IMPACT to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to be taken in view of the overall risk. How the risk score is derived can be seen from the risk matrix *(Figure 1)* and risk score table *(Table 3)* shown below. Four levels of risk score are shown in Figure 1 and Table 3, but OFIs can have as many levels as deemed necessary.

Figure 1: Risk matrix

Threat level for ML/TF risk

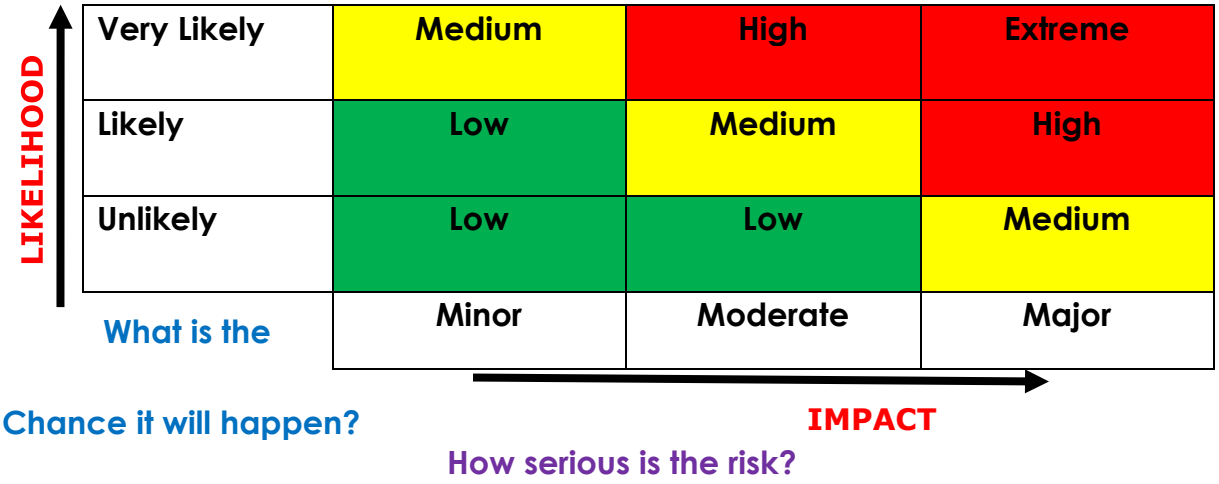

Table 3: Risk score table

Rating	Description
Extreme	Risk almost sure to happen and/or to have very serious consequences. Response: Do not allow transaction to occur without reducing the risk to acceptable level- Follow EDD
High	Risk likely to happen and/or to have major consequences. Response: Do not allow transaction until risk is reduced- Follow EDD
Medium	Possible this could happen and/or have moderate consequences. Response: May go ahead but preferably reduce risk- Follow standard CDD
Low	Unlikely to happen and/or have minor or negligible consequences. Response: Okay to go ahead.

7.3 Risk Reduction

This stage is about identifying and testing methods to manage the risks the OFI may have identified and assessed in the previous process. In doing this, they will need to consider putting in place strategies, policies and procedures to help reduce (or treat) the risk.

Examples of risk reduction or treatment are:

- setting transaction limits for high-risk products
- having a management approval process for higher-risk products
- process to place customers in different risk categories and apply different identification and verification methods
- not accepting transactions with a high-risk country.

Another way to reduce risk is to use a combination of risk groups to modify the overall risk of a transaction. The OFI may choose to use a combination of customer, product/service and geographic risk to modify an overall risk.

It is important to note that identifying a customer, transaction or geographic location as high risk, does not necessarily mean that money laundering or terrorism financing is involved. Similarly, where a customer or transaction is seen as low risk does not mean the customer or transaction is not involved in money laundering or terrorism financing. Therefore, judgement or experience should be applied to the risk management process of an entity.

7.4 Risk Monitoring and Review

In order to effectively monitor and review the risk plan:

- develop and carry out monitoring process;
- keep necessary records;
- review risk plan and AML/CFT programme;

- do internal audit or assessment; and
- do AML/CFT compliance report.

7.5 Review of ML/TF Risk Assessment

OFIs should put in place a mechanism to ensure that ML/TF risk assessment is up to date. Examples include:

- Setting a timeline on which the next risk assessment update will take place, to ensure emerging risks are included in risk assessment. Where the institution is aware of an emerging risk, or changes in the conditions affecting existing ratings, this should be reflected in risk assessment as soon as possible.

7. MONITORING AND INTERNAL CONTROLS

8.1 Internal Controls

The board of directors is ultimately responsible for the approval of AML/CFT programme and ensuring that the OFIs maintains an effective AML/CFT internal control structure, including suspicious activity monitoring and reporting. The Board is expected to create a culture of compliance to ensure that staff adhere to the institution's AML/CFT policies, procedures, and processes.

Internal controls are the institution's mechanism, rules, and procedures, designed to control risks in order to comply with the provisions of MLPA, 2011, TPA 2011 (as amended) and AML/CFT Regulations.

The level of sophistication of the internal controls should be commensurate with the size, structure, risks and complexity of the financial institution. The internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive AML/CFT compliance programme.

The internal controls should:

a. identify OFIs´ operations (i.e. products, services, customers, entities and geographic locations) that are more vulnerable to abuse by money launderers and criminals. They should ensure that the institution provides for periodic updates to its risk profile and has AML/CFT compliance programme that is tailored to manage risks;
b. be such that the board of directors or its committee thereof and senior management are informed of AML/CFT compliance initiatives, identified compliance deficiencies and corrective actions taken, and the directors and senior management should be notified of returns rendered to the regulatory authorities;
c. provide for programme continuity by way of back-up and retrieval;

d. provide for meeting all regulatory record-keeping and reporting requirements, implement all recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations;
e. cover the implementation of risk-based CDD policies, procedures and processes;
f. ensure that all the required AML/CFT reports are accurate and rendered promptly. OFIs are required to centralize their review and report-rendition functions within a unit in the branches and head-offices;
g. provide for dual controls and the segregation of duties as much as possible. For example, employees that complete the reporting forms (such as STRs and CTRs should not also be responsible for taking the decision to file the reports;
h. provide sufficient controls and systems for rendering CTRs;
i. provide sufficient controls and systems of monitoring timely detection and reporting of suspicious activity;
j. provide for adequate supervision of employees that handle currency transactions, complete reporting formats, grant exemptions, monitor suspicious activity or engage in any other activity covered by the MLPA, TPA, AML/CFT Regulations and other guidelines;
k. incorporate MLPA, TPA and AML/CFT Regulations compliance into the job descriptions and performance evaluations of staff, as appropriate; and
l. provide for the training of employees to be aware of their responsibilities under the AML/CFT Regulations and internal policy guidelines.

OFIs should ensure that they have controls in place to identify emerging ML/TF risks and incorporate them in their risk assessments in a timely manner. Examples of controls that could help in identifying emerging risks include:

- processes to ensure that internal information is reviewed regularly to identify trends and emerging issues;

- processes to ensure that institution regularly reviews relevant information from sources such as:
  a. the Nigerian National Risk Assessment.
  b. advisory issued by NFIU.
  c. guidance, circulars, and other administrative letters issued by the Central Bank of Nigeria and other relevant regulatory bodies.
  d. information obtained as part of the initial CDD process.
  e. the institution's own knowledge and expertise.
  f. information from industry bodies.
  g. changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates.
  h. information from international institutions and standard setting bodies relevant to ML/TF risks (e.g. UN, IMF, Basel, FATF, GIABA).
  i. other credible and reliable sources that can be accessed through commercially available databases or tools on a risk-sensitive basis.
- processes to capture and review information on risks relating to new products;
- engagement with other industry representatives, competent authorities (e.g. round tables, conferences and training providers), and processes to provide feedback on relevant findings; and
- establishing a culture of information sharing and strong ethics within the institution.

8.2 Self-Assessment of Controls

OFIs should ensure that a self-assessment of controls is conducted on an ongoing basis. The AML/CFT control assessment is an important component of the AML/CFT programme because of the adequacy and effectiveness it provides.

The assessments of business unit could be conducted by individuals in those units. OFIs should ensure that the assessment process is designed to enable results in each area to be consolidated for reporting and analysis.

The self-assessment in each relevant area of the OFI should at a minimum, cover the adequacy of the inherent risk assessment, AML/CFT policies and procedures, training, and other controls implemented to mitigate ML/TF risks.

OFIs should ensure that the self-assessment is neither too narrow nor too broad. For example, a narrow legal/regulatory-based assessment could fail to cover broader ML/TF controls. Similarly, an operational-based assessment might fail to cover prescribed controls.

All significant information used in the self-assessment process should be verified or readily verifiable. Methods used to ensure that information is verified or verifiable will depend on the size, complexity and governance structure of the OFI.

The self-assessment of controls should provide OFIs with:

- insight into the efficacy of controls in the AML/CFT programme, and the overall extent to which the programme adequately mitigates the identified ML/TF risks; and
- information to aid in prioritizing or allocating resources to areas of higher risk.

8.3 Testing for the Adequacy of the AML/CFT Compliance

Independent testing (audit) should be conducted by the internal audit department, external auditors, consultants or other qualified independent parties. While the frequency of the testing is not specifically defined in any guideline, a sound practice is for an OFI to conduct independent testing at least once in every 12 months or a shorter period that is commensurate with the ML/TF risk profile of the institution.

The person(s) conducting the AML/CFT testing should report directly to the board of directors or to a designated board committee.

Those persons responsible for conducting an objective independent evaluation of the written AML/CFT compliance programme should perform testing for specific compliance with the MLPA, TPA, AML/CFT Regulations and other related requirements. They are required to also evaluate pertinent management information systems (MIS). The audit has to be risk-based and must evaluate the quality of risk management for all the OFI's operations.

Risk-based audit testing will depend on the institution's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity and use of technology. An effective risk-based audit programme will cover all of the institution's activities.

The testing should assist the board of directors and management in identifying areas of weakness or areas where there is need for stronger controls.

Independent testing should at minimum include:

a. the evaluation of the overall adequacy and effectiveness of the AML/CFT Compliance programme, including policies, procedures and processes. This evaluation will contain an explicit statement about the AML/CFT compliance programme's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer to reach a conclusion about the overall quality of the AML/CFT compliance programme;
b. a review of risk assessment for reasonableness given the institution's risk profile (products, services, customers, entities and geographic locations);

c. appropriate risk-based transaction testing to verify record keeping and rendition of returns requirements on PEPs, STRs and CTRs information sharing requests;
d. an evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions (if applicable);
e. a review of staff training for adequacy, accuracy and completeness;
f. a review of the effectiveness of the suspicious transaction monitoring systems (whether manual, automated or a combination of both) used for AML/CFT compliance.
g. an assessment of the overall process for identifying and reporting suspicious transaction, including a review of filed or prepared STRs to determine their accuracy, timeliness, completeness and effectiveness of the institution's policy; and
h. an assessment of the integrity and accuracy of MIS used in the AML/CFT Compliance programme.

The auditors' reports should include their documentation on the scope of the audit, procedures performed, transaction testing completed and findings of the review. All audit documentation and work-papers should be made available for the regulators to review. Any violations, policy and/or procedures exceptions or other deficiencies noted during the audit exercise should be included in the audit report and forwarded to the board of directors or its designated committee in a timely manner.

The board or designated committee and the audit staff are required to track the deficiencies observed in the auditors' report.

8. RETURN RENDITION, MAINTENANCE OF RECORDS AND SANCTIONS

9.1 AML/CFT Returns Rendition

The AML/CFT Regulations, 2013 requires OFIs to render AML/CFT returns to the NFIU and CBN as appropriate. To comply with this requirement, it is proper for OFIs to configure their business applications to generate the returns and transmit the same to the appropriate competent authorities within the regulatory submission deadlines as specified by the CBN from time to time.

9.2 Maintenance of Records

Procedures for keeping paper and electronic records of pertinent information about customers and transactions must comply with all the requirements for record-keeping prescribed in Regulation 29 of the CBN AML/CFT Regulations, 2013 (as amended).

Also, other important information to be retained include:

- **corporate entities**: prescribed and additional information obtained on the entity and its beneficial owners;
- **large cash transactions**: large cash transaction records; related customer records;
- **account opening**: prescribed information about individuals and entities;
- **transactions in foreign currencies and with non-account holder**: prescribed information about the individual and entities;
- **prescribed incoming EFTs**: prescribed information;
- **trusts with respect to which trust companies are trustees**: a copy of trust deed and other prescribed information;
- **accounts of PEPs**: PEP office or position and other prescribed information;
- **transactions of PEPs**: PEP office or position and other prescribed information;
- **electronic card accounts, account opening and accounts of PEPs**: PEP office or position and other prescribed information;

- where applicable, for foreign correspondent banking relationships, names and addresses and other prescribed information;
- **suspicious transactions and attempted suspicious transactions**: investigations and conclusions; and
- other information not specifically mentioned above but would be relevant for AML/CFT control.

OFIs are expected to use record-keeping methods and formats that are appropriate in their particular circumstances, provided that records required by the ML/TF Acts and Regulations must, as a general rule, be kept for at least 5 years and they must be made available to competent authorities on a timely basis.

Customer information should be kept up to date in compliance with regulatory requirements.

A process should be implemented for dealing with incomplete documentation to ensure that it is up to date before doing more transactions.

9.3 Sanctions

OFIs should note that breaches and non-compliance with the relevant extant laws and regulations on AML/CFT/CPF would be penalized in accordance with the provisions of the CBN AML/CFT (Administrative Sanctions) Regulations, 2018.

Glossary

The following meanings apply in this Guidance Note:

AML	Anti-money laundering
AML/CFT programme	An OFI's AML/CFT programme designed to comply with this Guidance NoteNote
Board	Board of Directors. References to "Board" should be read as references to the Principal Officer of foreign bank branches and the Chief Agent of branches of foreign life insurance companies, as appropriate
AML/CFT Regulations	Central Bank of Nigeria Anti-Money Laundering and Combating of Terrorist Financing Regulation 2013 (as amended)
CDD	"Customer Due Diligence" this means identification and verification of customer's identity
CCO	"Chief Compliance Officer". A disignated indvidual responsible for the implemention of AML/CFT programme
CRT	"Currency Transaction Report" is the report filed with NFIU for cash transactions of over #5,000,000 for individual and #10,000,000 for body corporate in compliance with Regulation 10 (1) of MLPA, 2011
EDD	"Enhnanced Due Diligence" this refers to additional steps of examination and caution that financial institutions are required to obtain or take to identify their customers, their activities and confirm the legitimacy of the funds
EFTs	Electronic Funds Transfers
FATF	Financial Action Task Force on Money Laundering
GIABA	Inter-Governmental Action Group Against Money Laundering in West Africa
HOC	"Head of Compliance" Person designated under CBN AML/CFT Regulations for implementing the OFI's AML/CFT programme, referred to by CBN as the Chief Anti-Money Laundering Officer

KYC	"Know Your Customer" is used to describe a set of money laundering control policies and procedures that are employed to determine the true identity of customer.
MIS	Management Information System
ML/TF	Money Laundering and Terrorism Financing
NFIU	Nigeria Financial Intelligence Unit
OFIs	Other Financial Institutions – includes microfinance banks, primary mortgage banks, finance companies, development finance institution and bureau de change companies in respect of their business in Nigeria
ML	Money Laundering
MLPA	Money laundering Prohibition Act 2011 (as amended)
PEPs	Politically Exposed Persons
PRIVATE BANKING ACCOUNT	This is a special account for high-net worth individuals in which an indvidual "private banker" co-ordinates the financial institution's services with customer's requirements
STR	Suspicious Transaction Report
TF	Terrorism Financing
UN	United Nations
UNSC	United Nations Security Council