FRAMEWORK FOR AML/CFT RBS OF FINANCIAL INSTITUTIONS

CONTENTS

OUTLINE OF THE AML/CFT RBS FRAMEWORK

A. INTRODUCTION

The Money Laundering (Prohibition) Act, 2004 (MLPA), Central Bank of Nigeria Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Regulation, 2009 and other AML/CFT Guidelines provide guidance to Bank Examiners to carry out AML/CFT risk-based supervision (RBS), regulation and examination of banks and other financial institutions under the regulatory purview of the CBN. As effective AML/CFT Compliance Program requires sound risk management, **this AML/CFT RBS Manual provides guidance on identifying and controlling risks associated with money laundering and terrorist financing.**

The Manual therefore contains an overview of AML/CFT compliance program requirements, money laundering and terrorist financing risks, risk management expectations, industry sound practices and examination procedures. The purpose of developing this Manual is to ensure consistency in the application of the AML/CFT requirements.

STRUCTURE OF MANUAL

In order to effectively apply resources and ensure compliance with the requirements of the relevant laws and regulations, the Manual is structured to allow Bank Examiners to tailor the **scope** of their AML/CFT examination and **procedures** to the specific risk profile of the financial institution. The Manual consists of the following sections:

i. Introduction;
ii. Overview of Core Examination and Procedures for **Assessing the AML/CFT Compliance Program;**
iii. Overview of Core Examination and Procedures for **Regulatory Requirements and Related Topics;**
iv. Overview of Expanded Examination and Procedures for **Consolidated and Other Types of AML/CFT Compliance Program Structures;**
v. Overview of Expanded Examination and Procedures for **Products and Services;**
vi. Overview of Expanded Examination and Procedures for **Persons and Entities;** and
vii. Appendices.

The **core and expanded overview** sections provide narrative guidance and background information on each topic. Each overview is followed by examination procedures.

The sections on **"Core Examination Overview and Procedures for Assessing the AML/CFT Compliance Program" and the "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics"** (core) serve as a platform for the AML/CFT examination. They, for the most part, address the legal and regulatory requirements of the AML/CFT Compliance Program.
The sections on the **"Scoping and Planning" and "ML/FT Risk Assessment"** help the Bank Examiner develop an appropriate examination plan based on the risk profile of the financial institution.

Where a **topic is covered in both core and expanded sections** such as funds transfers and foreign correspondent banking, the core overview and examination procedures are articulated to address the requirements of laws and regulations while the expanded overview and examination procedures are made to address the money laundering risks of a specific activity.

At a minimum, Bank Examiners are required to use the following **examination procedures** (which are included within the "Core Examination Overview and Procedures for Assessing the AML/CFT Compliance Program" section of this manual) to ensure that the **financial institution has an adequate AML/CFT Compliance Program** which is commensurate with its risk profile:

i. Scoping and Planning;
ii. ML/FT Risk Assessment;
iii. AMLCFT Compliance Program; and
iv. Developing Conclusions and Finalizing the Examination.

Bank Examiner is required to have a good overview and examination procedures that will assist him to examine a financial institution's policies, procedures and processes in order to ensure compliance with sanctions imposed by CBN, Nigeria Deposit Insurance Corporation (NDIC), Nigeria Financial Intelligence Unit (NFIU) and other regulatory bodies. As part of the scoping and planning procedures, Bank Examiners are also required to **review the financial institution's risk assessment and independent testing** in order to **determine the extent to which a review of the institution's compliance program should be carried out** during the examination.

The **expanded sections** address specific lines of business, products, customers or entities that may present unique challenges and exposures for which the institution should institute appropriate policies, procedures and processes. It should be noted here that the absence of appropriate controls in these lines of business, products, customers or entities could elevate money laundering risks. The expanded section also provides guidance on AML/CFT Compliance Program structures and management.

Bank Examiner should be aware that all the core and expanded examination procedures contained in this Manual may not be applicable to every financial institution. The specific examination procedures that need to be performed will therefore depend on the money laundering risk profile of the institution, the quality & history of compliance with

MLPA,2004, AML/CFT Regulation, 2009 and quantity of independent testing and other relevant factors.

BACKGROUND

It is MLPA, 2004 and CBN AML/CFT Regulation, 2009 that establish the requirements for record-keeping and reporting by designated non-financial institutions, businesses & professions, banks and other financial institutions. Relevant provisions of the law and regulation above were designed to **help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of Nigeria, or deposited in financial institutions in the country.**

The enabling Act & Regulation under reference seek to achieve the above objective by requiring individuals, banks and other financial institutions to **render currency transaction reports** (CTRs) to the CBN (AML/CFT Office in Financial Policy & Regulation Department) and Nigerian Financial Intelligence Unit (NFIU), **properly identify persons conducting transactions** and **maintain a paper trail** by keeping appropriate records of their financial transactions. Should the need arise, these records will enable law enforcement and regulatory agencies to pursue investigations of criminal, tax & regulatory violations, and provide useful evidence in prosecuting money laundering and other financial crimes.

The MLPA, 2004 and CBN AML/CFT Regulation, 2009 apply equally to all banks, other financial institutions and persons that are under the regulatory purview of the CBN. The law also imposes criminal liability on a person or financial institution that knowingly assists in the laundering of money or fails to report suspicious transactions conducted through it. The CBN Regulation also directs financial institutions to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and record-keeping requirements of the MLPA, 2004.

SUSPICIOUS TRANSACTION REPORT

A financial institution is required to render a STR to NFIU and inform the CBN of same whenever it detects a known or suspected criminal violation of MLPA or a suspicious transaction related to money laundering activity or a violation of other laws & regulations.
The EFCC Act criminalizes the financing of terrorism. CBN AML/CFT Regulation, 2009 has also augmented the existing MLPA legal framework by strengthening customer identification procedures, prohibiting financial institutions from engaging in business with foreign shell banks, requiring financial institutions to have due diligence procedures (in some cases, have enhanced due diligence (EDD) procedures for foreign correspondent and private banking accounts) and improving information sharing between financial institutions and the law enforcement agencies (LEAs) and regulators.

PROVISIONS OF MLPA & CBN AML/CFT REGULATION:

i. Require financial institutions to have AMLCFT Program;
ii. Provide for civil and criminal penalties for money laundering;
iii. Give CBN the authority to impose sanctions for AML/CFT infractions committed by institutions and persons in course of transactions;
iv. Facilitate access to records and require financial institutions to give prompt response to regulatory requests for information; and
v. Require financial institutions to consider their AML/CFT records when reviewing mergers, acquisitions and other applications for business combinations.

ROLE OF GOVERNMENT AGENCIES IN THE MLPA & AML/CFT REGULATION, 2009

Certain government agencies play a critical role in implementing AML/CFT Regulations, developing examination guidance, ensuring compliance with and enforcement of the MLPA. These agencies include the CBN, EFCC/NFIU, Federal Ministry of Commerce and Nigeria Custom Service, etc.

There is no financial institution that is currently and temporarily exempted from the requirements of the law and regulation to establish an AMLCFT Program. All government bodies are therefore required to support the fight against money laundering and terrorist financing.

CENTRAL BANK OF NIGERIA

The law and regulation on AML/CFT authorize the CBN to require financial institutions to establish AML Programs, file certain reports and keep certain records of transactions. The relevant provisions have been extended to cover not only traditional deposit money banks but other financial institutions such as discount houses, micro-finance banks, finance houses, bureau de change, operators of credit card systems, etc that are under regulatory purview of the CBN, including their foreign branches, affiliates and subsidiaries.

The Federal Ministry of Commerce, Securities & Exchange Commission (SEC) and National Insurance Commission (NAICOM) are mandated to oversight designated non-financial institutions, businesses & professions (DNFBPs) such as dealers in jewellery, car & luxury goods, chartered accountants, audit firms, tax consultants, clearing & settlement companies, legal practitioners, hotels, casinos, supermarkets; savings associations and credit unions such as money services businesses, brokers/dealers in securities, futures commission merchants, mutual funds; and insurance companies respectively in order to properly cover the entire financial sector.

The CBN, NFIU, SEC, NAICOM, etc collaborate among themselves to carry out consolidated supervision/examination, carry out oversight and enforcement functions of

regulated institutions in order to eliminate any arbitrages. These regulatory agencies are empowered to use their authority to enforce compliance with appropriate banking rules and regulations, including compliance with the MLPA.

NIGERIAN FINANCIAL INTELLIGENCE UNIT

While the EFCC Act was first enacted in 2002 and amended in June 2004, the NFIU was established by Sections 1(2) & 12(2) of the EFCC Act, 2004. The unit is responsible for the **receipt, analysis and dissemination** of suspicious transaction (STRs) and currency transaction reports (CTRs). NFIU is an autonomous body residing in Economic and Financial Crimes Commission (EFCC). It interprets AML/CFT guidance issued, provides outreach to regulated institutions on rendition of returns, supports (by way of collaboration) the AML/CFT examination functions performed by regulatory agencies such as CBN, SEC, NAICOM, etc. NFIU's other significant responsibilities include providing intelligent information to support cases investigated by the law enforcement agencies (LEAs), identifying and communicating financial crime trends and patterns to the stakeholders and fostering international cooperation with its counterparts worldwide.

FEDERAL MINISTRY OF COMMERCE

The Federal Ministry of Commerce (FMC) is the competent supervisory authority for designated non-financial businesses & professions (DNFBPs), which include casinos, real estate agents, dealers in precious stones, and the legal and accounting professions. The DNFBPs were not regulated for AML/CFT measures before the enactment of the MLPA, 2004. Sections 46 of the EFCC Act, 2004 and 24 of the MLPA, 2004 have, however, expanded the definition of reporting entities to include DNFBPs.

Section 5 of MLPA, 2004 empowers the Ministry to monitor all DNFBPs in Nigeria and ensure appropriate compliance with AML/CFT requirements. Under section 5(6) of the MLPA, the FMC can impose sanctions on defaulting DNFBPs. While the supervisory functions of FMC are conducted through the Special Control Unit on Money Laundering (SCUML), section 7(2) of the EFCC Act, 2004 empowers the Commission to prosecute any designated non-financial institution for any breach of the MLPA.

SPECIAL CONTROL UNIT AGAINST MONEY LAUNDERING (SCUML)

SCUML was established in September, 2005 by Decision No EC (2005) 286 of the Federal Executive Council (FEC) as a specialized unit of the FMC with the responsibility to supervise DNFBPs in Nigeria. Consequently, SCUML has been mandated to monitor, supervise and regulate the activities of all DNFBPs.
The FMC in implementation of the relevant sections of MLPA, 2004 has developed the FMC/SCUML Register for all casinos in Nigeria. Though the officially known casinos is not significant in size, there is a number of small 'underground' ones.
In addition to measures taken to prevent criminals or their associates from holding controlling interests in casinos business, the Nigerian authorities have also ensured that

beneficiary owners of casinos are 'fit and proper' by the regulation and monitoring framework put in place by the FMC/SCUML.

THE NATIONAL INSURANCE COMMISSION (NAICOM)

The Commission is responsible for providing regulatory/supervisory oversight in the Nigerian insurance industry. It regulates, supervises, controls and ensures effective administration of regulated entities in the insurance sector. NAICOM is guided in its supervisory responsibilities by the National Insurance Commission Act (as amended), the Insurance Industry Policy Guidelines, 2005, Know Your Customer Guidelines for Insurance Institutions. Institutions operating in the Nigerian insurance sector are registered by NAICOM by sections 3, 4, 36 and 45 of the Insurance Act 2003.

THE SECURITIES AND EXCHANGE COMMISSION (SEC)

SEC is the apex regulatory and supervisory authority of the Nigerian capital market. The Investment and Securities Act (ISA) 1999, in section 8, grants the SEC powers to regulate investments and securities in Nigeria, protect the integrity of the securities market against abuses arising from activities of the operators and prevent fraudulent and unfair trade practices in the securities industry. SEC applies ISA, No.45,1999 and SEC Rules and Regulations, 2000 (as amended) in the performance of its regulatory and supervisory functions.

THE NIGERIA CUSTOMS SERVICE (NCS)

The Customs and Excise Management Act, CAP 84 (LFN 1990 (CEMA) established the Nigeria Customs Service (NCS). The Nigeria Customs Service is charged with the duty of controlling and managing the administration of the Customs and Excise laws. The NCS collects the revenue of Customs and Excise and accounts for same in such manner as provided for by the relevant legislation. The MLPA empowers NSC to report declaration in respect of information on the cross border transportation of currency in and out of the country [section 12 of the Foreign Exchange (Monitoring & Miscellaneous Provision) Act 1995] to the CBN and SEC while the latter institutions render weekly reports of same to EFCC.

THE NATIONAL FOCAL POINT (NFP)

In realization of the African Union's Plan of Action made in 2002 in Algiers, the 53 (fifty-three) member nations of the Union were required to establish a forum to facilitate timely exchange and sharing of ideas and intelligence in combating terrorism within the continent. This led to the establishment of the African Centre for the Study and Research on Terrorism (ACSRT).

Member countries were also mandated to establish National Focal Points on Terrorism. In compliance, the Nigerian government established the National Focal Point coordinated by the Department of State Services (DSS). The National Focal Point

membership is drawn from several stakeholder government ministries, departments and agencies.

The activities of the National Focal Point include:

i. Conducting research and analysis on terrorism-related matters in order to provide prompt and proactive response to terrorist threats;
ii. Collation, integration and preparation of input provided by intelligence services with a view to advising the relevant authorities on counter terrorism policies;
iii. Identifying, penetrating and monitoring of extremist/ fundamentalist groups and suspected NGOs with a view to intercepting the recruitment process of terrorists;
iv. Implementation of all policies on counter terrorism and its financing by monitoring the activities of financial institutions;
v. Developing and maintenance of a national repository data-base on terrorist groups;
vi. Maintaining and updating of data-base on the movement and activities of passengers from risk countries;
vii. Maintenance of security watch-list on individuals and groups; and
viii. Maintenance of close watch and regulation of the use of explosives in liaison with relevant government agencies or parastatals.

OVERVIEW OF REGULATORY AGENCIES IN NIGERIA FINANCIAL SECTOR

The regulatory agencies are responsible for the oversight of the various financial institutions operating in Nigeria, including foreign-owned subsidiaries of Nigerian banks and other financial institutions. While the Corporate Affairs Commission (CAC) is charged with the registration of banks and other financial institutions, the CBN is responsible for the licensing them. SEC & NAICOM license the capital market operators and insurance businesses respectively. The enabling statutes of these regulators require them to review the AML/CFT Compliance Program at each examination of the regulated institutions. They are also required to use the authority granted them under their Acts to enforce compliance with appropriate rules and regulations, including compliance with AML/CFT regulations.

These agencies require each institution under their supervisory purview to establish and maintain AML/CFT Compliance Program. **The program guards against money laundering and terrorist financing transactions and ensures compliance with and implementation of money laundering laws and regulations.** Financial institutions are required to take reasonable and prudent steps to combat money laundering and terrorist financing and minimize their vulnerability to the risk associated with such activities.

Some financial institutions have damaged their reputations and have been required to pay civil financial penalties for failing to implement adequate controls within their institutions as a result of non-compliance with the MLPA & AML/CFT Regulation, 2009.

In addition, AML/CFT assessment is also required as part of application process, since such AML/CFT concerns will have an impact on the financial institution's strategic plan. For this reason, it is the regulatory agencies' high supervisory priority to provide guidance that assists the regulated institutions in complying with the MLPA & AML/CFT Regulation.

The regulatory agencies are required to ensure that the institutions they supervise understand the importance of having an effective AML/CFT Compliance Program in place. Managements of the regulated institutions are also required to be vigilant & ensure they have AML/CFT Compliance Program, especially as business grows and new products and services are introduced. To this end, an evaluation of the institution's AML/CFT Compliance Program and its compliance with the regulatory requirements of the AML/CFT Regulation must be made an integral part of the supervisory process.

As part of a strong AML/CFT compliance program, the regulatory agencies are required to ensure that a financial institution has policies, procedures and processes to identify and report suspicious transactions to NFIU and inform the CBN and the appropriate law enforcement agencies as required by the AML/CFT Regulation. The Bank Examiners' supervisory processes are required to assess whether the financial institution has established the appropriate policies, procedures and processes based on its money laundering risk in order to identify and report suspicious transaction and that the AML/CFT reports produced provide sufficient details to the law enforcement agencies to make such reports useful for further investigation.

The regulatory authorities have specific powers to impose controls on transactions and freeze assets held within Nigeria-jurisdiction. Many of such sanctions are based on United Nations and other international mandates. They are multilateral in scope and involved close cooperation with allied governments and the financial institutions concerned.

MONEY LAUNDERING AND TERRORIST FINANCING

The MLPA & AML/CFT Regulation, 2009 are intended to safeguard Nigerian financial system and the financial institutions that make up the system from the abuses of financial crime, including money laundering, terrorist financing and other illicit financial transactions. Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects to the Nigerian and word economy.

From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign & local officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economy. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism or conduct other illegal activities in order to ultimately hide the actual purpose of their activity.

Financial institutions are required to develop, implement and maintain effective AML/ CFT Programs that address the ever-changing strategies of money launderers and terrorists who attempt to gain access to the Nigerian financial system. A sound AML/CFT Compliance Program is critical in deterring and preventing these types of activities at or through banks and other financial institutions.

MONEY LAUNDERING

Money laundering is the criminal practice of processing ill-gotten gains or "dirty" money through series of transactions. In this way, the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process.

Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

Placement

The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting attention of the financial institution or law enforcement agencies. Placement techniques include structuring currency deposits in small amounts in order to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund cheque from a cancelled vacation package, insurance policy or purchasing a series of monetary instruments (e.g. cashier's cheques or money orders) that are then collected and deposited into accounts at another location or financial institution.

Layering

The second stage of the money laundering process is layering and this involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in one or more financial institutions

Integration

The ultimate goal of the money laundering process is integration. Once the funds are in the financial system, they are insulated through the layering stage. The integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts or other assets.

TERRORIST FINANCING

The **motivation behind terrorist financing is ideological as opposed to profit-seeking.** The latter is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An ineffective AML/CFT controls in financial infrastructure could be readily exploited to the advantage of the terrorist financier(s).

Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Terrorists generally finance their activities through both **unlawful and legitimate sources. Unlawful activities** such as extortion, kidnapping and narcotics trafficking have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds and improper use of charitable or relief funds.

In the case of charitable or relief funds, donors may have no knowledge that their donations have been diverted to support terrorist causes. **Other legitimate sources** found to provide terrorist organizations with funding include foreign government sponsors, business ownership and personal employment. These legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers can use currency smuggling, structured deposits or withdrawals from bank accounts; purchase various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers.

There is also evidence that some forms of informal banking (e.g. "hawala") have played a role in moving terrorist funds. Transactions through hawalas are difficult to detect given the lack of documentation, their size and the nature of the transactions involved.

CRIMINAL PENALTIES FOR MONEY LAUNDERING/TERRORIST FINANCING, AND VIOLATIONS OF THE MLPA & AML/CFT REGULATION

Penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering risks serving certain terms of imprisonment as provided in the relevant sections of the MLPA and financial penalties as provided for in the law and AML/CFT Regulation. Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property (under certain conditions) entire bank accounts (even if some of the money in the account is legitimate) may be subject to forfeiture as provided for in the EFCC Act.

Pursuant to various statutes, banks, other financial institutions and individuals may incur criminal and civil liability for violating AML/CFT laws. For instance, the EFCC may bring criminal actions for money laundering that may include fines, imprisonment and forfeiture actions. In addition, banks and other financial institutions risk losing their licences, and their employees risk being removed and barred from the financial industry.

Moreover, there are penalties for wilful violations of the MLPA and AML/CFT Regulation, 2009 for structuring transactions to evade the reporting threshold. For example, a person, including a bank employee, wilfully violating the MLPA or the AML/CFT Regulation is subject to a financial sanction or some term of imprisonment or both as provided for in the MLPA, 2004. A financial institution that violates certain provisions of MLPA & AML/CFT Regulation, 2009 is subject to financial sanctions that must be published in its financial statements in line with the relevant section of Bank Other Financial Institution Act (as amended) [BOFIA].

CIVIL PENALTIES FOR VIOLATIONS OF THE MLPA

Pursuant to the relevant sections of their enabling statutes, the various regulatory agencies are empowered to bring administrative financial sanctions for violations of the MLPA. In addition to criminal and civil financial penalty imposed, individuals' appointment may be terminated in pursuant of section 1.18.1.4(b) of AML/CFT Regulation, 2009 as long as the violation was intentional.

It is proper we note here that the actions contained in this AML/CFT Risk-based Supervision Manual are publicly available in various documents.

B. OVERVIEW OF CORE EXAMINATION AND PROCEDURES FOR ASSESSING AML/CFT COMPLIANCE PROGRAM

1. OVERVIEW OF SCOPING AND PLANNING

Objective

Identify the financial institution's money laundering risks, develop the examination scope and document the plan.
This process includes determining the number of staff required for the examination (staffing needs) technical expertise involved and selecting the examination procedures to be adopted.

The AML/CFT examination is intended to assess the effectiveness of the financial institution's AML/CFT Compliance Program, its compliance with the Money Laundering (Prohibition) Act, CBN AML/CFT Regulation, 2009, etc and to review its risk management practices.

Whenever possible, the scoping and planning process should be completed before entering into the financial institution. During this process, it may be helpful to discuss AML/CFT matters with the financial institution management, including the Chief Compliance Officer (CCO), either in person or by telephone.

The scoping and planning process generally begins with analysis of the following:

i. Off-site monitoring of information/reports;
ii. Prior AML/CFT Examination Reports and Work-papers;
iii. Items requested to be supplied and form filled by the institution's management;
iv. The financial institution's ML/FT Risk Assessment Reports;
v. The financial institution's AML/CFT reporting database on Currency, Suspicious, Politically Exposed Persons (PEPs) transactions, etc; and
vi. Independent reviews or auditors' reports.

Review of the Financial Institution's ML/FT Risk Assessment Report

The scoping and planning process should be guided by the Bank Examiner's review of the financial institution's ML/FT risk assessment report. Information gained from the Examiner's review of the risk assessment will assist in the scoping and planning process as well as the evaluation of the adequacy of the AML/CFT Compliance Program.

If the financial institution has not developed a risk assessment, this fact should be discussed with management and noted.

For the purposes of the examination, whenever the financial institution has not completed its risk assessment or the risk assessment is inadequate, the Examiner must complete his risk assessment of the institution. As evaluation of ML/FT risk assessment is part of scoping and planning of the examination, we have therefore provided a section for it to emphasize its importance in both examination process and in the designing of effective risk-based controls in the institution.

Independent Testing

As part of the scoping and planning process, Bank Examiners are required to **obtain and evaluate the supporting documents of the independent testing (audit) report** of the financial institution's AML/CFT Compliance Program.
The scope and quality of the audit and report may provide the Examiners with a lead as to the particular risks in the financial institution, how these risks are being managed & controlled, and the status of its compliance with the MLPA, CBN AML/CFT Regulation, etc. The independent testing scope and work-papers may be of assistance to the Examiners in understanding the audit coverage and the quality and quantity of transaction testing.

The knowledge acquired is meant to assist the **Examiner in determining the scope of his examination, identifying areas requiring greater (or lesser) scrutiny and identifying when expanded examination procedures may be necessary.**

Examination Plan

At a minimum, Bank Examiners are required to conduct the examination procedures included in the following sections of this Manual in order to ensure that the financial institution has an adequate AML/CFT Compliance Program which is commensurate with its risk profile:

ii. Scoping and Planning;
iii. ML/FT Risk Assessment;
iv. AML/CFT Compliance Program;
v. Developing Conclusions and Finalizing the Examination.

The section on "Overview of Core Examination and Procedures for Regulatory Requirements and Related Topics" includes an overview and examination of the procedures used to examine a financial institution's AML/CFT policies, procedures and processes to ensure compliance with the relevant laws and regulation. As part of the scoping and planning procedures, Examiners are required to **review the financial institution's risk assessment and independent testing report** to determine the extent to which his review should be conducted on the financial institution's AML/CFT Compliance Program during the examination.

The Examiner is required to develop and document an initial examination plan commensurate with the overall ML/FT risk profile of the financial institution. This plan may change during the examination as a result of on-site findings and any changes to the plan should likewise be documented. In that case, the Examiner is required to **prepare a request letter to the financial institution, listing the items that will assist him effectively to carry out his work efficiently.**

On the basis of the risk profile, quality of audit, previous examination findings and initial examination work, the Bank Examiners should complete additional core and expanded examination procedures, as appropriate. To this end, the Bank Examiner must include an evaluation of the AML/CFT Compliance Program within the supervisory plan or cycle. At larger and more complex financial institutions, Examiners may review the various types of examination reports conducted throughout the supervisory plan or cycle to assess AML/CFT compliance. These reviews may focus on one or more business lines (e.g., private banking, trade financing or foreign correspondent banking relationships) based upon the financial institution's risk assessment and recent audit and examination findings.

Transaction Testing

Bank Examiners are required to perform transaction testing in order to evaluate the adequacy of the financial institution's compliance with regulatory requirements, determine the effectiveness of its policies, procedures, processes and evaluate suspicious activity monitoring systems. Transaction testing is an important factor that helps the Examiner in forming his conclusions about the integrity of the financial institution's overall controls and risk management processes. Transaction testing must be performed at each examination and should be risk-based. Transaction testing can be performed either through conducting the transaction testing procedures within the independent testing (audit) section or completing the transaction testing procedures within the core or expanded sections. The extent of transaction testing and activities conducted is based on various factors including the Examiner's judgment of risks, controls and the adequacy of the independent testing. Once on-site, the scope of the transaction testing can be expanded to address any issues or concerns identified during the examination.

Bank Examiners are required to document their decisions regarding the extent of transaction testing on **conduct**, the **activities** which the institution is required to perform, the **rationale for any changes to the scope of transaction testing** that occur during the examination cycle.

2. EXAMINATION PROCEDURES ON SCOPING AND PLANNING

Objective

Identify the financial institution's ML/FT risks, develop the examination scope and document the plan. This process includes **determining the number of staff required for the examination (staffing needs) and technical expertise and selecting examination procedures to adopt.**

In order to facilitate the Examiner's understanding of the financial institution's risk profile and to adequately establish the scope of AML/CFT examination, the Bank Examiner is required to carry out the following steps in conjunction with the review of the financial institution's ML/FT risk assessment:

ii. **Review prior examination or inspection reports, related work-papers and management's responses** to any previously identified MPLA and CBN AML Regulation issues. Identify the procedures adopted during a completed AML/CFT examination of the institution; identify in the reports the processes the financial institution uses to detect unusual activity; identify previously noted higher-risk in the institution's operations. Review the previous recommendations for the next examination.

In addition, **contact the appropriate management of the financial institution to discuss its:**

a. AML/CFT Compliance Program;

b. ML/FT Risk Assessment;

c. Suspicious transaction monitoring and reporting systems; and

d. Level and extent of its AML/CFT systems automation.

Bank Examiners are required to refer to the above topics in the appropriate sections on overview and examination procedures in this Manual for guidance.

iii. **Develop a list of MPLA and CBN AML Regulation items to be incorporated into the integrated examination request letter.** Bank Examiners are required to send their request letter to the financial institution where the AML/CFT examination is a stand-alone. Review the request letter and documents provided by the financial institution.

iv. **Review correspondence between the financial institution and its primary regulator,** if not already completed by the Bank Examiner in charge or other dedicated examination personnel. In addition, review correspondence that the financial institution or the primary regulators have received from or sent to outside regulatory and law enforcement agencies relating to AML/CFT compliance.

v. **Review STRs, PEPs, CTRs and CTR-exemption (if any) information obtained from AML/CFT reporting database.** The number of STRs, PEPs, CTRs and CTR-exemptions rendered should be obtained for a defined time period that covers the duration of the AML/CFT examination as determined by the Bank Examiner. Consider the above information and analyze the data for unusual patterns, considering the following:

a. Volume of activity and whether it is commensurate with the customer's occupation or type of business;
b. Number and Naira volume of transactions involving higher-risk customers;
c. Volume of CTRs in relation to the volume of exemptions (i.e., whether or not additional exemptions have resulted in significant decreases in CTR returns rendered); and
d. Volume of STRs and CTRs in relation to the financial institution's size, asset or deposit growth and geographic location. Bank Examiners should not criticize a financial institution solely because the number of STRs, PEPs or CTRs rendered is lower than STRs, PEPs or CTRs filed by "peer" institutions. However, as part of the examination, Bank Examiners must review significant changes in the volume or nature of STRs, PEPs and CTRs rendered and assess potential/possible reasons for these changes.

vi. **Review internal and external audit reports and work-papers for AML/CFT compliance** as necessary in order to determine the comprehensiveness and quality of audits, findings and management responses and corrective action. A review of the scope, procedures and

qualifications of the independent audit report will provide valuable information on the adequacy of the AML/CFT Compliance Program.

vii. **Though the CBN AML/CFT Regulation, 2009 are not part of the MPLA, evaluation of compliance with its provisions must be included in AML/CFT examinations.** It is the primary role of the Bank Examiner to identify the violations of the various provisions of MLPA and CBN AML/CFT Regulation and to evaluate the sufficiency of the institution's implementation of policies, procedures and processes to ensure compliance with AML/CFT laws and regulations.

In order to facilitate the Examiner's understanding of the financial institution's risk profile and to adequately establish the scope of the AML/CFT examination, the Examiner is required to:

a. **Review the reports of the financial institution's ML/FT risk assessment.** The risk assessment should consider the various types of products, services, customers, entities, transactions and geographic locations in which the financial institution is engaged, including those that are processed by, through, or to the financial institution in order to identify potential ML/FT exposures.
b. **Review the institution's independent testing of its AML/CFT Compliance Program.**
c. **Review correspondence received from Supervisory authorities** in order to determine whether or not the financial institution had any warning letters, fines or penalties imposed by them after the most recent AML/CFT examination.
d. **Review correspondence between the financial institutions and NFIU** (e.g. periodic reporting of suspicious & currency transactions and where applicable, the NFIU Annual reports on blocked property (if any)).

viii. **Develop an initial examination plan based on the above examination procedures and findings made from the review of the financial institution's ML/FT risk assessment.** Bank Examiners are required to adequately document the examination plan as well as any changes to it that occur during the examination. The scoping and planning process are designed to ensure that the Examiner is aware of the institution's AML/CFT Compliance Program, compliance history and risk profile of the institution's products, services, customers, entities, transactions and geographic locations.

Additional core and expanded examination procedures may be conducted, where necessary. While the examination plan may change at any time as a result of on-site findings, the initial risk assessment will enable the Bank Examiner to establish a reasonable scope for the AML/CFT review. In order for the examination process to be successful, the Bank Examiners is required to maintain an open communication line with the financial institution's management and discuss relevant concerns as they arise.

3. OVERVIEW OF ML/FT RISK ASSESSMENT

Objective

Assess the ML/FT risk profile of the financial institution and evaluate the adequacy of the institution's risk assessment process.

Evaluation of the ML/FT risk assessment is part of scoping and planning of the examination. Inclusion of a section on risk assessment in this Manual does not mean the two processes are separate. Rather, risk assessment is given its own section in order to emphasize its importance in the examination process and in the design of effective risk-based controls in the financial institution.

It is the same risk management principles that the financial institution uses in its traditional operational areas that applies to assessing and managing ML/FT risk. A well-developed risk assessment will therefore assist in identifying the financial institution's ML/FT risk profile. Understanding the risk profile enables the financial institution to apply appropriate risk management processes to the AML/CFT Compliance Program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the financial institution's controls.

The risk assessment should provide a comprehensive analysis of the ML/FT risks in a concise and organized presentation, and the latter should be shared and communicated with all business lines across the institution, board of directors, management and appropriate staff. As such, it is required (as sound practice) that the ML/FT risk assessment of the institution be reduced into writing by its management.

There are many effective methods and formats used in completing a ML/FT risk assessment as such, Bank Examiners are not required to advocate a particular method or format. Financial institution management should decide the appropriate method or format, based on its particular risk profile. However, the format chose by the management for the institution's risk assessment should be easily understood by all the stakeholders.

Development of the ML/FT risk assessment

i. **First, identify the specific risk categories (i.e. products, services, customers, entities, transactions and geographic locations) unique to the institution;** and
ii. **Second, conduct a more detailed analysis of the data identified for better assessment of the risk within the above categories.**

In reviewing the risk assessment during the scoping and planning process, Bank Examiners are required to determine whether or not the management of the institution has considered all the products, services, customers, entities, transactions and

geographic locations; and whether the management's detailed analysis within the specific risk categories above was adequate.

If the financial institution has not developed a risk assessment, this fact should be discussed with the management and observed by the Examiner. For the purposes of the examination (whether the financial institution has not completed a risk assessment or the risk assessment is inadequate) the Examiner is required to complete the risk assessment based on available information.

Evaluating financial institution's ML/FT Risk Assessment

Bank Examiner is required to review the financial institution's AML/CFT Compliance Program with sufficient knowledge of the institution's AML/CFT risks in order to determine whether the AML/CFT Compliance Program is adequate and contains the controls necessary to mitigate risks. For example, during the scoping and planning process of the examination, the Bank Examiner may initially observe that the financial institution has a high-risk profile, but during the AML/CFT examination proper, the Examiner may discover that the financial institution's AML/CFT Compliance Program contains adequate controls to mitigate these risks. Alternatively, the Examiner may initially observe that the institution has a low or moderate-risk profile while during the examination, the Examiner may notice that the financial institution's AML/CFT Compliance Program does not adequately mitigate these risks.

In evaluating the risk assessment, Examiner is not required to necessarily take any single indicator as determinative of the existence of a lower or higher ML/FT risk. The assessment of risk factors is financial institution-specific, and a conclusion regarding the risk profile should be based on a consideration of all pertinent information. The financial institution may determine that some factors should be weighed more heavily than others.

For example, the number of funds transfers is certainly one factor to be considered in assessing risk. However, in order to effectively identify and weigh the risks, the Examiner is required to look at other factors associated with those funds transfers, such as whether they are international or domestic, the dollar amounts involved and the nature of the customer relationships.

Identification of Specific Risk Categories

The first step of the risk assessment process is to **identify the specific products, services, customers, entities and geographic locations unique to the financial institution**. Although attempts to launder money, finance terrorism or conduct other illegal activities through a financial institution can emanate from many different sources, certain products, services, customers, entities and geographic locations may be more vulnerable or have been historically abused by money launderers and criminals.

Depending on the specific characteristics of the particular product, service or customer, the risks are not always the same. Various factors, such as **the number and volume of transactions, geographic locations and nature of the customer relationship**

should be considered when the financial institution prepares its risk assessment. The differences in the way a financial institution interacts with the customer (face-to-face contact versus electronic banking) also should be considered. Because of the factors above, risks will vary from one financial institution to another.

In reviewing the financial institution's risk assessment, the Examiner is required to **determine and note whether the management has developed an accurate risk assessment** that identifies the significant ML/FT risks to the financial institution.

Products and Services

Certain products and services offered by financial institution may pose a higher risk of money laundering or terrorist financing **depending on the nature** of the specific product or service. Such products and services may facilitate a higher degree of anonymity or are involved the handling of high volumes of currency or currency equivalents. **Some of these products and services listed below are not all inclusive:**

i. Electronic funds payment services-electronic cash (e.g. prepaid and payroll cards), funds transfers (domestic and international), payable upon proper identification (PUPID) transactions, third-party payment processors, remittance activity, automated clearing house (ACH) transactions, and automated teller machines (ATM).
ii. Electronic banking.
iii. Private banking (domestic and international).
iv. Trust and asset management services.
v. Monetary instruments.
vi. Foreign correspondent accounts (e.g. bulk shipments of currency, payable through accounts (PTA), and foreign currency drafts).
vii. Trade finance.
viii. Services provided to third party payment processors or senders.
ix. Foreign exchange.
x. Special use or concentration accounts.
xi. Lending activities, particularly loans secured by cash collateral and marketable securities.
xii. Non-deposit account services (e.g. non-deposit investment products and insurance).

Customers and Entities

Any type of account is potentially vulnerable to money laundering or terrorist financing. By the nature of their business, occupation or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that the financial institution exercises judgment and

neither define nor treat all members of a specific category of customer as posing the same level of risk.

In assessing **customer risk**, financial institutions are required to consider other variables such as **services sought and geographic locations**. **Guidance and discussion on specific customers and entities that are detailed below may be necessary:**

i. Foreign financial institutions, including banks and foreign money services providers (e.g. currency exchanges and money transmitters).
ii. Non-bank financial institutions (e.g. money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones, or jewels).
iii. Senior foreign & domestic political figures, their immediate family members and close associates [collectively known as politically exposed persons (PEPs)].
iv. Non-resident alien (NRA) and accounts of foreign individuals.
v. Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and private investment companies (PIC) and international business corporations (IBC)) located in higher-risk geographic locations.
vi. Deposit brokers particularly foreign deposit brokers.
vii. Cash-intensive businesses (e.g. convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs and parking garages).
viii. Non-governmental organizations and charities (foreign and domestic).
ix. Professional service providers (e.g. attorneys, accountants, doctors, or real estate brokers).

Geographic Locations

Identifying geographic locations that may pose a higher risk is essential to a financial institution's AML/CFT Compliance Program. Financial institutions are required to understand and evaluate the specific risks associated with doing business in, opening accounts for customers from or facilitating transactions involving certain geographic locations. However, **geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively.**

Analysis of Specific Risk Categories

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage. It is to help assess more accurately the associated ML/FT risk involved. This step involves evaluating data pertaining to the financial institution's activities (e.g. the number of domestic and international funds transfers; private banking customers; foreign correspondent accounts; PTAs and domestic and international geographic locations of the institution's business area and

customer transactions) in relation to customer identification program (CIP) and customer due diligence (CDD) information.

The level and sophistication of analysis may vary from one financial institution to another. The detailed analysis is important because within any type of product or category of customer there will be account holders that pose varying levels of risk.

This step (in the risk assessment process) gives management a better understanding of the financial institution's risk profile in order to develop the appropriate policies, procedures and processes to mitigate the overall risk. Specifically, **the analysis of the data pertaining to the financial institution's activities should consider, as appropriate, the following factors:**

ii. Purpose of the account.
iii. Actual or anticipated activity in the account.
iv. Nature of the customer's business/occupation.
v. Customer's location.
vi. Types of products and services used by the customer.

The value of a two-step risk assessment process is illustrated in the following example of data collected in the **first step of the risk assessment process which reflects that a financial institution sends out 100 international funds transfers per day:**

i. Further analysis may show that approximately 90 percent of the funds transfers are **recurring well-documented transactions for long-term customers;** and
ii. On the other hand, the analysis may show that 90 percent of these transfers **are non-recurring or are for non-customers.**

While the numbers are the same for the two examples above, the overall risks are different. As illustrated above, the institution's customer identification program (CIP) and customer due diligence (CDD) information must play important roles in this process.

Developing the Financial Institution's AML/CFT Compliance Program Based Upon Its Risk Assessment

Management is required to structure the financial institution's AML/CFT Compliance Program to adequately address its risk profile as identified by its risk assessment. Management should therefore understand its financial institution's ML/FT risk exposure and develop the appropriate policies, procedures and processes to monitor and control its ML/FT risks. For example, **the financial institution's monitoring systems should be able to identify, research and report suspicious activity. Such process must be risk-based with particular emphasis on higher-risk products, services, customers, entities and geographic locations as identified by the institution's ML/FT risk assessment.**

Note that independent testing (audit) is required to review the financial institution's risk assessment for reasonableness. Additionally, management is also required to consider the staffing resources and the level of training that are necessary to promote adherence with these policies, procedures and processes. For those financial institutions that assume a higher-risk AML/CFT profile, management should be required to provide a **more robust AML/CFT Compliance Program** that specifically monitors and controls the higher risks accepted by the management and board.

Consolidated AML/CFT Compliance Risk Assessment

Financial institutions that implement a consolidated or partially consolidated AML/CFT Compliance Program are required to **assess risk both individually within business lines and across all activities and legal entities**. Aggregating ML/FT risks on a consolidated basis for larger or more complex institutions may enable the organization to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the institution.

To avoid having an outdated understanding of the ML/FT risk exposures, the financial institution should be required to continually reassess its ML/FT risks and communicate with its business units, functions and legal entities. The identification of ML/FT risks or deficiency in one area of business may indicate concerns elsewhere in the institution. This therefore requires the management's attention to identify and control them.

Updating of Risk Assessment by Financial Institution

An effective AML/CFT Compliance Program must be able to control the risks associated with the institution's products, services, customers, entities and geographic locations. Therefore, an effective risk assessment is required to be an ongoing process, not a one-time exercise.

Management is required to update its risk assessment to identify changes in the financial institution's risk profile when it is necessary, especially **when new products and services are introduced, existing products and services change, higher-risk customers open and close accounts or the financial institution expands through mergers and acquisitions**.

In the absence of such changes and in the spirit of sound practice, financial institutions are required to periodically reassess their ML/FT risks at least every 12 to 18 months.

Development of ML/FT Risk Assessment by Bank Examiners

In some situations, financial institutions may not have performed or completed an adequate ML/FT risk assessment and it becomes necessary for the Bank Examiners to complete one based on available information. When doing so, the Examiners do not have to use any particular format. In such instances, **documented work-papers**

should include the financial institution's risk assessment, the deficiencies noted in the financial institution's risk assessment and the Examiner-prepared risk assessment. The Examiners should ensure that they have a general understanding of the financial institution's ML/FT risks and (at a minimum) document these risks within the examination scoping process.

This section provides some general guidance that Bank Examiners can use when they are required to conduct ML/FT risk assessment. In addition, Examiners may share this information with the financial institution to assist it develop or improve its own ML/FT risk assessment.

The risk assessment developed by Examiners generally will not be as comprehensive as one developed by a financial institution. Similar to what is expected in a financial institution's risk assessment, the Examiners are required to **obtain information on the financial institution's products, services, customers, entities and geographic locations to determine the volume and trend for potentially higher-risk areas. This process can begin with an analysis of:**

i. Prior examination or inspection reports and work-papers.
ii. Response to request letter-items.
iii. Discussions with financial institution management and the appropriate regulatory agency personnel.

The Examiners should complete the above analysis **by reviewing the level and trend of information pertaining to the institution's activities identified, for example:**

i. Funds transfers.
ii. Private banking.
iii. Monetary instrument sales.
iv. Foreign correspondent accounts and PTAs.
v. Branch locations.
vi. Domestic and international geographic locations of the institution's business area.

This information should be evaluated relative to such factors as the **financial institution's total asset size, customer base, entities, products, services and geographic locations.**

Examiners are required to exercise caution in comparing information between financial institutions and to use their experience and insight when performing this analysis:

i. Examiners should avoid comparing the number of STRs filed by a financial institution to those filed by another financial institution in the same geographic location.

ii. Examiners can and should use their knowledge of the risks associated with products, services, customers, entities and geographic locations to help them determine the institution's ML/FT risk profile.

iii. After **identifying the potential higher-risk operations**, Examiners should be able to form a preliminary ML/FT risk profile of the financial institution. The preliminary risk profile will provide the Examiner with the basis for the initial AML/CFT examination scope and the ability to determine the adequacy of the financial institution's AML/CFT Compliance Program.

Financial institution may have an appetite for higher-risk activities. These risks should, however, be appropriately mitigated by an effective AML/CFT Compliance Program tailored to those specific risks. The Examiner should develop an initial examination scoping and planning document commensurate with the preliminary ML/FT risk profile. As necessary, the Examiner should identify additional examination procedures beyond the minimum procedures that must be completed during the examination. While the initial scope may change during the examination, the preliminary risk profile will enable the Examiner to establish a reasonable scope for the AML/CFT review.

Determination of the Financial Institution's ML/FT

Aggregate Risk Profile by Bank Examiner

The Examiner, during the phase of "Developing Conclusions and Finalizing the Examination" of the AML/CFT examination, should assess whether the controls of the financial institution's AML/CFT Compliance Program are appropriate to manage and mitigate its ML/FT risks. Through this process, the Examiner should determine an aggregate risk profile for the financial institution. This aggregate risk profile should take into consideration the risk assessment developed either by the financial institution or by the Examiner and should factor in the adequacy of the AML/CFT Compliance Program.
Examiners should determine whether the financial institution's AML/CFT Compliance Program is adequate to appropriately mitigate the ML/FT risks based on the risk assessment. **The existence of ML/FT risk within the aggregate risk profile should not be criticized as long as the financial institution's AML/CFT Compliance Program adequately identifies, measures, monitors and controls this risk as part of a deliberate risk strategy.**
When the risks are not appropriately controlled, Examiners are required to communicate to management and the board of directors the need to mitigate ML/FT risk and should document deficiencies.
Examination Procedures of ML/FT Risk Assessment
Objective

Assess the ML/FT risk profile of the institution and evaluate the adequacy of its ML/FT risk assessment process

i. Review the financial institution's ML/FT risk assessment. Determine whether the institution has included all risk areas, including any new products, services or targeted customers, entities and geographic locations. Determine whether the

financial institution's process for periodically reviewing and updating its ML/FT risk assessment is adequate.

ii. If the financial institution has not developed a risk assessment or if the risk assessment is inadequate, the Examiner must complete a risk assessment.

iii. Examiners should document and discuss the financial institution's ML/FT risk profile and any identified deficiencies in the risk assessment process with the institution's management.

5. Overview of AML/CFT Compliance Program

Objective

Assess the adequacy of the financial institution's AML/CFT Compliance Program. Determine whether the financial institution has developed, administered and maintained an effective program for compliance with the MLPA and CBN AML/CFT Regulation, 2009.

The review of the financial institution's written policies, procedures and processes is a first step in determining the overall adequacy of the AML/CFT Compliance Program.

The completion of applicable core and (if warranted) expanded examination procedures is necessary to support the overall conclusions regarding the adequacy of the AML/CFT Compliance Program.

Examination findings should be discussed with the financial institution's management and significant findings are required to be included in the report of examination or supervisory correspondence. The AML/CFT Compliance Program must be in a written form, approved by the board of directors and noted in the board minutes.

An institution must have AML/CFT Compliance Program commensurate with its respective ML/FT risk profile.
Furthermore, the AML/CFT Compliance Program must be fully implemented and reasonably designed to meet the relevant AML/CFT laws and regulation's requirements.

Policy statements alone are not sufficient. Practices must coincide with the financial institution's written policies, procedures and processes.

Minimum requirements of AML/CFT Compliance Program

i. A system of internal controls to ensure on-going compliance.
ii. Independent testing of AML/CFT compliance.
iii. Designate an individual or individuals responsible for managing AML/CFT compliance (Chief compliance officer).
iv. Training for appropriate personnel.

Internal Controls

The board of directors, acting through senior management, is ultimately responsible for ensuring that the financial institution maintains an effective AML/CFT internal control structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the financial institution's AML/CFT policies, procedures and processes.

Internal controls are the institution's policies, procedures and processes designed to limit and control risks and to achieve compliance with the MPLA and CBN AML/CFT Regulation 2009.

The level of sophistication of the internal controls should be commensurate with the size, structure, risks and complexity of the financial institution. Large complex financial institutions are more likely to implement departmental internal controls for AML/CFT compliance.

Departmental 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 Program.

Internal controls should:

i. Identify financial institution's **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 Program that is tailored to manage risks.
ii. 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 action taken, and the directors and senior management should be notified of returns rendered to the regulatory authorities.
iii. **Identify a person or persons responsible for AML/CFT compliance.**
iv. Provide for **program continuity by way of back-up** in personnel and information storage & retrieval in cases of changes in management or employee composition or structure.
v. Provide for meeting all regulatory recordkeeping and reporting requirements, implement all recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.
vi. Cover the implementation of risk-based CDD policies, procedures and processes

vii. Identify reportable transactions and that all the required reports are accurately rendered promptly and these include STRs, PEPs, CTRs and CTR-exemptions (if any). Financial institutions are required to centralize their review and report-rendition functions within a unit in the branches and head-offices.
viii. Provide for dual controls and the segregation of duties as much possible. For example, employees that complete the reporting forms (such as STRs, CTRs and CTR-exemptions) generally should not also be responsible for taking the decision to file the reports or grant the exemptions.
ix. Provide sufficient controls and systems for rendering CTRs and CTR exemptions.
x. Provide sufficient controls and systems of monitoring timely detection and reporting of suspicious activity.
xi. 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, AML/CFT Regulation and other guidelines.
xii. Incorporate MLPA & AML/CFT Regulation-compliance into the job descriptions and performance evaluations of financial institution personnel, as appropriate.
xiii. Provide for the training of employees to be aware of their responsibilities under the AML/CFT Regulations and internal policy guidelines.

Independent Testing

Independent testing (audit) should be conducted by the internal audit department, external auditors, consultants or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, **a sound practice is for the financial institution to conduct independent testing generally every 12 to 18 months or commensurate with the ML/FT risk profile of the institution.**

Financial institutions that do not employ outside auditors, consultants or have internal audit departments **may comply with this requirement by using qualified persons who are not involved in the function that is tested**.

The persons conducting the AML/CFT testing should report directly to the board of directors or to a designated board committee consisting primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written AML/CFT Compliance Program should perform testing for specific compliance with the MLPA, AML/CFT Regulation 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 financial institution's operations, departments and subsidiaries.

Risk-based Audit Programs will vary depending 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 auditing program will **cover all of the institution's activities.** The frequency and depth of each audit activity will vary according to the activity's risk assessment.

It should be noted that the risk-based auditing will enable the board of directors and auditors to use the financial institution's risk assessment to **focus its scope of audit on the areas of greatest concern.** The testing should assist the board of directors and management in **identifying areas of weakness or areas where there is a need for enhancements or stronger controls**.

Independent testing should (at a minimum) include:

i. The evaluation of the overall adequacy and effectiveness of the AML/CFT Compliance Program, including policies, procedures and processes. This evaluation will contain an **explicit statement about the AML/CFT compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements.** At the very least, the audit should contain sufficient information for the reviewer (e.g. an Examiner, review auditor or NFIU officer) to reach a conclusion about the overall quality of the AML/CFT Compliance Program.
ii. A review of the financial institution's risk assessment for reasonableness given the institution's risk profile (products, services, customers, entities and geographic locations).
iii. Appropriate risk-based transaction testing to verify the financial institution's adherence to the MPLA and CBN AML/CFT Regulation, 2009 recordkeeping and rendition of returns requirements on PEPs, STRs, CTRs and CTR-exemptions and information sharing requests.
iv. 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).
v. A review of staff training for adequacy, accuracy and completeness.
vi. A review of the effectiveness of the suspicious transaction monitoring systems (are they manual, automated or a combination?) used for AML/CFT compliance. **Related reports may include, but are not limited to:**

a. Suspicious transaction monitoring reports.
b. Large currency aggregation reports.
c. Monetary instrument records.
d. Funds transfer records.
e. Non-sufficient funds (NSF) reports.
f. Large balance fluctuation reports.
g. Account relationship reports.
h. 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.

vii. An assessment of the integrity and accuracy of MIS used in the AML/CFT Compliance Program. MIS includes reports used to identify and extract data on the large currency transactions, aggregate daily currency transactions, funds-transfer transactions, monetary instrument sales transactions and analytical and trend reports.

The auditors' report 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 Examiner to review. Any violations, policy or procedures exceptions or other deficiencies noted during the audit should be included in the audit report and reported 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 and document the corrective actions recommended and taken.

Chief Compliance Officer

The institution's board of directors must designate a qualified individual that must not be less than a General Manager to serve as the Chief Compliance Officer (CCO). The CCO is responsible for the coordinating and monitoring of day-to-day AML/CFT compliance by the institution. The CCO is also charged with managing all aspects of the AML/CFT Compliance Program and with managing the institution's adherence to the MLPA, AML/CFT Regulation and other AML/CFT Requirements. However, it is the board of directors that is ultimately responsible for the institution's AML/CFT compliance.

As the title of the individual responsible for overall AML/CFT compliance is of importance, his/ her level of authority and responsibility within the financial institution is also critical. Though the CCO may delegate the AML/CFT duties to other employees, he/she will be held responsible for the overall AML/CFT compliance by the institution. The board of directors is responsible for ensuring that the CCO has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CFT Compliance Program based on the institution's risk profile.

The CCO should be fully knowledgeable of the MLPA, AML/CFT Regulation and all related requirements. The CCO should also understand the institution's products, services, customers, entities, geographic locations and the potential money laundering and terrorist financing risks associated with these activities. The appointment of a CCO is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority or time to satisfactorily carry out the job efficiently and effectively.
Confirm that the line of communication allows the CCO to regularly apprise the board of directors and senior management of ongoing compliance with AML/CFT regime of the institution. Ensure that pertinent MLPA-related information, including the reporting of STRs rendered to NFIU are reported to the board of directors or an appropriate board committee so that these individuals can make informed decisions about the overall

AML/CFT compliance of the institution. Ensure also that the CCO is responsible for carrying out the directives of the board and ensuring that employees adhere to the institution's AML/CFT policies, procedures and processes.

Training

Financial institutions are required to ensure that appropriate personnel are trained in applicable aspects of the MLPA & AML/CFT Regulation. The training should cover the **regulatory requirements and the institution's internal AML/CFT policies, procedures and processes.**

At a minimum, the financial institution's training program must provide training for all personnel whose duties require knowledge of the MPLA & AML/CFT Regulation. The training should be tailored to the person's specific responsibilities. In addition, an overview of the AML/CFT requirements typically should be given to new staff during employee orientation. Training should encompass information related to **applicable business lines such as trust services, international and private banking.**

The CCO should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall ML/FT risk profile of the institution.

The board of directors and senior management should be informed of changes and new developments in the MLPA and AML/CFT Regulation, other guidelines and directives, and regulations by other agencies. While the board of directors may not require the same degree of training as the institution operations personnel, they need to understand the importance of AML/CFT regulatory requirements, the ramifications of non-compliance and the risks posed to the institution. Without a general understanding of the MLPA & AML/CFT Regulation, the board of directors cannot adequately provide AML/CFT oversight, approve AML/CFT policies, procedures and processes or provide sufficient AML/CFT resources.

Training should be on-going and incorporate current developments and changes to the MLPA, AML/CFT Regulation and other related guidelines. Changes to internal policies, procedures, processes and monitoring systems should also be covered during training. The training program should reinforce the importance that the board and senior management place on the institution's compliance with the MLPA & AML/CFT Regulation and ensure that all employees understand their roles in maintaining an effective AML/CFT Compliance Program.

Examples of money laundering activity and suspicious transaction monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious transactions while training for the loan department should provide examples involving money laundering through lending arrangements.

Financial institutions are required to document their training programs. Training and testing materials, the dates of training sessions and attendance records should be maintained by the institution and be made available for the Bank Examiner to review.

6. EXAMINATION PROCEDURES OF AML/CFT COMPLIANCE PROGRAM

Objective

Assess the adequacy of the financial institution's AML/CFT Compliance Program. Determine whether the institution has developed, administered and maintained an effective program for compliance with the MLPA, AML/CFT Regulation & all other related Requirements.

1. Review the financial institution's **board approved- written AML/CFT Compliance Program** to ensure it contains the following required elements:

    i. A system of internal controls that ensures on-going compliance.

    ii. Independent testing of MLPA, AML/CFT Regulation and related guidelines for compliance.

    iii. A specifically designated person or persons responsible for managing MPLA and related regulations compliance (Chief Compliance Officer).

    iv. Training for appropriate personnel.

    v. Financial institutions are required to have AML/CFT Compliance Programs which are commensurate with their respective ML/FT risk profiles. A customer identification program (CIP) must also be included as part of the AML/CFT Compliance Program.

2. Assess whether or not the board of directors and senior management receive adequate reports on AML/CFT compliance.

Risk Assessment in AML/CFT Compliance Program

3. On the basis of examination procedures completed in the scoping and planning process, including the review of the risk assessment, **determine whether the financial institution has adequately identified the risk within its operations** (products, services, customers, entities and geographic locations) and **incorporated the risk into its AML/CFT Compliance Program.**

Internal Controls

4. Determine whether the AML/CFT Compliance Program includes policies, procedures and processes that:

i. Identify **higher-risk operations** (products, services, customers, entities and geographic locations); provide for **periodic updates** to the institution's risk profile and AML/CFT Compliance Program **tailored to manage risks.**
ii. Inform the board of directors or its committee and senior management of compliance initiatives, identified compliance deficiencies, STRs rendered and corrective action taken.
iii. Identify a person or persons responsible for AML/CFT compliance.
iv. Provide for program-continuity (in the form of back-up, storage & retrieval of information) despite changes in management or employee composition or structure.
v. Meet all regulatory requirements, enforce the recommendations for AML/CFT compliance and provide for timely updates to implement changes in regulations.
vi. Implement risk-based CDD policies, procedures and processes.
vii. Identify reportable transactions and accurately render promptly all the required returns including STRs, PEPs, CTRs and CTR-exemptions (where necessary). Ensure that the financial institution has centralized its review and return rendition functions within a unit/office at the branches & head office.
viii. Provide for dual controls and the segregation of duties as much as possible. For example, employees that complete the return formats (such as STRs, PEPs, CTRs and CTR-exemptions) generally should not also be responsible for the decision to render the reports or grant the exemptions.
ix. Provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious transaction.
x. Provide for adequate supervision of employees that handle currency transactions, complete reports & render the returns, grant exemptions, monitor for suspicious activity or engage in any other activity covered by the MLPA, AML/CFT Regulation and other related requirements.
xi. Train employees to be aware of their responsibilities under the MLPA, AML/CFT Regulation, other related and internal policy guidelines.
xii. Incorporate MLPA & AML/CFT Regulation compliance into job descriptions and performance evaluations of appropriate personnel.

Independent Testing

5. Determine whether the AML/CFT testing (audit) is independent (i.e. performed by a person (or persons) not involved with the institution's AML/CFT compliance) and whether persons conducting the testing report directly to the board of directors or to a designated board committee consisting primarily or completely of outside directors.

6. Evaluate the qualifications of the person (or persons) performing the independent testing to assess whether the financial institution can rely upon the findings and conclusions.

7. Validate the auditor's reports and work-papers to determine whether the financial institution's independent testing is comprehensive, accurate, adequate and timely. The independent test should address the following:

    i. The overall adequacy and effectiveness of the AML/CFT Compliance Program including policies, procedures and processes. The evaluation will include an explicit statement about the AML/CFT Compliance Program's overall adequacy and effectiveness and compliance with applicable regulatory requirements. At the very least, the audit should contain sufficient information for the reviewer (e.g. the Examiner, review auditor) to reach a conclusion about the overall quality of the AML/CFT Compliance Program.

    ii. ML/FT risk assessment.
    iii. MLPA & AML/CFT Regulation reporting and record-keeping requirements.
    iv. CIP implementation.
    v. CDD policies, procedures and processes and whether they comply with internal requirements.
    vi. Personnel adherence to the institution's AML/CFT policies, procedures and processes.
    vii. Appropriate transaction testing with particular emphasis on higher-risk operations (products, services, customers and geographic locations).
    viii. Training, including its comprehensiveness, accuracy of materials, the training schedule and attendance tracking.
    ix. The integrity and accuracy of MIS used in the AML/CFT Compliance Program. MIS includes reports used to identify large currency transactions, aggregate daily currency transactions, funds transfer transactions, monetary instrument sales transactions, and analytical and trend reports.
    x. Tracking of previously identified issues and deficiencies and verification that they have been corrected by management.
    xi. If an automated system is not used to identify or aggregate large transactions, determine whether the audit or independent review includes a sample test check of tellers' cash proof sheets, tapes or other documentation to determine whether large currency transactions are accurately identified and reported.

8. Determine whether the audit's review of suspicious transaction monitoring systems includes an evaluation of the system's ability to identify un-usual transaction. Ensure through a validation of the auditor's reports and work-papers that the institution's independent testing:

    i. Reviews policies, procedures and processes for suspicious transaction monitoring.
    ii. Evaluates the system's methodology for establishing and applying expected activity or filtering criteria.
    iii. Evaluates the system's ability to generate monitoring reports.
    iv. Determines whether the system filtering criteria are reasonable and include (at a minimum) cash, monetary instruments, funds transfers and

other higher-risk products, services, customers or geographies as appropriate.

9. Determine whether the audit's review of suspicious transaction reporting systems includes an evaluation of the research and referral of un-usual transaction. Ensure through a validation of the auditor's reports and work-papers that the institution's independent testing includes a review of policies, procedures and processes for referring un-usual transaction from all business lines (e.g. legal, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.
10. Review the audit scope, procedures and work-papers to determine adequacy of the audit based on the following:

    i. Overall audit coverage and frequency in relation to the risk profile of the institution.
    ii. Board reporting & supervision and its responsiveness to audit findings.
    iii. Adequacy of transaction testing, particularly for higher-risk operations and suspicious transaction monitoring systems.
    iv. Competency of the auditors or independent reviewers regarding AML/CFT requirements.

Chief Compliance Officer

11. Determine whether the board of directors has designated a person or persons responsible for the overall AML/CFT Compliance Program. Determine whether the CCO has the necessary authority and resources to effectively execute all the duties assigned to him as the CCO.
12. Assess the competency of the CCO and his/her staff. Determine whether the AML/CFT compliance area is sufficiently staffed for the institution's overall risk level based on products, services, customers, entities and geographic locations, size and compliance needs. In addition, ensure that no conflict of interest exists and that staff is given adequate time to execute all duties.

Training

13. Determine whether the following elements are adequately addressed in the training program and materials:

    i. The importance the board of directors and senior management place on on-going education, training and compliance.
    ii. Employees' accountability for ensuring compliance with MLPA & AMLCFT Regulation and related requirements.
    iii. Comprehensiveness of the training, considering the specific risks of individual business lines.
    iv. Training of personnel from all applicable areas of the financial institution.
    v. Frequency of training.
    vi. Documentation of attendance records and training materials.

vii. Coverage of the institution's policies, procedures, processes and new rules and regulations.
viii. Coverage of different forms of money laundering and terrorist financing as it relates to identification and examples of suspicious transaction.
ix. Penalties for non-compliance with internal policies and regulatory requirements.

Transaction Testing

Transaction testing must include (at a minimum) either examination procedures detailed below (independent testing) or transaction testing procedures selected from within the core or expanded sections. While there are many ways of conducting transaction testing, the Examiners have the discretion to decide what testing to conduct.

Examiners should document their decision regarding the extent of transaction testing to conduct and the transactions to be performed, as well as the rationale for any changes to the scope of transaction testing that occur during the examination. **Examiners should consider the following when determining how to proceed with transaction testing:**

i. Accounts or customers identified in the review of information obtained from returns rendered to the CBN.
ii. Higher-risk products and services, customer and entities, and geographic locations for which it appears from the scoping and planning process that the institution may not have appropriate internal controls.
iii. New products and services, customers and entities, and geographies introduced into the bank's portfolio since the previous AML/CFT examination.

Independent Testing

14. Select a judgmental sample that includes transactions other than those tested by the independent auditor and determine whether the independent testing carried out:

i. Is comprehensive, adequate and timely.
ii. Has reviewed the accuracy of MIS used in the AML/CFT Compliance Program.
iii. Has reviewed suspicious transaction monitoring systems to include the identification of un-usual transaction.
iv. Has reviewed whether suspicious transaction reporting systems include the research and referral of un-usual transaction.

Preliminary Evaluation

After the Bank Examiner has completed the review of all the four required elements of the institution's AML/CFT Compliance Program, the Examiner is required to document a preliminary evaluation of the institution's program.

At this point, the Examiner should revisit the initial examination plan, in order to determine whether any strengths or weaknesses identified during the review of the institution's AML/CFT Compliance Program warrant adjustments to the initial planned scope.

The Examiner should document and support any changes to the examination scope, then proceed to the applicable core and (if warranted) expanded examination procedures.

If there are no changes to the examination scope, the Examiner should proceed to the core examination procedures of "Developing Conclusions and Finalizing the Examination".

7. OVERVIEW OF HOW TO DEVELOP CONCLUSIONS AND FINALIZE AML/CFT EXAMINATION

Objective

Formulate conclusions, communicate findings to management, prepare report & comments, develop an appropriate supervisory response and close the examination.

In the final phase of the AML/CFT examination, the Examiner is required to assemble all findings from the examination procedures completed. From those findings, the Examiner should develop and document conclusions about the AML/CFT compliance program's adequacy, discuss preliminary conclusions with the institution management, present these conclusions in a written form for inclusion in the examination report. He is also required to determine and document the regulatory response (if any).

The appropriate regulatory response will include the citation of regulatory violations. The citation of violations of law and regulation is typically done in the context of supervisory activities. The extent to which violations affect the evaluation of an institution's AML/CFT Compliance Program is based on the nature, duration and severity of non-compliance. In some cases, the Bank Examiner may allow the institution to remedy the violation as part of the supervisory process. In appropriate circumstances, the Examiner may take either informal or formal enforcement actions to address violations of the MLPA & AML/CFT Regulation.

Systemic or Recurring Violations

Systemic or recurring violations of the MLPA and AML/CFT Regulation may involve either a substantial number of deficiencies or a repeated failure to effectively and accurately record and report information as required under the law & regulation.
The violation may be in the form of errors or incompleteness that can impair the integrity of the record or report, failure to adequately represent the transactions

required to be reported or impact on the effectiveness of the institution's suspicious transaction-monitoring and reporting-processes.

Systemic violations may be as the result of ineffective systems/controls meant to obtain, analyze and maintain required information or to render returns on customers, accounts or transactions as required under various provisions of the MLPA, AML/CFT Regulation and other related guidelines.

Recurring violations are repetitive occurrences of the same or similar issues. Unlike isolated or inadvertent issues, systemic or recurring issues demonstrate a pattern or practice of non-compliance with the MLPA, AML/CFT Regulation and other related guidelines.

When evaluating whether violations represent a pattern or practice, Examiners are required to analyze the pertinent facts and circumstances. Repeated, regular, usual or institutionalized practices will typically constitute a pattern or practice. The totality of the circumstances must be considered when assessing whether a pattern or practice exists.

Considerations in determining whether a pattern or practice exists

i. Whether the number of violations is high when compared with the institution's total transaction.
   This evaluation usually is determined through a sampling of transactions or records. Based on this process, determinations are made concerning the overall level of non-compliance. Even if the violations are few in number, they could reflect systemic non-compliance, depending on the severity, significant or egregious.
ii. Whether there is evidence of similar violations by the institution in a series of transactions or in different divisions or departments.
   This is not an exact calculation. The Examiners should balance the number, significance and frequency of violations identified throughout the organization. Violations identified within various divisions or departments may or may not indicate a systemic violation. These violations should be evaluated in a broader context to determine if there is presence of weakness in training or other compliance system.
iii. The relationship of the violations to one another.
   Determine whether they all occurred in the same area in the financial institution, in the same product-line, in the same branch or department or with one employee.
iv. The impact that the violation or violations have on the institution's suspicious transaction monitoring and reporting capabilities.
v. Whether the violations appear to be grounded in a written, unwritten policy, established procedure or result from a lack of an established procedure.
vi. Whether there is a common source or cause of the violations.
vii. Whether the violations were the result of an isolated software problem in a AML/CFT reporting software product and whether the institution has taken appropriate steps to address the issue.

Systemic or recurring violations of the MLPA, AML/CFT Regulation and other related guidelines could have a significant impact on the adequacy of the institution's AML/CFT Compliance Program. When systemic instances of non-compliance are identified, the Examiner should consider the non-compliance in the context of the overall program of internal controls, training, independent testing, responsible person and determine whether the institution's AML/CFT Compliance Program is deficient as a result of the systemic non-compliance.

All systemic violations should be brought to the attention of the institution's board of directors and management and be documented in the examination report or supervisory correspondence.

Types of systemic or recurring violations

i. Failure to establish a due diligence program that includes a risk-based approach, and when necessary, enhanced policies, procedures and controls concerning foreign correspondent accounts.
ii. Frequent, consistent or recurring late rendition of CTR, STR & PEPs.
iii. A significant number of CTRs, STRs & PEPs with errors or omissions of data elements.
iv. Consistently failing to obtain or verify required customer identification information at account opening.
v. Failure to consistently maintain or retain records as required by the MPLA, AML/CFT Regulation and other related guidelines.

Isolated or Technical Violations

Isolated or technical violations are limited instances of non-compliance with the MLPA & AML/CFT Regulation that occur within an otherwise adequate system of policies, procedures and processes. These violations generally do not prompt serious regulatory concern or reflect negatively on management's supervision or commitment to MLPA & AML/CFT Regulation compliance, unless the isolated violation represents a significant or egregious situation or is accompanied by evidence of bad faith.
Multiple isolated violations throughout the departments or divisions in the institution can be indicative of systemic or recurring system weaknesses or violations.

Corrective action for isolated violations is usually undertaken by the institution's management within the normal course of business.

All violations (regardless of type or significance) must be brought to the attention of the institution's management and be documented appropriately.

Types of isolated or technical violations

i. Failure to render or late-filing of CTRs, STRs & PEPs that is infrequent, not consistent or nonrecurring.
ii. Failure to obtain complete customer identification information on a monetary instrument sale-transaction that is isolated and infrequent.

iii. Infrequent, not consistent, non-recurring incomplete or inaccurate information in STR, PEPs & CTRs data fields.
iv. Failure to obtain or verify required customer identification information that is infrequent, not consistent or non-recurring.

In formulating a written conclusion, the Examiner does not need to discuss every procedure performed during the examination. During exit-discussions with management on examination conclusions, Examiners should include discussions on both the strengths and weaknesses of the institution's AML/CFT Compliance. Examiners are required to document all the relevant determinations and conclusions.

8. EXAMINATION PROCEDURES OF HOW TO DEVELOP CONCLUSIONS AND FINALIZE AML/CFT EXAMINATION

Objective

Formulate conclusions, communicate findings to management, prepare report & comments, develop an appropriate supervisory response and close the examination.

Formulating Conclusions

1. Accumulate all pertinent findings from the AML/CFT examination procedures performed. Evaluate the thoroughness and reliability of any risk assessment conducted by the institution. **Reach a preliminary conclusion as to whether the following requirements are met:**

    i. The AML/CFT Compliance Program is effectively monitored and supervised in relation to the institution's risk profile as determined by the risk assessment. The Examiner should ascertain if the AML/CFT Compliance Program is effective in mitigating the institution's overall risk.
    ii. The board of directors and senior management are aware of AML/CFT regulatory requirements, effectively oversee AML/CFT compliance and are committed to (as necessary) corrective actions in respect of audit and regulatory examination recommendations.
    iii. AML/CFT policies, procedures and processes are adequate to ensure compliance with applicable laws and regulations and appropriately address higher-risk operations in products, services, customers, entities and geographic locations.
    iv. Internal controls ensure compliance with the MLPA & AML/CFT Regulation and provide sufficient risk management, especially for higher-risk operations in products, services, customers, entities and geographic locations.
    v. Independent testing (audit) is appropriate and adequately tested for compliance with required laws, regulations and policies. Overall audit coverage and frequency are appropriate in relation to the risk profile of the institution. Transaction testing is adequate, particularly for higher-risk operations and suspicious transaction monitoring systems.

vi. The designated person responsible for coordinating and monitoring day-to-day compliance is competent and has the necessary resources.
vii. Personnel are sufficiently trained to adhere to legal, regulatory and policy requirements.
viii. Information and communication policies, procedures and processes are adequate and accurate.

Relevant determinations to be documented and explained.

Determine the Underlying Cause

2. Determine the underlying cause of policy, procedure or process deficiencies (if identified). **These deficiencies can be as a result of a number of factors, including but not limited to the following:**

i. Management has not assessed or has not accurately assessed the financial institution's AML/CFT risks.
ii. Management is unaware of the relevant issues.
iii. Management is unwilling to create or enhance policies, procedures and processes.
iv. Management or employees disregard established policies, procedures and processes.
v. Management or employees are unaware of or misunderstand the regulatory requirements, policies, procedures or processes.
vi. Higher-risk operations in products, services, customers, entities and geographic locations have grown faster than the capabilities of the AML/CFT Compliance Program.
vii. Changes in internal policies, procedures and processes are poorly communicated.

3. Determine whether deficiencies or violations were previously identified by management, audit or were only identified as a result of this examination.

Discuss findings with Examiner in charge and identify necessary action

4. Discuss preliminary findings with the Examiner in charge (EIC) or Examiner responsible for reviewing the institution's overall AML/CFT compliance. **The Examiner should document his work-papers appropriately with the following information:**

i. A conclusion regarding the adequacy of the AML/CFT Compliance Program and whether it meets all the regulatory requirements by providing the following:

a. A system of internal controls.
b. Independent testing for compliance.

c. A specific person to coordinate and monitor the AML/CFT Compliance Program.
d. Training of appropriate personnel.

ii. Conclusion as to whether the written CIP is appropriate for the institution's size, location and type of business.

iii. Any identified violations and assessment of the severity of those violations.

iv. Identification of actions needed to correct deficiencies or violations and (as appropriate) the possibility of, among other things, requiring the institution to conduct more detailed risk assessments or take formal enforcement action.

v. Recommendations for supervisory actions. Issues to confer with the institution's supervisory management and its legal staff.

vi. An appropriate rating based on overall findings and conclusions.

vii. Findings that have been or will be discussed with institution management and, if applicable, any institution commitment for improvements or corrective action.

Preparing the AML/CFT comments for the Examination report

5. Document your conclusion regarding the adequacy of the institution's AML/CFT Compliance Program. Discuss the effectiveness of each of these elements of the institution's AML/CFT Compliance Program. Indicate whether the AML/CFT Compliance Program meets all the regulatory requirements by providing the following:

i. A system of internal controls.
ii. Independent testing for compliance.
iii. A specific person to coordinate and monitor the AML/CFT Compliance Program.
iv. Training of appropriate personnel.

The AML/CFT Compliance Program must also include a written Customer Identification Program (CIP) appropriate for the institution's size, location and type of business.

The Examiner does not need to provide a written comment on every one of the following items 6 through 10. Written comments should cover only areas or subjects pertinent to the Examiner's findings and conclusions. All significant findings must be included in the examination report. The Examiner should ensure that work-papers are prepared in sufficient detail to support issues to be included in the examination report.

To this extent, there are items included in the work-papers for discussion that may not be in the examination report. Bank Examiner should ensure that his work-papers thoroughly and adequately document each review, as well as any other aspects of the

institution's AML/CFT Compliance Program that merits attention though they may not rise to the level of being included in the examination report. The Examiner should organize and reference his work-papers and document conclusions and supporting information within the internal databases, as appropriate.

Items for Examiners to discuss

6. To describe the board of directors' and senior management's commitment to AML/CFT compliance, consider whether management has the following:
   i. A strong AML/CFT Compliance Program that is fully supported by the board of directors; and
   ii. A requirement that the board of directors and senior management must be kept informed of AML/CFT compliance efforts, audit reports, compliance failures and the status of corrective actions.

7. Describe whether the institution's policies, procedures and processes for STR, CTRs & PEPs filings meet the regulatory requirements and are effective.
8. If applicable, describe whether the institution's policies, procedures and processes for CTR- exemptions meet regulatory reporting requirements, appropriately grant exemptions and use the correct forms.
9. Briefly discuss whether the policies, procedures and processes include effective internal controls on separation of duties, proper authorization for sending and receiving and posting to accounts, and provide a means to monitor transfers for CTR reporting purposes.
10. Describe the financial institution's record-keeping policies, procedures and processes. Indicate whether they meet the requirements of MLPA & AML/CFT Regulation.

C. OVERVIEW OF CORE EXAMINATION PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS

9. Overview of Customer Identification Program

Objective

Assess the financial institution's compliance with the statutory and regulatory requirements for the Customer Identification Program (CIP).

All financial institutions must have a written CIP. Each financial institution should **implement a written CIP** that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the

institution's AML/CFT Compliance Program which is subject to approval by the institution's board of directors.

The implementation of a CIP by the financial institution's subsidiaries is appropriate as a matter of safety, soundness and protection from reputational risks. Domestic subsidiaries (other than functionally regulated subsidiaries that are subject to separate CIP rules) of financial institutions should comply with the CIP rule that applies to the parent institution when opening an account.

The CIP is intended to enable the financial institution to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer.

Each financial institution is required to conduct a risk assessment of its customer base and product offerings. To determine the risks involved it must consider:

i. The types of accounts offered by it.
ii. The institution's methods of opening accounts.
iii. The types of identification information available.
iv. The institution's size, location and customer base, including types of products and services used by the customers in different geographic locations.

Pursuant to the CIP rule, an "account" is a formal banking relationship to provide or engage in services, dealings or other financial transactions. It includes a deposit account, a transaction or asset account, a credit account, or another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian or trust services.

An account does not include:

i. Products or services for which a formal banking relationship is not established with a person, such as cheque-cashing, funds transfer or the sale of a cheque or money order.
ii. Any account that the institution acquires. This may include single or multiple accounts as a result of a purchase of assets, acquisition, merger or assumption of liabilities.
iii. Accounts opened to participate in an employee benefit plan established under the Employee Retirement Scheme.

The CIP rule applies to a "customer." A customer is a "person" (an individual, a corporation, partnership, a trust, an estate or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club).

A customer does not include a person who does not receive banking services, such as a person whose loan application is denied. The definition of "customer" also include an existing customer as long as the bank has a reasonable belief that it knows the customer's true identity.

Customer Information Required

The CIP must contain account-opening procedures detailing the identification information that must be obtained from each customer. At a minimum, the financial institution **must obtain the following identification information from each customer before opening the account:**

i. Name.
ii. Date of birth for individuals.
iii. Address.
iv. Identification number such as Tax Identification Number (TIN), National Identity Card Number (NIN), Voter Card Registration Number, International Passport Number, Certificate of Incorporation Number (for legal person).

Based on its risk assessment, a financial institution may obtain additional identification information besides the above items for certain customers or product lines, referring to the appropriate sections of the AML/CFT Regulation, 2009.

Customer Verification

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. A financial institution need not establish the accuracy of every element of identification information obtained. It must however verify enough information to form a reasonable belief that it knows the true identity of the customer. The institution's procedures must describe when it will use documents, non documentary methods or a combination of both.

Verification through Documents

A financial institution using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation. The identification **must provide evidence of a customer's nationality or residence and bear a photograph or similar safeguard. E**xamples include a driver's licence or international passport. However, other forms of identification may be used if they enable the institution to form a reasonable belief that it knows the true identity of the customer. Nonetheless, given the availability of counterfeit and fraudulently obtained documents, a financial institution is encouraged to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.
For a "person" other than an individual (such as a corporation, partnership or trust), the institution should obtain documents showing the legal existence of the entity. Such

documents include certified Memorandum & Articles (Memart) of Association of the incorporation, an un-expired government-issued business licence, a partnership agreement or a trust instrument.

Verification through Non-documentary Methods

Financial institutions are not advised to use non-documentary methods to verify a customer's identity. However, a financial institution using non-documentary methods to verify a customer's identity must have procedures that set forth the methods to be used by the institution.

Non-documentary methods may include contacting a customer, independently in order to verify the customer's identity through comparison of information provided by the customer with information obtained from a consumer regulatory agency, public database or other sources such as checking references with other financial institutions and obtaining a financial statement.

The bank's non-documentary procedures must also address the following situations: An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the financial institution is not familiar with the documents presented; the account is opened without obtaining documents (e.g. the institution obtains the required information from the customer with the intent to verify it); the customer opens the account without appearing in person; or the institution is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

Additional Verification for Certain Customers

The CIP must address situations where, based on its risk assessment of a new account opened by a customer that is not an individual, the financial institution will obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity. This verification method applies only when the financial institution cannot verify the customer's true identity using documentary or non-documentary methods.

For example, a financial institution may need to obtain information about and verify the identity of a sole proprietor or the principals in a partnership when the financial institution cannot otherwise satisfactorily identify the sole proprietorship or the partnership.

Lack of Verification

The CIP must also have procedures for circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of the customer. **These procedures should describe:**

i. Circumstances in which the financial institution should not open an account.

ii. The terms under which a customer may operate an account while the financial institution attempts to verify the customer's identity.
iii. When the financial institution should close an account, after attempts to verify a customer's identity have failed.
iv. When the financial institution should file a STR in accordance with applicable law and regulation.

Record-keeping and Retention Requirements

A financial institution's CIP must include record-keeping procedures. At a minimum, the institution must retain the identification information such as name, address, date of birth for an individual, tax identification number (TIN) and any other information required by the CIP which are obtained at account opening for a period of five years after the account is closed. For credit cards, the retention period is also five years after the account closes or becomes dormant.

The financial institution must also keep a description of the following for five years after the record was made:

i. Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance and the date of issuance and expiration date (if any).
ii. The method and the results of any measures undertaken to verify identity.
iii. The results of any substantive discrepancy discovered when verifying the identity.

Comparison with Terrorist Lists

The CIP must include procedures for determining whether existing or potential customer appears on any list of known or suspected terrorists or terrorist organizations. As often as possible and in accordance with the requirements of the AML/CFT Regulation and other related requirements on the subject, financial institutions are required to compare customer names against the list of terrorists after the account opening procedure is completed.

Adequate Customer Notice

The CIP must include procedures and evidence in which the financial institution has provided customers with adequate notice for request of information to verify their identities. The notice must generally describe the financial institution's identification requirements and this should be provided in a manner that is reasonably designed to allow a customer to view it or otherwise receive the notice before the account is opened. **Examples include posting the notice in the lobby, on a Web site or within loan application documents. Sample of such notice is provided below:**

10. IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, the law and regulation require all financial institutions to obtain, verify and record information that identifies each person who opens an account. What this means is that when you open an account, we will ask for your name, address, date of birth and other information that will allow us identify you. We may also ask to see your driver's licence, international passport, TIN, National Identity Card, Voter Registration Card or other identifying documents.

Reliance on another Financial Institution

A financial institution is permitted to rely on another financial institution (including an affiliate) to perform some or all of the elements of the CIP. If such reliance is addressed in the CIP, the following criteria must be met:

i. The relied-upon financial institution must be subject to a rule that makes it mandatory to implement the AML program requirements.
ii. The customer has an account or is opening an account at the institution and at the other functionally regulated institution.
iii. Such reliance must be reasonable under the circumstances.
iv. The financial institution must enter into a contract, requiring the other financial institution to certify annually to the beneficiary financial institution that the agent-institution has implemented its own AML Program and that it will perform (or its agent will perform) the specified requirements of the institution's CIP.

Use of Third Parties

The CIP rule does not alter a financial institution's authority to use a third party such as an agent or service provider to perform services on its behalf. Therefore, a financial institution is permitted to arrange for a third party such as a Car Dealer or Mortgage Broker to act as its agent in connection with a loan for purpose of verifying the identity of its customer. The financial institution can also arrange for a third party to maintain its records. As with any other responsibility performed by a third party, the financial institution is ultimately responsible for that third party's compliance with the requirements of its CIP. As a result, financial institution should establish adequate controls and review procedures for such relationships.

Other Legal Requirements

Nothing in the CIP rule relieves a financial institution of its obligations under any provision of the MLPA, AML/CFT Regulation, other laws, rules and regulations,

particularly with respect to provisions concerning information that must be obtained, verified or maintained in connection with any account or transaction.

11. EXAMINATION PROCEDURES OF CUSTOMER IDENTIFICATION PROGRAM

Objective

Assess the financial institution's compliance with the statutory and regulatory requirements in respect of the Customer Identification Program (CIP).

Verify that the financial institution's policies, procedures and processes include a comprehensive program for identifying customers.

The written program must be included within the financial institution's AML/CFT Compliance Program. It must include (at a minimum) policies, procedures and processes for the following:

i. Identification of information required to be obtained, including name, address, TIN and date of birth for individuals and risk-based identity verification procedures (including procedures that address situations in which verification cannot be performed).
ii. Procedures for complying with recordkeeping requirements.
iii. Procedures for checking new accounts against prescribed terrorist lists.
iv. Procedures for providing adequate customer notice.
v. Procedures covering the financial institution's reliance on another financial institution or a third party, if applicable.
vi. Procedures for determining whether and when a STR should be filed.

Determine whether the institution's CIP considers the types of accounts offered, methods of account opening and the institution's size, location and customer base.
Determine whether the institution's policy for opening new accounts for existing customers appears reasonable.

Review board minutes and verify that the board of directors approved the CIP, either separately or as part of the AML/CFT Compliance Program.

Evaluate the institution's audit and training programs to ensure that the CIP is adequately incorporated.

Evaluate the institution's policies, procedures and processes for verifying that all new accounts are checked against prescribed lists of suspected terrorists or terrorist organizations on a timely basis.

Transaction Testing

7. On the basis of a risk assessment, prior examination reports and review of the financial institution's audit findings, select a sample of new accounts opened since the most recent AML/CFT examination and review for compliance with the financial institution's CIP. The sample should include a cross-section of accounts of consumers and businesses, loans & deposits, credit card relationships and internet accounts. **The sample should also include the following:**

    i. Accounts opened for a customer that provides an application for a TIN or accounts opened with incomplete verification procedures.
    ii. New accounts opened using documentary methods and new accounts opened using non-documentary methods.
    iii. Accounts identified as higher risk.
    iv. Accounts opened by existing higher-risk customers.
    v. Accounts opened with exceptions.
    vi. Accounts opened by a third party (e.g. indirect loans).

8. From the previous sample of new accounts, determine whether the institution has:

    i. Opened the account in accordance with the requirements of the CIP.
    ii. Formed a reasonable belief as to the true identity of a customer, including a higher-risk customer. The financial institution should already have a reasonable belief as to the identity of an existing customer.
    iii. Obtained from each customer, before opening the account, the identity information required by the CIP such as name, date of birth, address and identification number.
    iv. Within a reasonable time after account opening, verified enough of the customer's identity information to form a reasonable belief as to the customer's true identity.
    v. Appropriately resolved situations in which customer identity could not be reasonably established.
    vi. Maintained a record of the identity information required by the CIP, the method used to verify identity and verification results (including results of discrepancies).
    vii. Compared the customer's name against the list of known or suspected terrorists or terrorist organizations.
    viii. Filed STRs, as appropriate.

9. Evaluate the level of CIP exceptions to determine whether the financial institution is effectively implementing its CIP. A financial institution's policy may not allow staff to make or approve CIP exceptions. However, a financial institution may exclude isolated, non-systemic errors (such as an insignificant number of data entry errors) from CIP requirements without compromising the effectiveness of its CIP.

10 On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit, select a sample of relationships with third parties that the financial institution relies on to perform its CIP (or portions of its CIP), if applicable. If the financial institution is using the "reliance provision":

Review the contract between the parties, annual certifications and other information such as the third party's CIP.

Determine whether reliance is reasonable. The contract and certification will provide a standard means for a financial institution to demonstrate that it has satisfied the "reliance provision," unless the Examiner has reason to believe that the financial institution's reliance is not reasonable, based on the fact that, for example, the third party has been subject to an enforcement action for AML/CFT deficiencies or violations.

11. If the financial institution is using an agent or service provider to perform elements of its CIP, determine whether the financial institution has established appropriate internal controls and review procedures to ensure that its CIP is being implemented for third-party agent or service-provider relationships (e.g., car dealerships).
12. Review the adequacy of the financial institution's customer notice and the timing of the notice's delivery.
13. Evaluate the financial institution's CIP record retention policy and ensure that it corresponds to the regulatory requirements to maintain certain records. The financial institution must retain the identity information obtained at account opening for five years after the account closes. It must also maintain a description of documents relied on, methods used to verify identity and resolution of discrepancies for five years after the record is made.
14. On the basis of examination procedures conducted including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with CIP.

12. OVERVIEW OF CUSTOMER DUE DILIGENCE

Objective

Assess the appropriateness and comprehensiveness of the financial institution's customer due diligence (CDD) policies, procedures and processes for obtaining customer information and assess the value of this information in detecting, monitoring and reporting suspicious transaction.
The cornerstone of a strong AML/CFT Compliance Program is the adoption and implementation of comprehensive CDD policies, procedures and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing.

The objective of CDD is to enable the financial institution predict with relative certainty the types of transactions in which a customer is likely to engage. These processes assist

the financial institution in determining when transactions are potentially suspicious. The concept of CDD begins with verifying the customer's identity and assessing the risks associated with that customer. Processes should also include enhanced CDD for higher-risk customers and ongoing due diligence of the customer base.

Effective CDD policies, procedures and processes provide the critical framework that enables the financial institution to comply with regulatory requirements and to report suspicious transaction. We have provided an illustration of this concept under "Customer Risk versus Due Diligence and Suspicious Transaction Monitoring". CDD policies, procedures and processes are critical to the financial institution because they can aid in:

i. Detecting and reporting unusual or suspicious transactions that potentially expose the financial institution to financial loss, increased expenses and/or reputational risk.
ii. Avoiding criminal exposure from persons who use or attempt to use the financial institution's products and services for illicit purposes.
iii. Adhering to safe and sound banking practices.

Customer Due Diligence Guidance

AML/CFT policies, procedures and processes should include CDD guidelines that:

i. Are commensurate with the financial institution's AMLCFT risk profile, paying particular attention to higher-risk customers.
ii. Contain a clear statement of management's overall expectations and establish specific staff responsibilities, including who is responsible for reviewing or approving changes to a customer's risk rating or profile, as applicable.
iii. Ensure that the financial institution possesses sufficient customer information to implement an effective suspicious transaction monitoring system.
iv. Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.
v. Ensure the financial institution maintains current customer information.

Customer Risk

The Examiner should review and note whether or not the financial institution management has a thorough understanding of the money laundering or terrorist financing risks of the financial institution's customer base. Under this approach, the financial institution should obtain information at account-opening sufficient to develop an understanding of normal and expected activity for the customer's occupation or business operations. This understanding may be based on account type or customer classification.

This information should enable the financial institution to differentiate between lower-risk customers and higher-risk customers at account-opening. Financial institutions should monitor their lower-risk customers through regular suspicious transaction monitoring and customer due diligence processes. If there is indication of a potential change in the customer's risk profile (e.g. expected account activity, change in employment or business operations), management should reassess the customer risk-rating and follow established financial institution's policies and procedures for maintaining or changing customer risk ratings.

Examiners should note if much of the CDD information was confirmed through an information-reporting agency, banking references (for larger accounts), correspondence and telephone conversations with the customer and visits to the customer's place of business. Additional steps may include obtaining third-party references or researching public information (e.g. on the internet or commercial databases).

Examiner should review CDD processes of the financial institution which should include periodic risk-based monitoring of the customer relationship to determine whether there are substantive changes to the original CDD information (e.g. change in employment or business operations).

Enhanced Due Diligence for Higher-Risk Customers

Customers that pose higher money laundering or terrorist financing risks present increased exposure to financial institution. Due diligence policies, procedures and processes should be enhanced as a result. Enhanced due diligence (EDD) for higher-risk customers is especially critical in understanding their anticipated transactions and implementing a suspicious transaction monitoring system that reduces the financial institution's reputation, compliance and transaction risks. Higher-risk customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the financial institution. **A guidance for identifying higher-risk customers is provided in the core overview section of "ML/FT Risk Assessment".**

The financial institution may determine that a customer poses a higher risk because of the customer's business activity, ownership structure, anticipated or actual volume and types of transactions, including those transactions involving higher-risk jurisdictions. If so, the financial institution should consider obtaining, both at account-opening and throughout the relationship, the following information on the customer:

i. Purpose of the account.
ii. Source of funds and wealth.
iii. Individuals with ownership or control over the account, such as beneficial owners, signatories, or guarantors.
iv. Occupation or type of business (of customer or other individuals with ownership or control over the account).

v. Financial statements.
vi. Banking references.
vii. Domicile (where the business is organized).
viii. Proximity of the customer's residence, place of employment or place of business to the financial institution.
ix. Description of the customer's primary trade area and whether international transactions are expected to be routine.
x. Description of the business operations, the anticipated volume of currency and total sales, and a list of major customers and suppliers.
xi. Explanations for changes in account activity.

As due diligence is an ongoing process, a financial institution should take measures to ensure account profiles are current and monitoring should be risk-based. Financial institutions should consider whether risk profiles should be adjusted or suspicious transaction reported when the activity is inconsistent with the profile.

13. EXAMINATION PROCEDURES IN RESPECT OF CUSTOMER DUE DILIGENCE

Objective

i. Assess the appropriateness and comprehensiveness of the financial institution's customer due diligence (CDD) policies, procedures and processes for obtaining customer information and assess the value of this information in detecting, monitoring and reporting suspicious transaction.

ii. Determine whether the financial institution's CDD policies, procedures and processes are commensurate with the financial institution's risk profile. Determine whether the financial institution has processes in place for obtaining information at account opening, in addition to ensuring current customer information is maintained.

iii. Determine whether policies, procedures and processes allow for changes to a customer's risk rating or profile. Determine who is responsible for reviewing or approving such changes.

iv. Review the enhanced due diligence procedures and processes, the financial institution uses to identify customers that may pose higher risk for money laundering or terrorist financing.

v. Determine whether the financial institution provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient information or inaccurate information is obtained.

Transaction Testing

i. On the basis of a risk assessment, prior AML/CFT Bank Examination Reports and a review of the financial institution's audit findings sample CDD information for higher-risk customers. Determine whether the financial institution collects appropriate information and effectively incorporates this information into the suspicious transaction monitoring process. This sample can be performed when testing the financial institution's compliance with its policies, procedures and processes as well as when reviewing transactions or accounts for possible suspicious transaction.

ii. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with CDD.

14. OVERVIEW OF SUSPICIOUS TRANSACTION REPORTING

Objective

Assess the financial institution's policies, procedures, processes and overall compliance with statutory and regulatory requirements for monitoring, detecting and reporting suspicious activities.

Suspicious transaction reporting forms the cornerstone of the AML/CFT reporting system. It is critical to Nigeria's ability to utilize financial information to combat terrorism, terrorist financing, money laundering and other financial crimes. Examiners and financial institutions should recognize that the quality of STR content is critical to the adequacy and effectiveness of the suspicious transaction reporting system.

Within this system, regulatory agencies recognize that, as a practical matter, it is not possible for a financial institution to detect and report all potentially illicit transactions that flow through the financial institution. Bank Examiners should focus on evaluating a financial institution's policies, procedures and processes to identify, evaluate and report suspicious transaction. However, as part of the examination process, Examiners should review individual STR filing decisions to determine the effectiveness of the financial institution's suspicious transaction identification, evaluation and reporting process. Financial institutions, their holding companies and subsidiaries are required by MLPA, CBN AML/CFT Regulation 2009 and other regulations to file STR.

Systems to Identify, Research and Report Suspicious Transaction

Suspicious transaction monitoring and reporting are critical internal controls tool. Proper monitoring and reporting processes are essential to ensuring that the financial institution has an adequate and effective AML/CFT Compliance Program. Appropriate policies, procedures and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the financial institution's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities and geographies. The financial institution should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the financial institution's overall risk profile and

the volume of transactions. **Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.**

Generally, effective suspicious transaction monitoring and reporting systems include four key components. The components, listed below, are interdependent and an effective suspicious transaction monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect STR reporting and AML/CFT compliance.

The four key components to an effective monitoring and reporting system

i. **Identification or alert of unusual activity** which may include: employee identification, PEPs inquiries, other referrals, transaction and surveillance monitoring system output.
ii. Managing alerts.
iii. STR decision making.
iv. STR completion and filing.

These four components are present in financial institutions of all sizes. However, the structure and formality of the components may vary. Larger financial institutions will typically have greater differentiation and distinction between functions and may devote entire departments to the completion of each component. Smaller financial institutions may use one or more employees to complete several tasks (e.g. review of monitoring reports, research activity and completion of the actual STR). Policies, procedures and processes should describe the steps the financial institutions takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file STR, complete STR and file same.
Bank Examiners should review the adequacy and effectiveness of the policies, procedures and processes. They should describe the steps the financial institution takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file it as STR, complete STR and filing same.

Identification of Unusual/Suspicious Transaction

Financial institutions use a number of methods to identify potentially suspicious transaction, including but not limited to activity identified by employees during day-to-day operations, inquiries or requests on PEPs.

Identification of Suspicious Transaction by Employee

During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity. Financial institutions should implement appropriate training, policies and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious transaction. Financial institutions should be aware of all methods of identification and should ensure

that their suspicious transaction monitoring system includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research.

Inquiries and Requests by PEPs

Financial institutions should establish policies, procedures and processes for identifying PEPs' requests, monitoring their transaction activity when appropriate, identifying unusual or potentially suspicious transaction related to those subjects and filing, as appropriate, STRs related to them.

Examiners should review the adequacy and effectiveness of the policies, procedures and processes of identifying PEPs' requests, monitoring their transaction activity when appropriate, identifying unusual or potentially suspicious transaction related to them, filing as appropriate, STRs related to the subjects.

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system (sometimes referred to as a manual transaction monitoring system) typically targets specific types of transactions (e.g. those involving large amounts of cash, those send to or coming from foreign geographies) and includes a manual review of various reports generated by the financial institution's MIS or vendor systems in order to identify unusual activity. **Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports.** The process may involve review of daily reports, reports that cover a period of time (e.g. rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the financial institution's AML/CFT risk profile and appropriately cover its higher-risk products, services, customers, entities and geographic locations.

MIS or vendor system-generated reports typically use a discretionary currency threshold. Thresholds selected by financial institution's management for the production of transaction reports should enable management to detect unusual activity. Upon identification of unusual activity, assigned personnel should review CDD and other pertinent information to determine whether the activity is suspicious. Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each financial institution should evaluate and identify filtering criteria most appropriate to it.

Bank Examiners are required to review the programming of the financial institution's monitoring systems for reasonable filtering criteria. Typical transaction monitoring reports are as follows.

Currency Transaction Reports

Most vendors offer reports that identify all currency activity or currency activity greater than **USA $10,000**. These reports assist financial institutions with the filing of CTRs and identifying suspicious currency activity. Most financial institution information service providers offer currency activity reports that can filter transactions using various parameters, for example:

i. Currency transaction including multiple transactions greater than **$10,000**.

ii. Currency transaction (single and multiple transactions) below the **$10,000** reporting requirement **(e.g. between $7,000 and $10,000).**

iii. Currency transactions involving multiple lower dollar transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g. $30,000).

iv. Currency transactions aggregated by customer's name, tax identification number or customer information file number.

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, will significantly enhance a financial institution's ability to identify and evaluate unusual currency transactions.

Funds transfer records

The MLPA 2004 and CBN AML/CFT Regulation 2009 require financial institutions to maintain records of funds transfer in amounts of N1 million & above for individuals; and N2 million & above for corporate bodies. Periodic review of this information can assist financial institutions in identifying patterns of unusual activity. A periodic review of the funds transfer records in financial institutions with low funds transfer activity is usually sufficient to identify unusual activity. For financial institutions with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious transaction filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger currency funds transfer transactions for individuals and businesses.

Each institution should establish its own filtering criteria for both individuals and businesses. Non customer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed by Examiners for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, financial institutions may need to conduct a global relationship review to determine if a STR is warranted.

Monetary instrument records

Records for monetary instrument sales are required by the MLPA and CBN AML/CFT Regulation 2009. Such records can assist the financial institution in identifying possible currency structuring through the purchase of cashier's cheques, official bank/financial institution cheques, money orders, or traveller's cheques in amounts of USA $10,000 or its equivalent. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees. Reviews for suspicious transaction should **encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of**

commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system (sometimes referred to as an automated account monitoring system) can cover multiple types of transactions and use various rules to identify potentially suspicious transaction. In addition, many can adapt over time based on historical activity, trends or internal peer comparison. These systems typically use computer programs to identify individual transactions, patterns of unusual activity or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions and automated teller machine (ATM) transactions, directly from the financial institution's core data processing system.

Examiners should review the system with focus on specific parameters or filters in order to ensure that intended information is accurately captured and that the parameter or filter is appropriate for the financial institution's particular risk profile.

Understanding the filtering criteria of a surveillance monitoring system is critical to assessing the effectiveness of the system. System filtering criteria should be developed through a review of specific higher-risk products and services, customers and entities, and geographies. System filtering criteria, including specific profiles and rules should be based on what is reasonable and expected for each type of account. Monitoring accounts purely based on historical activity can be misleading if the activity is not actually consistent with similar types of accounts. For example, an account may have a historical transaction activity that is substantially different from what would normally be expected from that type of account (e.g. a cheque-cashing business that deposits large sums of currency versus withdrawing currency to fund the cashing of cheques).

The Examiner should check the level of authority in order to establish or change expected activity profiles that are clearly defined. He should check the approval limit of the CCO and senior management staff; controls & functions that limit access to the monitoring system; whether the management documents or is able to explain filtering criteria, thresholds used and how they are appropriate for the financial institution's risks; and whether management periodically reviews the filtering criteria and thresholds established to ensure that they are still effective. In addition, the monitoring system's programming methodology and effectiveness should be evaluated by the Examiner to ensure that the models are detecting potentially suspicious transaction.

Managing Alerts

Bank Examiners should ascertain and evaluate **alert management procedures and processes used** to investigate and evaluate identified unusual activity, noting the

financial institution's all methods of identification and should ensure that their suspicious transaction monitoring program includes processes to evaluate any unusual activity identified, regardless of the method of identification. Banks or financial institutions should have policies, procedures and processes in place for referring unusual activity from all areas of the financial institution or business lines to the Officer or department responsible for evaluating unusual activity. Within those procedures, **Examiners should assess if management has an established, clear and defined escalation process from the point of initial detection to disposition of the investigation.**

Examiners should evaluate financial institution's **management understanding of suspicious transaction monitoring across the institution's affiliates, subsidiaries and business lines that it enhances the institution's ability to detect suspicious transaction, and thus minimize the potential for financial losses, increased legal or compliance expenses and reputational risk to the institution.**

STR Completion and Filing

STR completion and filing are a critical part of the STR monitoring and reporting process. Appropriate policies, procedures and processes should be in place to ensure that STR forms are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing.

15. EXAMINATION PROCEDURES OF SUSPICIOUS TRANSACTION REPORTING

Objective

Assess the financial institution's policies, procedures, processes and overall compliance with statutory and regulatory requirements for monitoring, detecting and reporting suspicious activities.

Examiners may elect to "map out" the process followed by the financial institution to monitor, identify, research and report suspicious activities. Once the Examiner has an understanding of the process, he should follow an alert through the entire process.

Identification of Unusual Activity

1. Review the financial institution's policies, procedures and processes for identifying, researching and reporting suspicious transaction. **Determine whether they 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.
iv. Procedures for reviewing and evaluating transaction activity reported to law enforcement agencies. Examiners should also evaluate the policies, procedures and processes for:

a. Responding to LEA's requests.
b. Evaluating the account of the target for suspicious transaction.
c. Filing STRs, if necessary.
d. Handling account closures.

2. Review the financial institution's monitoring systems and how the system(s) fits into the institution's overall suspicious transaction monitoring and reporting process. When evaluating the effectiveness of the financial institution's monitoring systems, Examiners should consider the financial institution's overall risk profile (higher-risk products, services, customers, entities and geographic locations), volume of transactions and adequacy of staffing.

Transaction (Manual Transaction) Monitoring

3. Review the financial institution's transaction monitoring reports. Determine whether the reports capture all areas that pose money laundering and terrorist financing risks. **Examples of these reports include:** CTRs, PEPs returns, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, non-sufficient funds (NSF) reports and non-resident alien (NRA) reports.
4. Determine whether the financial institution's transaction monitoring systems use reasonable filtering criteria whose programming has been independently verified. Determine whether the monitoring systems generate accurate reports at a reasonable frequency.

Surveillance (Automated Account) Monitoring

5. Examiners should:

i. Identify the types of customers, products and services that are included within the surveillance monitoring system.
ii. Identify the system's methodology for establishing and applying expected activity or profile filtering criteria and for generating monitoring reports. Determine whether the system's filtering criteria are reasonable, adequate and effective.
iii. Determine whether the programming of the methodology has been independently validated.
iv. Determine that controls ensure limited access to the monitoring system and sufficient oversight of assumption changes.

Managing Alerts

6. Determine whether the financial institution has policies, procedures and processes to ensure the timely generation & review of and response to reports used to identify unusual activities.
7. Determine whether policies, procedures and processes require appropriate research for the monitoring of reports of unusual activity identified.
8. Evaluate the financial institution's policies, procedures and processes for referring unusual activity from all business lines to the CCO or department responsible for evaluating unusual activity.
9. Verify that staffing levels are sufficient to review reports, alerts and investigate items, and that staff possess the requisite experience level and proper investigatory tools. **The volume of system-alerts and investigations should not be tailored solely to meet existing staffing levels.**
10. Determine whether the financial institution's STR decision process appropriately considers all available CDD and EDD information.

STR Decision Making

11. Determine whether the financial institution's policies, procedures and processes include procedures for:

    i. Documenting decisions not to file a STR.
    ii. Escalating issues identified as the result of repeat STR filings on accounts.
    iii. Considering closing accounts as a result of continuous suspicious transaction.

STR Completion and Filing

12. Determine whether 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.
    iii. Sharing STRs with head offices and controlling companies, as necessary.

Transaction Testing

13. Transaction testing of suspicious transaction monitoring systems and reporting processes is intended to determine whether the financial institution's policies, procedures and processes are adequate and effectively implemented. Examiners should document the factors they used to select samples and should maintain a list of the accounts sampled. **The size and the sample should be based on the following:**

    i. Weaknesses in the account monitoring systems.

ii. The financial institution's overall ML/FT risk profile (e.g., number and type of *higher-risk products, services, customers, entities and geographies).*
iii. Quality and extent of review by audit or independent parties.
iv. Prior AML/CFT Bank examination findings.
v. Recent mergers, acquisitions or other significant organizational changes.
vi. Conclusions or questions from the review of the financial institution's STRs.

14. On the basis of a risk assessment, prior AML/CFT Bank Examination Reports and a review of the financial institution's audit findings, **sample specific customer accounts to review the following:**

i. Suspicious Transaction monitoring reports.
ii. CTR download information.
iii. Higher-risk banking operations (products, services, customers, entities and geographies).
iv. Customer activity.
v. Subpoenas received by the financial institution.
vi. Decisions not to file a STR.

15. For the customers selected previously, obtain the following information, if applicable:

i. CIP and account-opening documentation.
ii. CDD documentation.
iii. Two to three months of account statements covering the total customer relationship and showing all transactions.
iv. Sample items posted against the account (e.g., copies of cheques deposited and written debit or credit notes, and funds transfer beneficiaries and originators).
v. Other relevant information, such as loan files and correspondence.

16 . Review the selected accounts for unusual activity.

If the Examiner identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e. the sort of activity in which the customer is normally expected to engage). **When reviewing for unusual activity, consider the following:**

i. For individual customers: whether the activity is consistent with CDD information (e.g. occupation, expected account activity and sources of funds and wealth).

ii. For business customers: whether the activity is consistent with CDD information (e.g. type of business, size, location and target market).

17. Determine whether the transaction or surveillance suspicious transaction monitoring system detected the activity that the Examiner identified as unusual.

18. For transactions identified as unusual, discuss the transactions with the management. Determine whether the account officer demonstrates knowledge of

the customer and the unusual transactions. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions.

19. Determine whether the financial institution has failed to identify any reportable suspicious transaction.
20. From the results of the sample, determine whether the transaction or surveillance-suspicious-transaction monitoring system effectively detects unusual or suspicious transaction. Identify the underlying cause of any deficiencies in the monitoring systems (e.g. inappropriate filters, insufficient risk assessment or inadequate decision making).
21. On the basis of a risk assessment, prior AML/CFT Bank Examination Reports and a review of the financial institution's audit findings, select a sample of management's research decisions to determine the following:
    i. Whether management decisions of whether to file or not STR are supported and reasonable.
    ii. Whether documentation is adequate.
    iii. Whether the decision process is completed and STRs are filed in a timely manner.

22. On the basis of a risk assessment, prior AML/CFT Examination Reports and a review of the financial institution's audit findings, sample the STRs downloaded from the AML/CFT-reporting database or the financial institution's internal STR records. **Review the quality of STR content to assess the following:**
    iv. STRs contain accurate information.
    v. STR narratives are complete and thorough, and clearly explain why the activity is suspicious.
    vi. If STR narratives from the AML/CFT-reporting database are blank or contain language, such as "see attached," ensure that the financial institution is not mailing attachments to the database.

23. On the basis of AML/CFT examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with monitoring, detecting and reporting suspicious transaction.

16. OVERVIEW OF CURRENCY TRANSACTION REPORTING

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for the reporting of large currency transactions.

A financial institution must file Currency Transaction Report (CTR) for each transaction in cash (deposit, withdrawal, exchange or other payment or transfer) of N1,000,000 &

above or N5,000,000 & above for individuals or corporate bodies respectively **through, from or to the financial institution**. All types of currency transactions are to be reported, there are no "exempt persons".

Aggregation of Currency Transactions

Multiple cash transactions totaling more than N1,000,000 or N5,000,000 and above for individuals or corporate bodies respectively during any one business day are treated as a single transaction if the financial institution has knowledge that they are by or on behalf of the same person. Transactions throughout the financial institution should be aggregated when determining multiple transactions. Types of currency transactions subject to reporting requirements individually or by aggregation include but are not limited to **denomination exchanges, individual retirement accounts (IRA), loan payments, automated teller machine (ATM) transactions, purchases of certificates of deposit, deposits and withdrawals, funds transfers paid for in currency and monetary instrument purchases.** Financial institutions are strongly encouraged to develop systems necessary to aggregate currency transactions throughout the institution. Management should ensure that an adequate system exists and is implemented that will appropriately report currency transactions subject to the CBN AML/CFT Regulation 2009 requirement.

Filing Time Frames and Record Retention Requirements

A completed CTR must be filed (manually or electronically) with NFIU & AML/CFT Office, CBN **within 7days after the date of the transaction**. The financial institution must retain copies of CTRs for five years from the date of the report.

CTR Back-filing

If a financial institution has failed to file CTRs on reportable transactions, the institution is required to file the un-filed CTRs immediately.

17. CURRENCY TRANSACTION REPORTING EXAMINATION PROCEDURES

Objective

1. Assess the financial institution's compliance with statutory and regulatory requirements for the reporting of large currency transactions.
2. Determine whether the financial institution's policies, procedures and processes adequately address the preparation, filing and retention of CTRs. Ensure the returns are in accordance with the format designed by the **CBN & NFIU.**

3. Review correspondence that the financial institution has received from the **CBN & NFIU** relating to incorrect or incomplete CTRs (errors). Determine whether management has taken corrective action, when necessary.

4. Review the currency transaction system (e.g. how the financial institution identifies transactions applicable for the filing of CTRs). Determine whether the financial institution aggregates all or some currency transactions within the institution. Determine whether the institution **aggregates transactions by taxpayer identification number (TIN), individual taxpayer identification number (ITIN), employer identification number (EIN), or customer information file (CIF) number. Also, evaluate how CTRs are filed on customers with missing TINs or EINs.**

Transaction Testing

5. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of filed CTRs (hard copy or from computer-generated filings) to **determine whether:**

   i. CTRs are completed in accordance with CBN & NFIU instructions.
   ii. CTRs are filed for large currency transactions identified by tellers' cash proof sheets, automated large currency transaction systems or other types of aggregation systems that cover all relevant areas of the financial institution (there is no exemption for the customer).
   iii. CTRs are filed accurately and completely within **7** calendar days (whether manually or electronically) after the date of the transaction.
   iv. The financial institution's independent testing confirms the integrity and accuracy of the Management Information System (MIS) used for aggregating currency transactions. If not, the Examiner should confirm the integrity and accuracy of the MIS. The Examiner's review should confirm that tellers do not have the capability to override currency aggregation systems.
   v. Discrepancies exist between the financial institution's records of CTRs and the CTRs rendered to **CBN & NFIU as downloaded from the** reporting database. Confirm that the financial institution retains copies of CTRs for five years from the date of the report.

6. On the basis of examination procedures completed (including transaction testing) form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with currency transaction reporting.

18. OVERVIEW OF INFORMATION SHARING

Objective

Assess the financial institution's compliance with the statutory and regulatory requirements for the **"Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity".**

Information Sharing Between Law Enforcement and Financial Institutions

A federal, state, local or foreign law enforcement agency investigating terrorist activity or money laundering may request that CBN/NFIU solicit, on its behalf, certain information from a financial institution or a group of financial institutions. The law enforcement agency must provide a written certification to CBN/NFIU attesting that there is credible evidence of engagement or reasonably suspected engagement in terrorist activity or money laundering for each individual, entity or organization about which the law enforcement agency is seeking information. The law enforcement agency (LEA) also **must provide specific identifiers, such as a date of birth and address, which would permit a financial institution to differentiate among common or similar names.** Upon receiving a completed written certification from a LEA, CBN/NFIU **shall** require a financial institution to search its records to determine whether it maintains or has maintained accounts for or has engaged in transactions with, any specified individual, entity, or organization.

Search Requirements

Upon receiving an information-request, a financial institution must conduct a one-time search of its records to identify accounts or transactions of a named suspect. **Unless otherwise instructed by an information-request, financial institutions must search their records for current accounts, accounts maintained during the preceding 12 months and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months.** The financial institution must search its records and report any positive matches to CBN/NFIU within seven (7) days, unless otherwise specified in the information-request. If a financial institution identifies any account or transaction, it must report to the CBN/NFIU that it has a match. Relevant details are required to be provided to CBN/NFIU in addition to the fact that the financial institution has found a match. Where no match is found, a nil report must be submitted within the deadline. The institution is forbidden to keep silence or provide no response.

A financial institution may provide subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the institution takes the necessary steps, through the use of an agreement or procedures to ensure that the third party safeguards and maintains the confidentiality of the information.

If a financial institution that receives the subject lists fails to perform or complete searches on one or more information-request received during the previous 12 months, it must immediately obtain these prior requests from CBN/NFIU and perform a retroactive search of its records.

A financial institution is not required to perform retroactive searches in connection with information sharing requests that were transmitted more than 12 months before the date upon which it discovers that it failed to perform or complete searches on prior information requests. Additionally, in performing retroactive searches a financial institution is not required to search records created after the date of the original information request.

Restrictions and Confidentiality

Financial institutions should develop and implement comprehensive policies, procedures and processes for responding to requests. A financial institution may use the required information rendered to CBN/NFIU to determine whether to establish or maintain an account or engage in a transaction, or to assist in its AML/CFT compliance. While the subject-list could be used to determine whether to establish or maintain an account, CBN/NFIU strongly discourages financial institutions from using this as the sole factor in reaching a decision to do so, unless the request specifically states otherwise.

Subject-lists are not permanent "watch lists". They generally relate to one-time inquiries and could not be updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Furthermore, such names do not necessarily correspond to convicted or indicted persons. **A subject need only be "reasonably suspected" based on credible evidence of engaging in terrorist acts or money laundering.** Moreover, CBN/NFIU advises that inclusion of a name on subject-list should not be the sole factor used to determine whether to file STR. Financial institutions are required to establish a process for determining when and if a STR should be filed.

Actions taken pursuant to information provided in a request from CBN/NFIU do not affect a financial institution's obligations to comply with all of the rules and regulations of **MLPA 2004 and CBN AML/CFT Regulation 2009** nor do they affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to a request do not relieve a financial institution of its obligation to file a STR and immediately notify LEA, if necessary, in accordance with applicable laws and regulations.

A financial institution must not disclose to any person (other than to CBN/NFIU, the institution's primary regulator or the LEA on whose behalf CBN/NFIU is requesting information) the fact that CBN/NFIU has requested or obtained information. A financial institution should designate one or more points of contact for receiving information-requests. **An affiliated group of financial institutions may establish one point of contact to distribute the subject-list to respond to requests.** However, the subject-lists cannot be shared with any foreign office, branch or affiliate (unless the request specifically states otherwise). The lists cannot be shared with affiliates or subsidiaries of financial institutions' holding companies, if the affiliates or subsidiaries are not financial institutions.

Each financial institution must maintain adequate procedures to protect the security and confidentiality of requests from CBN/NFIU. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to those it has established to comply with regulatory requirements in order to **protect its customers' non-public personal information.** Financial institutions may keep a log of all requests received and of any positive matches identified and reported to CBN/NFIU

Documentation

Additionally, documentation of how all the required searches were conducted is essential. **A financial institution may maintain copies of the cover page of the request on which it signed-off that the records were checked, the date of the search and search results (positive or negative).** For positive matches with subject-lists received, copies of the form returned to CBN/NFIU and the supporting documentation should be retained. Financial institutions are required to print search self-verification document and subject response list for documentation purpose.

The **Subject Response List** displays the total number of positive responses submitted to CBN/NFIU for that transmission, the transmission date, the submitted date, the tracking number and subject name that had the positive hit. If the financial institution elects to maintain copies of such requests, the Examiner should not criticize it for doing so, **as long as it appropriately secures them and protects their confidentiality.** Audit reports should include an evaluation of compliance with these guidelines within their scope.

CBN/NFIU will regularly updates a list of search transmissions, including information on the date of transmission, tracking number and number of subjects listed in the transmission. Examiners may review this subject-list to verify that search requests have been received. Each financial institution should contact its primary regulator for guidance to ensure it obtains the subject-list and for updating contact information.

Voluntary Information Sharing

Financial institutions and their associates are encouraged to share information in order to identify and report activities that may involve terrorist activity or money laundering. Financial institutions should however notify the CBN/NFIU of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. Failure to comply with this requirement will result in loss of safe-harbour protection for information sharing and may result in a violation of privacy laws or other laws and regulations.
If a financial institution chooses to voluntarily participate in VIS, policies, procedures and processes should be developed and implemented for sharing and receiving of information.

Notice to share information given to CBN/NFIU

The financial institution should designate a point of contact for receiving and providing information. A financial institution should establish a process for sending and receiving information sharing requests. Additionally, a financial institution must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to CBN/NFIU. The CBN/NFIU provides participating financial institutions with access to a list of other participating financial institutions and their related contact information.

If a financial institution receives such information from another financial institution, it must also limit the use of the information and maintain its security and confidentiality. **Such information may be used only to identify and render returns on money laundering and terrorist financing; to determine whether to establish or maintain an account; to engage in other forms of transactions; or to assist in complying with MLPA & AML/CFT Regulation.**

The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to the ones it has established to comply with the regulation on the protection of its customers' non-public personal information. The VIS does not authorize a financial institution to share information on suspicious transactions, nor does it permit the financial institution to disclose the existence or non-existence of such transactions.

If financial institution shares information under VIS about the subject on STR, the information shared should be limited to underlying transaction and customer information. A financial institution may use information obtained under VIS to determine whether to file a STR, but the intention to prepare or file a STR cannot be shared with another financial institution. Financial institutions should establish a process for determining when and if a STR should be filed.

Actions taken pursuant to information obtained through the VIS process do not affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to information obtained through the voluntary information sharing process do not relieve a financial institution of its obligation to file a STR and to immediately notify the LEA (if necessary) in accordance with all applicable laws and regulations.

19. EXAMINATION PROCEDURES ON INFORMATION SHARING

Objective

Assess the financial institution's compliance with the statutory and regulatory requirements for the "Special Information Sharing Procedures to Deter Money Laundering and Terrorist Financing".

Information Sharing Between LEA and Financial Institutions

1. Verify that the financial institution is currently receiving VIS requests from CBN/NFIU or from an affiliated financial institution that serves as the subject financial institution's point of contact. If the financial institution is not receiving information requests or changes in its information contact, the financial institution should update its information point of contact with its primary regulator.

2. Verify that the financial institution has sufficient policies, procedures and processes to document compliance; maintain sufficient internal controls; provide ongoing training; and independently test its compliance with AML/CFT Regulation 2009. **The procedures should accomplish the following:**

   i. Designate a point of contact for receiving information requests.
   ii. Ensure that the confidentiality of requested information is safeguarded.
   iii. Establish a process for responding to CBN/NFIU's requests.
   iv. Establish a process for determining if and when a STR should be filed.

3. Determine whether the search policies, procedures and processes the financial institution uses to respond to VIS requests are comprehensive and cover all records identified in the General Instructions Manual for such requests. The General Instructions Manual includes searching for accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last six months. Financial institutions have seven (7) days from the transmission date of the request to respond to a VIS request.
4. If the financial institution uses a third-party vendor to perform or facilitate searches, determine whether an agreement or procedures are in place to ensure confidentiality.

5. Review the financial institution's internal controls and determine whether its documentation to evidence compliance with VIS requests is adequate. **This documentation should include:**

   i. Copies of VIS requests.
   ii. A log that records the tracking numbers and includes a sign-off column.
   iii. For VIS subject lists received, copies of the cover page of the requests, with a financial institution sign-off, that the records were checked, the date of the search and search results (positive or negative).
   iv. Copies of generated search self-verification documents.
   v. For positive matches, copies of the form returned to CBN/NFIU (generated Subject Response Lists) and the supporting documentation should be retained.

Voluntary Information Sharing

6. Determine whether the financial institution has decided to share information voluntarily. If so, verify that the financial institution has filed a notification form with CBN/NFIU and provides an effective date for the sharing of information that is within the previous 12 months.
7. Verify that the financial institution has policies, procedures and processes for sharing information and receiving shared information.

8. Financial institutions that choose to share information voluntarily should have policies, procedures and processes to document compliance; maintain adequate internal controls; provide ongoing training; and independently test its compliance with regulatory provisions.

At a minimum, the procedures should:

i. Designate a point of contact for receiving and providing information.
ii. Ensure the safeguarding and confidentiality of information received and information requested.
iii. Establish a process for sending and responding to requests, including ensuring that other parties with whom the financial institution intends to share information (including affiliates) have filed the proper notice.
iv. Establish procedures for determining whether and when a STR should be filed.

9. If the financial institution is sharing information with other entities and is not following the outlined regulatory procedures, the Examiners are required to review the privacy rules.

They should review the financial institution's documentation (including account analysis) on a sample of the information shared and received, evaluate how the financial institution determined whether a STR was warranted. They should note that the financial institution is not required to file STRs solely on the basis of information obtained through the voluntary information sharing process. In fact, the information obtained through the voluntary information sharing process may enable the financial institution to determine that no STR is required for transactions that may have initially appeared suspicious. The financial institution should have considered account activity in determining whether a STR was warranted.

Transaction Testing

10. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of positive matches or recent requests to determine whether the following requirements have been met:

i. The financial institution's policies, procedures and processes enable it to search all of the records identified in the General Instructions Manual for VIS requests. Such processes may be electronic, manual or both.
ii. The financial institution searches appropriate records for each information request received. **For positive matches:**

    a. Verify that a response was provided to CBN/NFIU within the designated time period.
    b. Review the financial institution's documentation (including account analysis) to evaluate how the financial institution determined whether a STR was warranted. Financial institutions are not required to file STRs solely on the basis of a match with a named subject; instead, account activity should be considered in determining whether a STR is warranted.

iii. The financial institution uses information only in the manner and for the purposes allowed and keeps information secure and confidential.

11. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with information sharing.

20. Overview of Purchase and Sale of Monetary Instruments Record-keeping

Objective

Assess the institution's compliance with statutory and regulatory requirements for the recording of information required for the purchase and sale of monetary instruments for currency in amounts **N1 million & above for individuals, N5 million & above in respect of corporate entities and USA $1,000 .** This section covers the regulatory requirements as set forth by the MLPA. Additional discussions and procedures on specific money laundering risks for purchase and sale of monetary instruments activities are discussed in the expanded sections of this Manual .

Financial institutions sell a variety of monetary instruments (e.g. bank cheques or drafts, including foreign drafts, cashier's cheques and traveler's cheques) in exchange for Naira currency. Purchasing these instruments in amounts of less **than the reportable threshold of N1 million or USA $1,000** is a common method used by money launderers to evade large currency transaction reporting requirements. Once converted from cash, criminals typically deposit these instruments in accounts with other institutions to facilitate the movement of funds through the payment system. In many cases, the persons involved do not have an account with the bank**/other financial institution** from which the instruments are purchased.

Purchaser Verification

Financial institutions are required to verify the identity of persons purchasing monetary instruments for cash in **tandem with the reportable threshold amount of N1 million & above or USA $1,000**, and to maintain records of all such sales.

Financial institutions **should** either verify that the purchaser of monetary instruments is a deposit account holder with identifying information on record with the financial institution, or a financial institution may verify the identity of the purchaser in accordance with the form of identification contained in AML/CFT Regulation in respect of the customer's name and address and other means of identification acceptable by the financial community for cashing cheques by non-customers. The financial institution must obtain additional information for purchasers who do not have deposit accounts. The method used to verify the identity of the purchaser must be recorded.

Acceptable Identification

The CBN AML/CFT Regulation 2009 provides guidance on how a financial institution can verify the identity of an elderly, disabled or "financial exclusion" customer who does not possess the normally acceptable forms of identification. A financial institution may accept a International Passport, National Identity Card or Driver's License along with another form of documentation bearing the customer's name and address. Additional forms of documentation include a utility bill, a tax identification number (TIN). **The forms of alternate identification a financial institution decides to accept should be included in its formal policies, procedures and processes.**

Contemporaneous Purchases

Contemporaneous purchases of the same or different types of instruments totaling **N1 million for individuals, N5 million for corporate entities or more and USA $1,000, must be treated as one purchase.** Multiple purchases during one business day totaling **N1 million for individuals, N5 million for corporate entities or more, or USA $ 1,000** must be aggregated and treated as one purchase if the financial institution has knowledge that such purchases have occurred.

Indirect Currency Purchases of Monetary Instruments

Financial institutions may implement a policy requiring customers who are deposit account holders and who want to purchase monetary instruments in amounts of **N1 million for individuals, N5 million for corporate entities or USA $1,000** with cash to first deposit the cash into their deposit accounts. Nothing within the CBN AML/CFT Regulation 2009 or other regulations prohibits a financial institution from instituting such a policy.

However, when a customer purchases a monetary instrument in amounts of **N1 million for individuals, N5 million for corporate entities or USA $1,000** using cash, the customer should first deposits such cash into his/its account, the transaction is still subject to the regulatory recordkeeping and reporting requirements. These requirements apply whether the transaction is conducted in accordance with a financial institution's established policy or at the request of the customer. Generally, when a

bank**/other financial institution** sells monetary instruments to deposit account holders, it is expected to already maintain most of the regulatory required information in the normal course of its business.

Record keeping and Retention Requirements

A financial institution's records of sales must contain, at a minimum, the following information:

If the purchaser **has a deposit account** with the bank:

i. Name of the purchaser.
ii. Date of purchase.
iii. Types of instruments purchased.
iv. Serial numbers of each of the instruments purchased.
v. Amounts of each of the instruments purchased in Naira or other currencies.
vi. Specific identifying information, if applicable.

If the **purchaser does not have a deposit account** with the financial institution:

i. Name and address of the purchaser.
ii. Social security or alien identification number of the purchaser.
iii. Date of birth of the purchaser.
iv. Date of purchase.
v. Types of instruments purchased.
vi. Serial numbers of each of the instruments purchased.
vii. Naira **or other currencies** amount of each of the instruments purchased.
viii. Specific identifying information for verifying the purchaser's identity (e.g. state of issuance and number on driver's licence).

If the purchaser cannot provide the required information at the time of the transaction or through the financial institution's own previously verified records, **the transaction should be refused.** The records of monetary instrument sales must be retained for five years and be available for & reported to CBN, NFIU, auditors **and other** competent authorities.

21. EXAMINATION PROCEDURES OF PURCHASE AND SALE OF MONETARY INSTRUMENTS & RECORD-KEEPING

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for the recording of information required for the purchase and sale of monetary instruments for currency in amounts of N1million & above, N5 million & above for individuals and corporate entities respectively or USA $1,000 & above or its equivalent.

This section covers the regulatory requirements as set forth by the MLPA, 2004 and CBN AML/CFT Regulation, 2009.

1. Determine whether the financial institution maintains the required records (in a manual or an automated system) for sales of its cheques or drafts including foreign drafts, cashier's cheques, and traveler's cheques for currency in amounts between **$1,000** (or its equivalent) to purchasers who have deposit accounts with it.
2. Determine whether the financial institution's policies, procedures and processes permit currency sales of monetary instruments to purchasers who do not have deposit accounts with the institution (non-depositors):

    i. **If so**, determine whether the financial institution maintains the required records for sales of monetary instruments to non-depositors; and
    ii. **If not permitted**, determine whether the financial institution allows sales on an exception basis.

Transaction Testing

3. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of monetary instruments sold for currency in amounts between USA $1,000, inclusive to determine whether it obtains, verifies and retains the required records to ensure compliance with regulatory requirements.
4. On the basis of examination procedures completed (including transaction testing) form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with the purchase and sale of monetary instruments.
5. On the basis of the previous conclusion and the risks associated with the financial institution's activity in this area, proceed to expanded-examination procedures, if necessary.

22. OVERVIEW OF FUNDS TRANSFERS RECORD-KEEPING

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for funds transfers.

This section covers the regulatory requirements as set forth in the MLPA, 2004 and CBN AML/CFT Regulation, 2009. Refer to the expanded sections of this manual for discussions and procedures regarding specific money laundering risks for funds transfer activities.

Funds transfer systems enable the instantaneous transfer of funds, including both domestic and cross-border transfers. Consequently these systems can present an

attractive method to disguise the source of funds derived from illegal activity. The CBN AML/CFT Regulation, 2009 requires each financial institution involved in funds transfers to collect and retain certain information in connection with funds transfers of USA$1,000 or more. The information required to be collected and retained depends on the financial institution's role in the particular funds transfer (originator's financial institution, intermediary financial institution, or beneficiary's financial institution). The requirements may also vary depending on whether an originator or beneficiary is an established customer of a financial institution and whether a payment order is made in person or otherwise.

It also requires all financial institutions to include certain information in transmittal orders for funds transfers of USA $1,000 or more.

Responsibilities of Originator's Financial Institutions
Record-keeping Requirements

For each payment order in the amount of USA $1,000 or more that a financial institution accepts as an originator's financial institution, it must obtain and retain the following records:

i. Name and address of the originator.
ii. Amount of the payment order.
iii. Date of the payment order.
iv. Any payment instructions.
v. Identity of the beneficiary's institution.
vi. As many of the following items as are received with the payment order:
    a. Name and address of the beneficiary.
    b. Account number of the beneficiary.
    c. Any other specific identifier of the beneficiary.

Additional Record-keeping Requirements for Non-established Customers

If the originator is not an established customer of the financial institution, the originator's financial institution must collect and retain the information listed above. In addition, the originator's financial institution must collect and retain other information, depending on whether the payment order is made in person by the originator.

Payment Orders Made in Person

If the payment order is made in person by the originator, the originator's financial institution must verify the identity of the person placing the payment order before it accepts the order. If it accepts the payment order, the originator's financial institution must obtain and retain the following records:

i. Name and address of the person placing the order.
ii. Type of identification document reviewed.
iii. Number of the identification document (e.g., driver's licence).

iv. The person's Taxpayer Identification Number (TIN) [e.g., National I.D. number or Employer Identification Number (EIN)] or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of lack of it thereof.

If the originator's financial institution has knowledge that the person placing the payment order is not the originator, the originator's financial institution must obtain and record the originator's TIN or, if none, the alien identification number or passport number and country of issuance, or a notation of lack of it thereof.

Payment Orders Not Made in Person

If a payment order is not made in person by the originator, the originator's financial institution must obtain and retain the following records:

i. Name and address of the person placing the payment order.
ii. The person's TIN or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of lack of it thereof, and a copy or record of the method of payment (e.g., cheque or credit card transaction) for the funds transfer.

If the originator's financial institution has knowledge that the person placing the payment order is not the originator, the originator's financial institution must obtain and record the originator's TIN or, if none, the alien identification number or passport number and country of issuance, or a notation of lack of it thereof.

Irretrievability

Information retained must be **retrievable by reference to the name of the originator**. When the originator is an established customer of the financial institution and has an account used for funds transfers, information retained must also be **retrievable by account number.** Records must be maintained for five years.

Travel Rule Requirement

For funds transmittals of USA $1,000 or more, the transmittor's financial institution must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution:

i. Name and account number of the transmittor, and, if the payment is ordered from an account.
ii. Address of the transmittor.
iii. Amount of the transmittal order.
iv. Date of the transmittal order.
v. Identity of the recipient's financial institution.
vi. As many of the following items as are received with the transmittal order:

a. Name and address of the recipient.
b. Account number of the recipient.
c. Any other specific identifier of the recipient.

vii. Either the name and address or the numerical identifier of the transmittor's financial institution.

Responsibilities of Intermediary Institutions

Recordkeeping Requirements

For each payment order of **USA $1,000** or more that a financial institution accepts as an intermediary financial institution, the institution must retain a record of the payment order.

Travel Rule Requirements

For funds transmittals of USA $1,000 or more, the intermediary financial institution must include the following information if received from the sender in a transmittal order at the time that order is sent to a receiving financial institution:

i. Name and account number of the transmittor.
ii. Address of the transmittor.
iii. Amount of the transmittal order.
iv. Date of the transmittal order.
v. Identity of the recipient's financial institution.
vi. As many of the following items as are received with the transmittal order:

a. Name and address of the recipient.
b. Account number of the recipient.
c. Any other specific identifier of the recipient.

vii. Either the name and address or the numerical identifier of the transmittor's financial institution.

Intermediary financial institutions must pass on all of the information received from a transmittor's financial institution or the preceding financial institution, but they have no duty to obtain information not provided by the transmittor's financial institution or the preceding financial institution.

Responsibilities of Beneficiary's Financial Institutions

Recordkeeping Requirements

For each payment order of USA $1,000 or more that a financial institution accepts as a beneficiary's financial institution, the institution must retain a record of the payment order.

If the beneficiary is not an established customer of the financial institution, the beneficiary's institution must retain the above information for each payment order of USA $1,000 or more.

Proceeds Delivered in Person

If proceeds are delivered in person to the beneficiary or its representative or agent, the institution must verify the identity of the person receiving the proceeds and retain a record of the following:

i. Name and address.
ii. The type of document reviewed.
iii. The number of the identification document.
iv. The person's TIN, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.
v. If the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification.

Proceeds Not Delivered in Person

If proceeds are not delivered in person, the institution must retain a copy of the cheque or other instrument used to effect the payment, or the institution must record the information on the instrument. The institution must also record the name and address of the person to whom it was sent.

Irretrievability

Information retained must be retrievable by reference to the name of the beneficiary. When the beneficiary is an established customer of the institution and has an account used for funds transfers, information retained must also be retrievable by account number.
There are **no Travel Rule requirements** for beneficiary financial institutions.

Abbreviations and Addresses

Although the use of coded names or pseudonyms are not permitted, the use of abbreviated names, names reflecting different accounts of a corporation (e.g., XYZ Payroll Account), and trade and assumed names of a business ("doing business as") or the names of unincorporated divisions or departments of the business are allowed.

Customer Address

Customer's street address is required to be included in a transmittal order and this should be known to the transmittor's financial institution.

The regulatory interpretation of the term "address" means either the transmittor's street address or the transmittor's address maintained in the financial institution's automated CIF (not mailing address such as post office box) as long as the institution maintains the transmittor's address on file and the address information is retrievable upon request by LEA.

23. OBJECTIVE OF EXAMINATION PROCEDURES FUNDS TRANSFERS RECORD-KEEPING

Assess the financial institution's compliance with statutory and regulatory requirements for funds transfers. This section covers the regulatory requirements as set forth in the CBN AML/CFT Regulation, 2009.

i. Verify that the financial institution obtains and maintains appropriate records.
ii. Verify that the financial institution transmits payment information as required.
iii. Verify that the financial institution files CTRs when currency is received or
    a. dispersed in a funds transfer that exceeds USA $10,000.
iv. If the financial institution sends or receives funds transfers to or from institutions in other countries, especially those with strict privacy and secrecy laws, assess whether the financial institution has policies, procedures and processes to determine whether amounts, the frequency of the transfer and countries of origin or destination are consistent with the nature of the business or occupation of the customer.

Transaction Testing

On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of funds transfers processed **as an originator's financial institution, an intermediary financial institution and a beneficiary's financial institution** to ensure the institution collects, maintains or transmits the required information, depending on the institution's role in the transfer.
On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with funds transfers.

24. OVERVIEW OF FOREIGN CORRESPONDENT ACCOUNT RECORD KEEPING AND DUE DILIGENCE

Assess the financial institution's compliance with statutory and regulatory requirements for correspondent accounts for foreign shell banks, foreign correspondent account record keeping and due diligence programs to detect and report money laundering and suspicious activity.

Foreign Shell Bank Prohibition and Foreign Correspondent Account Record keeping

A "correspondent account" is an account established by a financial institution for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of the foreign financial institution, or to handle other financial transactions related to the foreign financial institution.

An "account" means any formal banking or business relationship established to provide regular services, dealings and other financial transactions. It includes a demand deposit, savings deposit, or other transaction or asset account and a credit account or other extension of credit.

Accounts maintained by foreign financial institutions for financial institutions covered by the rule are not "correspondent accounts" subject to this regulation.

A financial institution is prohibited from establishing, maintaining, administering, or managing a correspondent account for, or on behalf of, a foreign shell bank.

A foreign shell bank is defined as a foreign financial institution without a physical presence in any country. A financial institution is also required to take reasonable steps to ensure that any correspondent account established, maintained, administered, or managed for a foreign financial institution is not being used by that foreign financial institution to provide banking services indirectly to foreign shell banks.

Certifications

A financial institution that maintains a correspondent account for a foreign financial institution must **maintain records identifying the owners of each foreign financial institution.** A financial institution must also record the name and street address of a person who resides in Nigeria and who is authorized, and has agreed, to be an agent to accept service of legal process. A financial institution must produce these records within seven days upon receipt of a written request from a LEA.

Account Closure

Financial institutions must obtain certifications (or re-certifications) or otherwise obtain the required information within 30 calendar days after the date an account is established and at least once every three years thereafter. If the financial institution is unable to obtain the required information, it must close all correspondent accounts with the foreign financial institution within a commercially reasonable time.

Verification

A financial institution should review certifications for reasonableness and accuracy. If a financial institution at any time knows, suspects, or has reason to suspect that any information obtained or that any other information it relied on is no longer correct, the financial institution must request that the foreign financial institution verify or correct such information, or the financial institution must take other appropriate measures to ascertain its accuracy. Therefore, financial institutions should review certifications for

potential problems that may warrant further review, such as use of post office boxes or forwarding addresses.

If the financial institution has not obtained the necessary or corrected information within 90 days, it must close the account within a commercially reasonable time. During this time, the financial institution may not permit the foreign financial institution to establish any new financial positions or execute any transactions through the account, other than those transactions necessary to close the account. Also, a financial institution may not establish any other correspondent account for the foreign financial institution until it obtains the required information.

A financial institution must also retain the original of any document provided by a foreign financial institution, and retain the original or a copy of any document otherwise relied on for the purposes of the regulation, for at least five years after the date that the financial institution no longer maintains any correspondent account for the foreign financial institution.

Requests for AML Records by Regulator

Also, upon request by its regulator(s), a financial institution must provide or make available records related to its AML compliance or one of its customers, within 120 hours from the time of the request.

Special Due Diligence Program for Foreign Correspondent Accounts

This subsection requires each financial institution that establishes, maintains, administers, or manages a correspondent account for a foreign financial institution to take certain AML measures for such accounts.

General Due Diligence

Financial institutions are required to establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures and controls that are reasonably designed to enable the financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by it for a foreign financial institution.

Due diligence policies, procedures and controls

i. Determining whether each such foreign correspondent account is subject to "Enhanced Due Diligence" (EDD).
ii. Assessing the money laundering risks presented by each such foreign correspondent account.
iii. Applying risk-based procedures and controls to each such foreign correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the

correspondent account activity sufficient to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

Risk assessment of foreign financial institutions

A financial institution's general due diligence program must include policies, procedures and processes to assess the risks posed by its foreign financial institution customers. A financial institution's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. Its due diligence program should provide for the risk assessment of foreign correspondent accounts considering all relevant factors, including, as appropriate:

i. The nature of the foreign financial institution's business and the markets it serves.
ii. The type, purpose and anticipated activity of the foreign correspondent account.
iii. The nature and duration of the financial institution's relationship with the foreign financial institution (and, if relevant, with any affiliate of the foreign financial institution).
iv. The AML and supervisory regime of the jurisdiction that issued the charter or licence to the foreign financial institution and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
v. Information known or reasonably available to the financial institution about the foreign financial institution's AML record, including public information in standard industry guides, periodicals and major publications.

Monitoring of foreign correspondent accounts

As part of ongoing due diligence, financial institutions should periodically review their foreign correspondent accounts. Monitoring will not, in the ordinary situation, involve scrutiny of every transaction taking place within the account, but, instead, should involve a review of the account sufficient to ensure that the financial institution can determine whether the nature and volume of account activity are generally consistent with information regarding the purpose of the account and expected account activity and to ensure that the financial institution can adequately identify suspicious transactions.

An effective due diligence program will provide for a range of due diligence measures, based upon the financial institution's risk assessment of each foreign correspondent account. The starting point for an effective due diligence program, therefore, should be a stratification of the money laundering risk of each foreign correspondent account based on the financial institution's review of relevant risk factors (such as those identified above) to determine which accounts may require increased measures. The due diligence program should identify risk factors that would warrant the institution

conducting additional scrutiny or increased monitoring of a particular account. As due diligence is an ongoing process, a financial institution should take measures to ensure account profiles are current and monitoring should be risk-based. Financial institutions should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile.

Enhanced Due Diligence

Financial institutions are required to establish risk-based EDD policies, procedures and controls when establishing, maintaining, administering or managing a correspondent account in Nigeria for foreign financial institutions operating under any one or more of the following:

i. An **offshore banking licence**.
ii. A **banking licence issued by a foreign country** that has been designated as non-cooperative with international AML principles or procedures by an inter-governmental group or organization of which Nigeria is a member and Nigeria representative to the group or organization concurs its decision.
iii. A **banking licence issued by a foreign country that has been designated by the CBN as warranting special measures** due to money laundering concerns.

If such an account is established or maintained, the financial institution is required to establish EDD policies, procedures and controls to ensure that the financial institution, at a minimum, takes reasonable steps to:

i. Determine, for any such foreign financial institution whose shares are not publicly traded, the identity of each of the owners of the foreign financial institution and the nature and extent of the ownership interest of each such owner;
ii. Conduct enhanced scrutiny of such account to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable laws and regulations. This enhanced scrutiny is to reflect the risk assessment of the account and shall include, as appropriate;
iii. Obtain and consider information relating to the foreign financial institution's anti-money laundering program to assess the risk of money laundering presented by the foreign financial institution's correspondent account;
iv. Monitor transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity;
v. Obtain information from the foreign financial institution about the identity of any person with authority to direct transactions through any correspondent account that is a payable through account, and the sources and the beneficial owner of funds or other assets in the payable through account; and
vi. Determine whether the foreign financial institution for which the correspondent account is maintained in turn maintains correspondent accounts for other foreign financial institutions that use the foreign financial

institution's correspondent account. If so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign financial institution's correspondent accounts for other foreign financial institutions, including, as appropriate, the identity of those foreign financial institutions.

In addition to those categories of foreign financial institutions identified in the regulation as requiring EDD, financial institutions may find it appropriate to conduct additional due diligence measures on foreign financial institutions identified through application of the financial institution's general due diligence program as posing a higher risk for money laundering. Such measures may include any or all of the elements of EDD set forth in the regulation, as appropriate for the risks posed by the specific foreign correspondent account.

As also noted in the above section on general due diligence, a financial institution's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. Accordingly, where a financial institution is required or otherwise determines that it is necessary to conduct EDD in connection with a foreign correspondent account, the financial institution may consider the risk assessment factors discussed in the section on general due diligence when determining the extent of the EDD that is necessary and appropriate to mitigate the risks presented. In particular, the anti-money laundering and supervisory regime of the jurisdiction that issued a charter or licence to the foreign financial institution may be especially relevant in a financial institution's determination of the nature and extent of the risks posed by a foreign correspondent account and the extent of the EDD to be applied.

Special Procedures When Due Diligence Cannot Be Performed

A financial institution's due diligence policies, procedures and controls established **must include procedures to be followed in circumstances when appropriate due diligence or EDD cannot be performed** with respect to a foreign correspondent account and when the financial institution should:

i. Refuse to open the account
ii. Suspend transaction activity
iii. File STR
iv. Close account

25. EXAMINATION PROCEDURES OF FOREIGN CORRESPONDENT ACCOUNT RECORD-KEEPING AND DUE DILIGENCE

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for correspondent accounts for foreign shell banks, foreign correspondent account

record keeping and due diligence programs to detect and report money laundering and suspicious activity.

1. Determine whether the financial institution engages in foreign correspondent banking.

Foreign Shell Bank Prohibition and Foreign Correspondent Account Recordkeeping

2. If so, review the financial institution's policies, procedures and processes. At a minimum, policies, procedures and processes should accomplish the following:

    i. Prohibit dealings with foreign shell banks and specify the responsible party for obtaining, updating and managing certifications or information for foreign correspondent accounts.
    ii. Identify foreign correspondent accounts and address the sending, tracking, receiving and reviewing of certification requests or requests for information.
    iii. Evaluate the quality of information received in responses to certification requests or requests for information.
    iv. Determine whether and when a STR should be filed.
    v. Maintain sufficient internal controls.
    vi. Provide for ongoing training.
    vii. Independently test the financial institution's compliance with related regulatory requirements.

3. Determine whether the financial institution has a file on current certification or current information (that would otherwise include the information contained within a certification) for each foreign correspondent account to determine whether the foreign correspondent is not a foreign shell bank.
4. If the financial institution has foreign branches, determine whether the financial instituion has taken reasonable steps to ensure that any correspondent accounts maintined for its foreign branches are not used to indirectly provide banking services to a foreign shell bank.

Special Due Diligence Program for Foreign Correspondent Accounts

5. Determine whether the financial institution has established a general due diligence program that includes appropriate, specific, risk-based and (where necessary) enhanced policies, procedures and controls for correspondent accounts established, maintained, administered or managed in Nigeria for foreign financial institutions ("foreign correspondent account"). The general due diligence program must be applied to each foreign correspondent account. **Verify that due diligence policies, procedures and controls include:**

    i. Determining whether any foreign correspondent account is subject to EDD.
    ii. Assessing the money laundering risks presented by the foreign correspondent account.

iii. Applying risk-based procedures and controls to each foreign correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

6. Review the due diligence program's policies, procedures and processes governing the AML risk assessment of foreign correspondent accounts. **Verify that the financial institution's due diligence program considers the following factors (as appropriate) as criteria in the risk assessment:**

i. The nature of the foreign financial institution's business and the markets it serves.
ii. The type, purpose and anticipated activity of the foreign correspondent account.
iii. The nature and duration of the financial institution's relationship with the foreign financial institution and any of its affiliates.
iv. The AML and supervisory regime of the jurisdiction that issued the charter or license to the foreign financial institution and (to the extent that information regarding such jurisdiction is reasonably available) of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
v. Information known or reasonably available to the financial institution about the foreign financial institution's AML record.

7. Ensure the program is reasonably designed to:

i. Detect and report (on an ongoing basis) known or suspected money laundering activity.
ii. Perform periodic reviews of correspondent account activity to determine consistency with the information obtained about the type, purpose and anticipated activity of the account.

8. For foreign financial institutions subject to EDD, evaluate the criteria that the Nigerian financial institution uses to guard against money laundering in and report suspicious activity in connection with any correspondent accounts held by such foreign financial institutions. **Verify that the EDD procedures are applied to each correspondent account established for foreign financial institutions operating under:**

i. An offshore banking licence.
ii. A banking licence issued by a foreign country that has been designated as non-cooperative with international AML principles or procedures by an inter-governmental group or organization of which Nigeria is a member, and with which Nigeria representative to the group or organization concurs its decision.
iii. A banking licence issued by a foreign country that has been designated by the CBN as warranting special measures due to AML concerns.

iv. Review the financial institution's policies, procedures and processes and determine whether they include reasonable steps for conducting enhanced scrutiny of foreign correspondent accounts to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable laws and regulations. **Verify that this enhanced scrutiny reflects the risk assessment of each foreign correspondent account that is subject to such scrutiny and includes, as appropriate:**

i. Obtain and consider information relating to the foreign financial institution's anti-money laundering program to assess the risk of money laundering presented by the foreign financial institution's correspondent account.
ii. Monitor transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity.
iii. Obtain information from the foreign financial institution about the identity of any person with authority to direct transactions through any correspondent account that is a payable through account, and the sources and beneficial owner of funds or other assets in the payable through account.

9. Review the financial institution's policies, procedures and processes to determine whether foreign correspondent financial institutions subject to EDD maintain correspondent accounts for other foreign financial institutions. If so, determine whether the financial institution's policies, procedures and processes include reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign correspondent financial institution's correspondent accounts for other foreign financial institutions, including (as appropriate) the identity of those foreign financial institutions.

10. Determine whether policies, procedures and processes require the financial institution to take reasonable steps to identify each of the owners with the power to vote 10 percent or more of any class of securities of a non-public traded foreign correspondent financial institution for which it opens or maintains an account that is subject to EDD. For such accounts, evaluate the financial institution's policies, procedures and processes to determine each such owner's interest.

Transaction Testing

Foreign Shell Bank Prohibition and Foreign Correspondent Account Record keeping

11. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of foreign financial institution accounts. **From the sample selected, determine the following:**

i. Whether certifications and information on the accounts are complete and reasonable.
ii. Whether the financial institution has adequate documentation to evidence that it does not maintain accounts for or indirectly provide services to foreign shell banks.
iii. For account closures, whether closures were made within a reasonable time period and that the relationship was not re-established without sufficient reason.
iv. Whether there are any LEA requests for information regarding foreign correspondent accounts. If so, ascertain that requests were met in a timely manner.
v. Whether the financial institution received any official notifications to close a foreign financial institution account. If so, ascertain that the accounts were closed within ten business days.
vi. Whether the financial institution retains (for five years from the date of account closure) the original of any document provided by a foreign financial institution, as well as the original or a copy of any document relied on in relation to any summons or subpoena of the foreign financial institution issued.
vii. Special Due Diligence Program for Foreign Correspondent Accounts

12. From a sample selected, determine whether the financial institution consistently follows its general due diligence policies, procedures and processes for foreign correspondent accounts. It may be necessary to expand the sample to include correspondent accounts maintained for foreign financial institutions other than foreign financial institutions (such as money transmitters or currency exchangers), as appropriate.
13. From the original sample, determine whether the financial institution has implemented EDD procedures for foreign financial institutions operating under:

i. An offshore banking licence.
ii. A banking licence issued by a foreign country that has been designated as Non-cooperative with international AML principles or procedures.
iii. A banking licence issued by a foreign country that has been designated by the CBN as warranting special measures due to AML concerns.
iv. From a sample of accounts that are subject to EDD, verify that the financial institution has taken reasonable steps, in accordance with the financial institution's policies, procedures and processes, to:

a. Determine, for any such foreign financial institution whose shares are not publicly traded, the identity of each of the owners of the foreign financial institution with the power to vote 10 percent or more of any class of securities of the financial institution, and the nature and extent of the ownership interest of each such owner.
b. Conduct enhanced scrutiny of any accounts held by such financial institutions to guard against money laundering and report suspicious activity.

c. Determine whether such foreign financial institution provides correspondent accounts to other foreign financial institutions and, if so, obtain information relevant to assess and mitigate money laundering risks associated with the foreign financial institution's correspondent accounts for other foreign financial institutions, including, as appropriate, the identity of those foreign financial institutions.

14. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures and processes to meet regulatory requirements associated with foreign correspondent account record keeping and due diligence.

15. On the basis of the previous conclusion and the risks associated with the financial institution's activity in this area, proceed to expanded examination procedures, if necessary.

26. OVERVIEW OF PRIVATE BANKING DUE DILIGENCE PROGRAM (NON-NIGERIANS)

Objective

Assess the financial institution's compliance with the statutory and regulatory requirements to implement policies, procedures and controls to detect and report money laundering and suspicious activity through private banking accounts established, administered or maintained for non-Nigerian persons.

Private banking can be broadly defined as providing personalized financial services to wealthy clients. In particular, a financial institution must establish appropriate, specific and (where necessary) EDD policies, procedures and controls that are reasonably designed to enable the financial institution to detect and report instances of money laundering through such accounts.

CBN AML/CFT Regulation, 2009 mandates enhanced scrutiny to detect and, if appropriate, report transactions that may involve proceeds of foreign corruption for private banking accounts that are requested or maintained by or on behalf of a senior foreign/local political figure or the individual's immediate family and close associates.

Private Banking Accounts

A "private banking account" is an account (or any combination of accounts) maintained at a financial institution that satisfies all three of the following criteria:

16. Requires a minimum aggregate deposit of funds or other assets of not less than USA$500,000 or its equivalent.

17. Is established on behalf of or for the benefit of one or more Nigerian or non-igerian persons who are direct or beneficial owners of the account.
18. Is assigned to, or is administered by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between a financial institution overed by the regulation and the direct or beneficial owner of the account.

With regard to the minimum deposit requirement, a "private banking account" is an account (or combination of accounts) that requires a minimum deposit of not less than USA $500,000 or its equivalent. A financial institution may offer a wide range of services that are generically termed private banking, and even if certain (or any combination, or all) of the financial institution's private banking services do not require a minimum deposit of not less than USA $500,000 or its equivalent, **these relationships should be subject to a greater level of due diligence under the financial institution's risk- based AML compliance program.**

Due Diligence Program

A financial institution must establish and maintain a due diligence program that includes policies, procedures and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account for a Nigerian or non-Nigerian person that is established, maintained, administered, or managed in the Nigeria by the financial institution. **The due diligence program must ensure that, at a minimum, the financial institution takes reasonable steps to do each of the following:**

i. Ascertain the identity of all nominal and beneficial owners of a private banking account.
ii. Ascertain whether the nominal or beneficial owner of any private banking account is a senior local/foreign political figure.
iii. Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account.
iv. Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, and to file a STR, as appropriate, to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account.

Risk Assessment of Private Banking Accounts for Nigerian/Non-Nigerian Persons

The nature and extent of due diligence conducted on private banking accounts for Nigerian/non- Nigerian persons will likely vary for each client depending on the presence of potential risk factors. More extensive due diligence, for example, may be appropriate for new clients; clients who operate in, or whose funds are transmitted from or through jurisdictions with weak AML controls; and clients whose lines of business are primarily currency-based (e.g., casinos or currency exchangers). Due diligence should also be commensurate with the size of the account. Accounts with

relatively more deposits and assets should be subject to greater due diligence. In addition, if the financial institution at any time learns of information that casts doubt on previous information, further due diligence would be appropriate.

Ascertaining Source of Funds and Monitoring Account Activity

Financial institutions that provide private banking services generally obtain considerable information about their clients, including the purpose for which the customer establishes the private banking account. This information can establish a baseline for account activity that will enable a financial institution to better detect suspicious activity and to assess situations where additional verification regarding the source of funds may be necessary. Financial institutions are not expected, in the ordinary course of business, to verify the source of every deposit placed into every private banking account. However, financial institutions should monitor deposits and transactions as necessary to ensure that activity is consistent with information that the financial institution has received about the client's source of funds and with the stated purpose and expected use of the account. Such monitoring will facilitate the identification of accounts that warrant additional scrutiny.

Enhanced Scrutiny of Private Banking Accounts for Senior Local/Foreign Political Figures

The term "senior political figure" is defined to include one or more of the following:

i. A current or former: Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not).
ii. Senior official of a major foreign political party.
iii. Senior executive of a foreign-government-owned commercial enterprise.
iv. A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.
v. An immediate family member (including spouses, parents, siblings, children, and a spouse's parents and siblings) of any such individual.
vi. A person who is widely and publicly known (or is actually known by the relevant financial institution) to be a close associate of such individual.

Senior political figures as defined above are often referred to as "Politically Exposed Persons" or PEPs. For private banking accounts for which a senior local/foreign political figure is a nominal or beneficial owner, the financial institution's due diligence program must include enhanced scrutiny that is reasonably designed to detect and report transactions that may involve the proceeds of local/foreign corruption. The term "proceeds of local/foreign corruption" means any asset or property that is acquired by, through, or on behalf of a senior local/foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and includes any other property into which any such assets have been transformed or converted.

Enhanced scrutiny of private banking accounts for senior local/foreign political figures should be risk-based. Reasonable steps to perform enhanced scrutiny may include consulting publicly available information regarding the home country of the client, contacting branches of the financial institution operating in the home country of the client to obtain additional information about the client and the political environment, and conducting greater scrutiny of the client's employment history and sources of income. For example, funds transfers from a government account to the personal account of a government official with signature authority over the government account may raise a financial institution's suspicions of possible political corruption. In addition, if a financial institution's review of major news sources indicates that a client may be or is involved in political corruption, the financial institution should review the client's account for unusual activity and:

i. Refuse to open the account.
ii. Suspend transaction activity.
iii. File an STR.
iv. Close the account.

Identifying Senior Political Figures

Financial institutions are required to establish policies, procedures and controls that include reasonable steps to ascertain the status of an individual as a senior political figure. Procedures should require obtaining information regarding employment and other sources of income, and the financial institution should seek information directly from the client regarding possible senior local/foreign political figure status. The financial institution should also check references, as appropriate, to determine whether the individual holds or has previously held a senior political position or may be a close associate of a senior local/foreign political figure. In addition, the financial institution should make reasonable efforts to review public sources of information regarding the client.

Financial institutions applying reasonable due diligence procedures in accordance with regulatory requirements may not be able to identify, in every case, individuals who qualify as senior local/foreign political figures, and, in particular, their close associates, and thus may not apply enhanced scrutiny to all such accounts. If the financial institution's due diligence program is reasonably designed to make this determination, and it administers this program effectively, then the financial institution should generally be able to detect, report and take appropriate action when suspected money laundering is occurring with respect to these accounts, even in cases when the financial institution has not been able to identify the accountholder as a senior foreign political figure warranting enhanced scrutiny.

Special Procedures When Due Diligence Cannot Be Performed

A financial institution's due diligence policies, procedures and controls established must include special procedures when appropriate due diligence cannot be performed. **These special procedures must include when the financial institution should:**

i. Refuse to open the account.
ii. Suspend transaction activity.
iii. File an STR.
iv. Close the account.

27. EXAMINATION PROCEDURES OF PRIVATE BANKING DUE DILIGENCE PROGRAM (NIGERIAN/NON-NIGERIA PERSONS)

Objective

Assess the financial institution's compliance with the statutory and regulatory requirements to implement policies, procedures and controls to detect and report money laundering and suspicious activity through private banking accounts established, administered or maintained for Nigerian/non-Nigeria persons.

1. Determine whether the financial institution offers private banking accounts in accordance with the regulatory definition of a private banking account. A private banking account means an account (or any combination of accounts) maintained at a financial institution covered by the regulation t**hat satisfies all three of the following criteria:**

i. Requires a minimum aggregate deposit of funds or other assets of not less than USA $500,000 or its equivalent.
ii. Is established on behalf of or for the benefit of one or more Nigerian/non-Nigerian persons who are direct or beneficial owners of the account.
iii. Is assigned to, or is administered or managed by, in whole or in part, an officer, employee, or agent of the financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account.

If an account satisfies the last two criteria in the definition of a private banking account as described above, but the institution does not require a minimum balance of USA $500,000 or its equivalent, then the account does not qualify as a private banking account under this rule. However, the account is subject to the internal controls and risk-based due diligence included in the institution's general AML Compliance program.

2. Determine whether the financial institution has implemented due diligence policies, procedures and controls for private banking accounts established, maintained, administered, or managed in Nigeria by the financial institution for Nigerian/non-Nigerian persons. Determine whether the policies, procedures and controls are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account.

3. Review the financial institution's policies, procedures and controls to assess whether the financial institution's due diligence program includes reasonable steps to:

   i. Ascertain the identity of the nominal and beneficial owners of a private banking account.
   ii. Ascertain whether any nominal or beneficial owner of a private banking account is a senior local/foreign political figure.
   iii. Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the private banking accounts.
   iv. Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds and with the stated purpose and expected use of the account, as needed, to guard against money laundering and to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking accounts.

4. Review the financial institution's policies, procedures and controls for performing enhanced scrutiny to assess whether they are reasonably designed to detect and report transactions that may involve the proceeds of local/foreign corruption for which a senior political figure is a nominal or beneficial owner.

Transaction Testing

5. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of customer files to determine whether the financial institution has ascertained the identity of the nominal and beneficial owners of, and the source of funds deposited into private banking accounts. **From the sample selected determine the following:**

   i. Whether the financial institution's procedures comply with internal policies and statutory requirements.
   ii. Whether the financial institution has followed its procedures governing risk assessment of private banking accounts.
   iii. Whether the financial institution performs enhanced scrutiny of private banking accounts for which senior foreign political figures are nominal or beneficial owners, consistent with its policy, regulatory guidance, and statutory requirements.

6. On the basis of examination procedures completed, including transaction testing form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with private banking due diligence programs.

28. OVERVIEW OF SPECIAL MEASURES

Objective

Assess the financial institution's compliance with statutory and regulatory requirements.

Financial institutions and domestic financial agencies are required to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern.

Types of Special Measures

The following five special measures can be imposed, either individually, jointly or in any combination:

Record keeping and Reporting of Certain Financial Transactions

Under the first special measure, financial institutions may be required to maintain records or to file reports or both, concerning the aggregate amount of transactions or the specifics of each transaction with respect to a jurisdiction, financial institution, class of transactions or type of account that is of primary money laundering concern.

Information Relating to Beneficial Ownership

Under the second special measure, financial institutions may be required to take reasonable and practicable steps to obtain and retain information concerning the beneficial ownership of any account opened or maintained by a foreign person (other than a foreign entity whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or trading market), or a representative of such foreign person that involves a jurisdiction, financial institution, class of transactions or type of account that is of primary money laundering concern.

Information Relating to Certain Payable through Accounts

Under the third special measure, financial institutions that open or maintain a payable through account involving a jurisdiction, financial institution, class of transactions or type of account **that is of primary money laundering concern** are required:

i. To identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and
ii. To obtain information about each customer (and representative) that is substantially comparable to that which the financial institution obtains in the ordinary course of business with respect to its customers residing in Nigeria.

Information Relating to Certain Correspondent Accounts

Under the fourth special measure, financial institutions that open or maintain a correspondent account involving a jurisdiction, financial institution, class of transactions or type of account **that is of primary money laundering concern** are required to:

i. Identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and
ii. Obtain information about each such customer (and representative) that is substantially comparable to that which a depository institution obtains in the ordinary course of business with respect to its customers residing in Nigeria.

29. EXAMINATION PROCEDURES OF SPECIAL MEASURES

Objective

Assess the financial institution's compliance with statutory and regulatory requirements.

1. Determine the extent of the financial institution's international banking activities and the foreign jurisdictions in which the financial institution conducts transactions and activities with particular emphasis on foreign correspondent banking and payable through accounts.

2. As applicable, determine whether the financial institution has established policies, procedures and processes to respond to specific special measures imposed by regulators that are applicable to its operations. Evaluate the adequacy of the policies, procedures and processes for detecting accounts or transactions within jurisdictions, financial institutions or transactions subject to final special measures.

3. Determine, through discussions with management and review of the financial institution's documentation, whether the financial institution has taken action in response to final special measures.

Transaction Testing

4. Determine all final special measures issued by regulators that are applicable to the financial institution.

5. For any of the first four types of special measures, determine whether the financial institution obtained, recorded or reported the information required by each particular special measure.

6. For the fifth special measure (prohibition), determine whether the financial institution complied with the prohibitions or restrictions required by each particular special measure and complied with any other actions required by the special measures.

7. As necessary, search the financial institution's MIS and other appropriate records for accounts or transactions with jurisdictions, financial institutions or transactions subject to final special measures.

8. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with special measures.

30. EXAMINATION PROCEDURES FOREIGN FINANCIAL INSTITUTION AND FINANCIAL ACCOUNTS REPORTING

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for the reporting of foreign financial institution and financial accounts.

1. Determine whether the financial institution has a financial interest in, or signature or other authority over the financial institution, securities, or other financial accounts in a foreign country, as well as **whether the financial institution is required to file a Report of Foreign Financial Institution and Financial Accounts.**

2. If applicable, review the financial institution's policies, procedures and processes for filing annual reports.

Transaction Testing

3. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of accounts to determine whether the financial institution has appropriately completed, submitted and retained copies of returns.

4. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements.

31. OVERVIEW OF INTERNATIONAL TRANSPORTATION OF CURRENCY OR MONETARY INSTRUMENTS REPORTING

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for the reporting of international shipments of currency or monetary instruments.
Each person (including a financial institution) who physically transports, mails or ships currency or monetary instruments in excess of USA $10,000 at one time out of or into Nigeria (and each person who causes such transportation, mailing or shipment) **must file a Declaration Report with the Nigeria Customs Services (NCS) at the time of entry into or departure from Nigeria.**

When a person receives currency or monetary instruments in an amount exceeding USA $10,000 at one time that have been shipped from any place outside Nigeria, a report must be filed with NCS within 15 days of receipt of the instruments (unless a report has already been filed). The report is to be completed by or on behalf of the person requesting transfer of the currency or monetary instruments.

Financial institutions are also required to report these items if they are mailed or shipped through the postal service or by common carrier. However, a financial institution or trust company recognized under the law is not required to report overland shipments of currency or monetary instruments if they are shipped to or received from an established customer maintaining a deposit relationship with the financial institution where the latter can reasonably conclude that the amounts do not exceed what is commensurate with the customary conduct of the business, industry or profession of the customer concerned.

Management should implement applicable policies, procedures and processes for filing these declaration reports. Management should review the international transportation of currency and monetary instruments.

32. EXAMINATION PROCEDURES OF INTERNATIONAL TRANSPORTATION OF CURRENCY OR MONETARY INSTRUMENTS REPORTING

Objective

Assess the financial institution's compliance with statutory and regulatory requirements for the reporting of international shipments of currency or monetary instruments.

1. Determine whether the financial institution has (or has caused to be) physically transported, mailed or shipped currency or other monetary instruments in excess of USA $10,000, at one time, out of Nigeria or whether the financial institution has received currency or other monetary instruments in excess of USA $10,000, at one time that has been physically transported, mailed or shipped into Nigeria.

2. If applicable, review the financial institution's policies, procedures and processes for filing a Report of International Transportation of Currency or Monetary Instruments for each shipment of currency or other monetary instruments in excess of USA $10,000 out of or into Nigeria (including shipments sent through the postal service, common carrier, etc).

Transaction Testing

3. On the basis of a risk assessment, prior examination reports and a review of the financial institution's audit findings, select a sample of transactions conducted after

the previous examination to determine whether the financial institution has appropriately completed, submitted and retained copies of the reports.
4. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures and processes to meet regulatory requirements associated with these reports.

33. MONITORING OF OFFICE OF FOREIGN ASSETS CONTROL (OFAC) LIST

Objective

Assess the financial institution's procedures and processes of monitoring and identifying OFAC blocked countries, entities, etc. Also assess the appropriateness of these procedures and processes taking into consideration the financial institution's products, services, customers, entities, transactions, geographical locations and its scope of international operations.

Though complying with OFAC requirements is mandatory to only U.S. based banks, it is important that financial institutions in Nigeria be aware of these requirements and take notice of all OFAC blocked/banned countries, terrorists, entities, etc. This would enable the financial institutions know and avoid carrying out transactions with blocked entities as transactions that pass through a U.S. correspondent bank would be confiscated. This could cause both financial and reputation loss to the Nigerian financial institution victims.

Financial institutions are therefore required to have procedures and processes of knowing the requirements, updating them, monitoring and reporting transactions with entities, countries, etc on the OFAC List.

34. EXAMINATION PROCEDURES TO ENSURE COMPLIANCE

Objective

Assess the financial institution's procedures and processes of monitoring and identifying OFAC blocked countries, entities, etc. Also assess the appropriateness of these procedures and processes taking into consideration the financial institution's products, services, customers, entities, transactions and its scope of international operations.

1. Review the financial institution's procedure and processes in the context of the following:

    i. The extent of and method for conducting OFAC searches of each relevant department or business line.
    ii. Timeliness of obtaining and updating OFAC lists or filtering criteria.

iii. The appropriateness of the filtering criteria used by the institution.
iv. The process used to block and reject transactions.
v. The process used to inform management of blocked or rejected transactions.
vi. The adequacy and timeliness of reports to CBN and NFIU.
vii. The record retention requirements (e.g. five-year requirement to retain relevant records)

Transaction Testing

2. On the basis of the financial institution's risk assessment, prior examination reports and review of its audit findings, select the following samples to test the institution's effectiveness of its processes and procedures in monitoring the OFAC list:

    i. If the financial institution uses an automated system to conduct searches, assess the timing of when updates are made to the system, and when the most recent OFAC changes were made to the system.
    ii. If the institution does not use an automated system, evaluate the process used to check the existing customer base against the OFAC list and the frequency of such checks.
    iii. Review a sample of potential OFAC matches and evaluate the institution's resolution for blocking and rejection processes.
    iv. Review a sample of reports to CBN and NFIU and evaluate their completeness and timeliness.

Blocked Transactions

U.S. law requires that assets and accounts of an OFAC-specified country, entity or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. bank to an offshore bank, and there is an OFAC-designated party on the transaction, it must be blocked.

The definition of assets and property is broad and is specifically defined within each sanction program. Assets and property includes anything of direct, indirect, present, future or contingent value (including all types of bank transactions). **Financial institutions are required to block transactions that:**

i. Are owned by or held on behalf of a blocked individual or entity;
ii. Are to or go through a blocked entity; or
iii. Are in connection with a transaction in which a blocked individual or entity has an interest.

Note that if, for example, a U.S. bank receives instructions to make a funds transfer payment that falls into one of the above categories, it must execute the payment order, block the funds and report such transaction to the appropriate authorities.

Prohibited Transactions

In some cases, an underlying transaction (**a transaction that would constitute a support of the prohibited entity**) may be prohibited, but there is no block- able interest in the transaction. It means that the transaction should not be accepted and there is no OFAC requirement to block the assets. In these cases, the transaction should simply be rejected (i.e., not processed).

OFAC Licences

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a licence to engage in an otherwise prohibited transaction when it determines that the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licences, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC.

Specific licences are issued on a case-by-case basis. A specific licence is a written document issued by OFAC authorizing a particular transaction or set of transactions. To receive a specific licence, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms to U.S. foreign policy under a particular program, the licence will be issued. If a financial institution's customer claims to have a specific licence, the institution is required to verify that the transaction conforms to the terms of the licence and obtain and retain a copy of the authorizing licence.

OFAC Reporting

Financial institutions are required to report all blockings to CBN and NFIU within 10 days of the occurrence and annually by December 31 concerning those assets blocked. Once assets or funds are blocked, they should be placed in a blocked account. Prohibited transactions that are rejected must also be reported to CBN and NFIU within 10 days of the occurrence.

Financial institutions are required to also keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.
Officers are requested to obtain additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries Brochures; the **Specially Designated Nationals (SDN) or Blocked Persons List** (including both entities and individuals); recent OFAC actions; and "Frequently Asked Questions," from OFAC's Web site.

OFAC Compliance Program

As a matter of sound banking practice and in order to ensure compliance, financial institutions should establish and maintain an effective written OFAC compliance program commensurate with their OFAC risk profile based on products, services, customers, and geographic locations. The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate the institution's employee or employees as responsible for OFAC compliance and create adequate training programs for appropriate officers.

OFAC Risk Assessment

A fundamental element of a sound OFAC compliance program is the institution's assessment of its specific product lines, customer base and nature of transactions and identification of higher-risk areas for OFAC transactions. The initial identification of higher-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of operations, financial institutions should consider all types of transactions, products and services when conducting their risk assessment and establishing appropriate policies, procedures and processes.

An effective risk assessment should be a composite of multiple factors. It depends upon the circumstances and certain factors may be weighed more heavily than others.
Another consideration for the risk assessment is the account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the institution includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the institution's risk profile and available technology.

Based on the institution's OFAC risk profile for each area and available technology, it should establish policies, procedures and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser and jurisdiction). In evaluating the level of risk, the institution should exercise judgment and take into account all indicators of risk. **Although not an exhaustive list, examples of products, services, customers and geographic locations that may carry a higher level of OFAC risk include:**

i. International funds transfers.
ii. Nonresident alien accounts.
iii. Foreign customer accounts.
iv. Cross-border automated clearing house (ACH) transactions.
v. Commercial letters of credit and other trade finance products.
vi. Transactional electronic banking.
vii. Foreign correspondent bank accounts.

viii. Payable through accounts.
ix. International private banking.
x. Overseas branches or subsidiaries.

Internal Controls

An effective OFAC compliance program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. **Internal controls should include the following elements:**

i. Identifying and reviewing suspicious transactions

The institution's policies, procedures and processes should address how it will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software or a combination of both. For screening purposes, the institution should clearly define its criteria for comparing names provided on the OFAC list with the names in its files or on transactions and for identifying transactions or accounts involving sanctioned countries. The policies, procedures and processes should also address how it will determine whether an initial OFAC hit is a valid match or a false hit.

A high volume of false hits may indicate a need to review the institution's interdiction program. The screening criteria used by financial institutions to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high-volume of transactions, the institution's interdiction software should be able to identify close name derivations for review. The Specially Designated Nationals (SDN)/Blocked Persons List's attempts to provide name derivations may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list.

Lower-risk institutions or areas and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on an institution's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), financial institutions should consider the likelihood of incurring a violation. In addition, financial institutions should periodically reassess their OFAC filtering system. For example, if an institution identifies a name derivation of an OFAC target, OFAC guidelines suggest that the institution adds the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter. Financial institutions that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check are subject to penalty action. In addition, financial

institutions are required to have policies, procedures and processes in place to check existing customers when there are additions or changes to the OFAC list.
The frequency of the review should be based on the institution's OFAC risk. For example, institutions with a lower OFAC risk level may periodically (e.g., monthly or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit and noncustomer transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures and processes, the institution should keep in mind that the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program will be a factor in determining penalty actions to be imposed. **The institution should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.**

If an institution uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, it is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, financial institutions should establish adequate controls and review procedures for such relationships.

ii. **Updating OFAC lists**

An institution's OFAC compliance program should include policies, procedures and processes for timely updating of the lists of blocked countries, entities and individuals and disseminating such information throughout its domestic operations and its offshore offices, branches and foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

iii. **Reporting**

An OFAC compliance program should also include policies, procedures and processes for handling items that are validly blocked or rejected items under the various sanctions programs. In the case of interdictions related to narcotics trafficking or terrorism, financial institutions are required to notify CBN & NFIU as soon as possible by phone about potential hits with a follow-up in writing within ten days. Most other items should be reported through usual channels within ten days of the occurrence.
The policies, procedures and processes should also address the management of blocked accounts. Financial institutions are responsible for tracking the amount of blocked funds, the ownership of those funds and interest paid on those funds. Total amounts blocked, including interest must be reported to the CBN & NFIU by December 31 & June 30 of each year. When an institution acquires or merges with another, both institutions should take into consideration the need to review and maintain such records and information. Financial institutions are required to also file STRs on blocked narcotics- or terrorism-related transactions in addition to the blocking reports rendered on OFAC.

iv. **Maintaining licence information**

Financial institutions are required to maintain copies of customers' OFAC licences in their files. This will allow the institution to verify whether or not a customer is initiating a legal transaction. institutions should also be aware of the expiration date on the licence. If it is unclear whether a particular transaction is authorized by a licence, the institution should confirm with OFAC. Maintaining copies of licences will also be useful if another institution in the payment chain requests verification of a licence's validity. Copies of licences should be maintained for five years, following the most recent transaction conducted in accordance with the licence.

v. Independent Testing

Every institution should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants or other qualified independent parties. For large institutions, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller institutions, the audit should be consistent with their OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC compliance program.

vi. Responsible Individual

Every financial institution is required to designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC compliance program, including the reporting of blocked or rejected transactions to the CBN & NFIU and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the institution's OFAC risk profile.

vii. Training

The institution should provide adequate training for all appropriate employees. The scope and frequency of the training should be consistent with its OFAC risk profile and appropriate to employee responsibilities.

D. EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR CONSOLIDATED AND OTHER TYPES OF AML/CFT COMPLIANCE PROGRAM STRUCTURES

35. OVERVIEW OF AML/CFT COMPLIANCE PROGRAM STRUCTURES

Objective

Assess the structure and management of the institution's AML/CFT Compliance Program and (if applicable) its consolidated or partially consolidated approach to AML/CFT compliance.

Every financial institution is required to have a comprehensive AML/CFT Compliance Program that addresses the requirements of the Money Laundering (Prohibition) Act and CBN AML/CFT Regulation 2009 applicable to all its operations.

Each financial institution has discretion as to how its AML/CFT Compliance Program is structured and managed. It may structure and manage its AML/CFT Compliance Program or some parts of the program within a legal entity; with some degree of consolidation across entities within the institution; or as part of a comprehensive enterprise risk management framework.
Many large, complex financial institutions aggregate risk of all types (e.g., compliance, operational, credit, interest rate risk, etc.) on an institution-wide basis in order to maximize efficiencies and better identify, monitor and control all types of risks within or across affiliates, subsidiaries, lines of business or jurisdictions. In such institutions, management of MLPA, CBN AML/CFT Regulation 2009 risk is generally the responsibility of a corporate compliance function that supports and oversees the AML/CFT Compliance Program.

Other financial institutions may adopt a structure that is less centralized but still consolidates some or all aspects of AML/CFT compliance. For example, risk assessment, internal controls, suspicious transaction monitoring, independent testing or training may be managed centrally. Such centralization can effectively maximize efficiencies and enhance assessment of risks and implementation of controls across business lines, legal entities and jurisdiction of operation. For example, a centralized AML/CFT risk assessment function may enable a financial institution to determine its overall risk exposure to a customer doing business with it in multiple business lines or jurisdiction. Regardless of how a consolidated AML/CFT Compliance Program is organized, it should reflect the institution's business structure, size and complexity. It should be designed to effectively address risks, exposures and applicable legal requirements across the institution.

A consolidated approach should also include the establishment of corporate standards for AML/CFT compliance that reflect the expectations of the financial institution's board of directors, with senior management working to ensure that the Chief Compliance Officer implements these corporate standards. Individual lines of business policies would then supplement the corporate standards and address specific risks within the line of business or department.

A consolidated AML/CFT Compliance Program typically includes a central point where its risks throughout the institution are aggregated. Under a consolidated approach, risk should be assessed both within and across all business lines, legal entities and jurisdictions of operation. **Compliance Programs for global institutions should**

incorporate the AML laws and requirements of the various jurisdictions in which they operate. Internal audit should assess the level of compliance with the consolidated AML/CFT Compliance Program.

Bank Examiners should be aware that some complex and diversified financial institutions may have various subsidiaries that hold different types of licences and banking charters or may organize business activities and AML/CFT Compliance Program components across their legal entities. For instance, a highly diversified financial institution may establish or maintain accounts using multiple legal entities that are examined by multiple regulators. This action may be taken in order to maximize efficiencies, enhance tax benefits, adhere to jurisdictional regulations, etc. This methodology may present a challenge to the Bank Examiner reviewing AML/CFT compliance in a legal entity within an institution. As appropriate, Examiners should coordinate efforts with other regulatory agencies in order to address these challenges or ensure the examination scope appropriately covers the legal entity examined.

Structure of the AML/CFT compliance function

Financial institution has discretion as to how to structure and manage its AML/CFT Compliance Program. For example, a small institution may choose to combine its compliance with other functions and utilize the same personnel in several roles. In such circumstances, **there should still be adequate senior-level attention to AML/CFT compliance and sufficient dedicated resources. As is the case in all structures, the audit function should remain independent.**

A larger and more complex institution may establish a corporate AML/CFT compliance function to coordinate some or all its responsibilities. **For example, when there is delegation of AML/CFT compliance responsibilities and its Chief Compliance Officer is located within lines of business, expectations should be clearly set forth in order to avoid conflicts and ensure effective implementation of the AML/CFT Compliance Program.** In particular, allocation of responsibility should be clear with respect to the content and comprehensiveness of MIS reports, the depth and frequency of monitoring efforts, and the role of different parties within the financial institution (e.g., risk, business lines, operations) in AML/CFT compliance decision-making processes. **A clear communication of which functions have been delegated and which remain centralized help to ensure consistent implementation of the AML/CFT Compliance Program among lines of business, affiliates and jurisdictions.** In addition, a clear line of responsibility may help to avoid conflicts of interest and ensure that objectivity is maintained.

Regardless of the management structure or size of the institution, AML/CFT compliance staff located within lines of business are not precluded from close interaction with the management and staff of the various business lines. AML/CFT compliance functions are often most effective when strong working relationships exist between compliance and business line staff.

In some compliance structures, the compliance officers could report to the management of the business line. This can occur in smaller institutions when the AML/CFT compliance officer reports to a senior officer; in larger institutions, the compliance officer could report to a line business manager; or in a foreign owned financial institution, its Nigeria's operations could be reported by the compliance officer to a single officer or executive. **These situations can present risks of potential conflicts of interest that could hinder effective AML/CFT compliance.**

Maintenance of compliance independence

i. Providing AML/CFT compliance officer a reporting line to the corporate compliance or other independent function;
ii. Ensuring that AML/CFT compliance officer is actively involved in all matters affecting AML risk (e.g., new products, review or termination of customer relationships, filing determinations);
iii. Establishing a process for escalating and objectively resolving disputes between AML/CFT compliance officer and business line management; and
iv. Establishing internal controls to ensure that compliance objectivity is maintained when AML/CFT compliance officer is assigned additional responsibilities.

36. MANAGEMENT AND OVERSIGHT OF THE AML/CFT COMPLIANCE PROGRAM

The board of directors and senior management of a financial institution have different responsibilities and roles in overseeing and managing AML/CFT compliance risk. The board of directors has primary responsibility for ensuring that the financial institution has a comprehensive and effective AMLCFT Compliance Program and oversight framework that is reasonably designed to ensure compliance with MLPA, AML/CFT Regulation and related regulations. Senior management is responsible for implementing the board-approved AML/CFT Compliance Program.

Board of directors

The board of directors is responsible for approving the AML/CFT Compliance Program and for overseeing the structure and management of its compliance function. The board is responsible for setting an appropriate culture of AML/CFT compliance, establishing clear policies regarding the management of key AML/CFT risks and ensuring that these policies are adhered to in practice.

The board should ensure that senior management is fully capable, qualified and properly motivated to manage the AML/CFT compliance risks arising from the institution's business activities in a manner that is consistent with the board's expectations. The board should ensure that its compliance function has an appropriately prominent status within the organization. Senior management within the AML/CFT compliance function and senior compliance personnel within the individual business

lines should have the appropriate authority, independence and access to personnel and information within the organization and appropriate resources to conduct their activities effectively.

The board should ensure that its views about the importance of AML/CFT compliance are understood and communicated across all levels of the financial institution. The board also should ensure that senior management has established appropriate incentives to integrate AML/CFT compliance objectives into management goals and compensation structure across the organization, and that corrective actions, including disciplinary measures, if appropriate, are taken when serious AML/CFT compliance failures are identified.

Senior management

Senior management is responsible for communicating and reinforcing the AML/CFT compliance culture established by the board, and implementing and enforcing the board-approved AML/CFT Compliance Program. If the financial institution has a separate AML/CFT compliance function, the senior management is required to establish, support and oversee the institution's AML/CFT Compliance Program. **AMLCFT chief compliance officer should report to the board or a committee thereof on effectiveness of the AML/CFT, Compliance Program and significant AML/CFT compliance matters.**

Senior management of a foreign owned financial institution is required to provide sufficient AML/CFT compliance information relating to its Nigerian operations to the board/senior management and control unit in its home country. It should also ensure that responsible senior management in the home country has an appropriate understanding of the Nigerian AML/CFT risk and control environment governing its Nigeria operations. The management of such Nigerian financial institution should assess the effectiveness of established AML/CFT control mechanisms for Nigerian operations on an on-going basis, report and escalate areas of concern as needed. As appropriate, corrective action then should be developed and implemented.

Consolidated AML/CFT compliance programs

Financial institutions that centrally manage the operations and functions of their subsidiary financial institutions, other subsidiaries and business lines should ensure **that comprehensive risk management policies, procedures and processes are in place across the organization to address the entire organization's spectrum of risk.** An adequate consolidated AML/CFT Compliance Program provides the framework for all subsidiaries, business lines and foreign branches to meet their specific regulatory requirements (e.g., country or industry requirements). Accordingly, financial institutions that centrally manage a consolidated AML/CFT Compliance Program should, among other things, provide appropriate structure and advise the business lines, subsidiaries and foreign branches on the development of appropriate guidelines.

An organization applying a consolidated AML/CFT Compliance Program may choose to manage only specific compliance controls (e.g. STR monitoring systems & audit) on a consolidated basis, with other compliance controls managed solely within affiliates, subsidiaries and business lines. **When this approach is taken, Examiners must identify which portions of the AML/CFT Compliance Program are part of the consolidated AML/CFT Compliance Program**. This information is critical when scoping and planning an AML/CFT examination.

When evaluating a consolidated AML/CFT Compliance Program for adequacy, the Examiner should determine reporting lines and how each affiliate, subsidiary, business line and jurisdiction fit into the overall compliance structure. This should include an assessment of how clearly roles and responsibilities are communicated across the financial institution.

Assess the effectiveness of how the financial institution or entire organization monitors AML/CFT compliance

The evaluation of a consolidated AML/CFT Compliance Program should take into consideration available information about the adequacy of the individual subsidiaries AML/CFT Compliance Program. Regardless of the decision to implement a consolidated AML/CFT Compliance Program in whole or in part, the program should ensure that all affiliates, including those operating within foreign jurisdictions meet their applicable regulatory requirements. For example, an audit program implemented solely on a consolidated basis that does not conduct appropriate transaction testing at all subsidiaries subject to the Money Laundering Prohibition Act, CBN AML/CFT Regulation 2009, etc would not be sufficient to meet regulatory requirements for independent testing for those subsidiaries.

37. SUSPICIOUS TRANSACTION REPORTING

Financial institution's holding companies (FIHC) or any non-bank subsidiary thereof, or a foreign owned financial institution that is subject to the BOFI Act or any non-bank subsidiary of such a foreign owned financial institution operating in Nigeria, are required to file STRs. A FIHC's non-bank subsidiaries operating only outside Nigeria are also required to file STRs. Certain savings and loan holding companies and their non depository subsidiaries are required to file STRs pursuant to CBN AML/CFT Regulations 2009. In addition, savings and loan holding companies are strongly required to file STRs.

38. EXAMINATION PROCEDURES FOR AML/CFT COMPLIANCE PROGRAM STRUCTURES

Objective

Assess the structure and management of the financial institution's AML/CFT Compliance Program and (if applicable) its consolidated or partially consolidated approach to

AML/CFT compliance. An AML/CFT Compliance Program may be structured in a variety of ways and an Examiner should perform procedures based on the structure of the institution. **Completion of these procedures may require communication with other regulators.**

1. Review the structure and management of the AML/CFT Compliance Program. Communicate with peer regulators, if necessary, to confirm their understanding of the institution's AML/CFT Compliance Program. This approach promotes consistent supervision and lessens regulatory burden for financial institution. **Determine the extent to which the structure of the AML/CFT Compliance Program affects the institution being examined, by considering:**

   i. The existence of consolidated or partially consolidated operations or functions responsible for day-to-day AML/CFT operations, including, but not limited to, the centralization of suspicious transaction monitoring and reporting, currency transaction reporting,(CTR) or recordkeeping activities.
   ii. The consolidation of operational units dedicated to and responsible for monitoring transactions across activities, business lines or legal entities. Assess the variety and extent of information that data or transaction sources (e.g., banks/other financial institutions, broker/dealers, trust companies, agreement corporations, insurance companies, or foreign branches) are entering into the monitoring and reporting systems.
   iii. The extent to which the financial institution (or a corporate-level unit, such as audit or compliance) performs regular independent testing of AML/CFT activities.
   iv. Whether and to what extent a corporate-level unit sponsors AML/CFT training.

2. Review testing for AML/CFT compliance throughout the financial institution, as applicable, and identify program deficiencies.
3. Review board minutes to determine the adequacy of MIS and of reports provided to the board of directors. Ensure that the board of directors has received appropriate notification of STRs filed.
4. Review policies, procedures, processes and risk assessments formulated and implemented by the institution's board of directors, a board committee thereof or senior management. **As part of this review, assess effectiveness of the institution's ability to perform the following responsibilities:**

   i. Manage the AML/CFT Compliance Program and provide adequate oversight.
   ii. Set and communicate corporate standards that reflect the expectations of the institution's board of directors and provide for clear allocation of AML/CFT compliance responsibilities.
   iii. Promptly identify and effectively measure, monitor and control key risks throughout the institution.
   iv. Develop an adequate risk assessment and the policies, procedures and processes to comprehensively manage those risks.

v. Develop procedures for evaluation, approval and oversight of risk limits, new business initiatives and strategic changes.
vi. Oversee the compliance of subsidiaries with applicable regulatory requirements (e.g., country and industry requirements).
vii. Oversee the compliance of subsidiaries with the requirements of the AML/CFT Compliance Program.
viii. Identify weaknesses in the AML/CFT Compliance Program and implement necessary and timely corrective action at both the institutional and subsidiary levels.

5. To ensure compliance with regulatory requirements, review the financial institution's procedures for monitoring and filing STRs.
6. Once the Examiners have completed the above procedures, they should discuss their findings with the following parties, as appropriate:
   i. Examiner in charge.
   ii. Person (or persons) responsible for on-going supervision of the institution and subsidiary financial institutions, as appropriate
   iii. Corporate management.
   iv. On the basis of examination procedures completed, form a conclusion about the adequacy of the AML/CFT Compliance Program structures and management including, if applicable, the effectiveness of the consolidated or partially consolidated approach to compliance.

39. OVERVIEW OF FOREIGN BRANCHES AND OFFICES OF NIGERIAN FINANCIAL INSTITUTIONS

Objective

Assess the adequacy of the Nigerian financial institution's systems to manage the risks associated with its foreign branches and offices, and management's ability to implement effective monitoring and reporting systems.

Nigerian financial institutions open foreign branches and offices to meet specific customer demands, to help the financial institution grow, or to expand products or services offered. Foreign branches and offices vary significantly in size, complexity of operations, and scope of products and services offered. Examiners must take these factors into consideration when reviewing the foreign branches and offices AML/CFT Compliance Program. Financial institutions are expected to have policies, procedures and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. AML/CFT policies, procedures and processes at the foreign office or branch should comply with local requirements and be consistent with the Nigerian financial institution's standards; however, they may need to be tailored for local or business practices.

Risk factors

Examiners should understand the type of products and services offered at foreign branches and offices, as well as the customers and geographic locations served at the foreign branches and offices. Any service offered by the Nigerian financial institution may be offered by the foreign branches and offices if not prohibited by the host country. Such products and services offered at the foreign branches and offices may have a different risk profile from that of the same products or services offered in Nigerian. Therefore, the Examiner should be aware that risks associated with foreign branches and offices may differ (e.g., wholesale versus retail operations).
The Examiner should understand the foreign jurisdiction's various AML/CFT requirements. Secrecy laws or their equivalent may affect the ability of the foreign branch or office to share information with the Nigerian financial institutions parent institution, or the ability of the Examiner to examine on-site. While financial institution with overseas branches or subsidiaries may find it necessary to tailor monitoring approaches as a result of local privacy laws, the compliance oversight mechanism should ensure it can effectively assess and monitor risks within such branches and subsidiaries. Although specific MLPA requirements are not applicable at foreign branches and offices, financial institutions are expected to have policies, procedures and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. In this regard, foreign branches and offices should be guided by the Nigerian financial institutions' AML/CFT policies, procedures and processes. The foreign branches and offices must comply with applicable provisions of Money Laundering Prohibition Act (MLPA), AML/CFT Regulation requirements and all other local AML/CFT related laws, rules and regulations.

Risk mitigation

Branches and offices of Nigerian financial institutions located in higher-risk geographic locations may be vulnerable to abuse by money launderers. To address this concern, the **Nigerian financial institution's policies, procedures and processes for the foreign operation should be consistent with the following recommendations:**

i. The Nigerian financial institution's head office and management in Nigeria & the one at the foreign country should understand the effectiveness and quality of supervision and the legal and regulatory requirements of the host country. The Nigerian financial institution's head office should be aware of and understand any concerns that the host country supervisors may have with respect to the foreign branch or office.
ii. The Nigerian financial institution's head office should understand the foreign branches' or offices' risk profile (e.g., products, services, customers and geographic locations).
iii. The Nigerian financial institution's head office and management should have access to sufficient information in order to periodically monitor the activity of their foreign branches and offices, including the offices' and branches' level of

compliance with head office policies, procedures and processes. Some of this may be achieved through MIS reports.

The Nigerian financial institution's head office should develop a system for testing and verifying the integrity and effectiveness of internal controls at the foreign branches or offices by conducting in-country audits. Senior management at the head office should obtain and review copies (written in English) of audit reports and any other reports related to AML/CFT and internal control evaluations.

iv. The Nigeria financial institution's head office should establish robust information-sharing practices between branches and offices, particularly regarding higher-risk account relationships. The institution should use the information to evaluate and understand account relationships throughout the corporate structure (e.g., across borders or legal structures).
v. The Nigerian institution's head office should be able to provide Examiners with any information deemed necessary to assess compliance with the applicable laws.

Foreign branch and office compliance and audit structures can vary substantially based on the scope of operations (e.g., geographic locations) and the type of products, services and customers. Foreign branches and offices with multiple locations within a geographic region are frequently overseen by branch compliance and audit staff. Regardless of the size or scope of operations, the compliance and audit staff and audit programs should be sufficient to oversee ML/FT risk.

40. SCOPING OF AML/CFT EXAMINATIONS OF FOREIGN BRANCHES & OFFICES

Examinations may be completed in the host country or in Nigeria. **The factors that will be considered in deciding whether the examination work should occur in the host jurisdiction or Nigeria include:**

i. The risk profile of the foreign branch or office and whether the profile is stable or changing as a result of a reorganization, the introduction of new products or services, or other factors, including the risk profile of the jurisdiction itself.
ii. The effectiveness and quality of financial institution supervision in the host country.
iii. Existence of an information-sharing arrangement between the host country and the Nigerian supervisor.
iv. The history of examination or audit concerns at the foreign branch or office.
v. The size and complexity of the foreign branch's or office's operations.
vi. Effectiveness of internal controls, including systems for managing AML/CFT risks on a consolidated basis and internal audit.

vii. The capability of management at the foreign branch or office to protect the entity from money laundering or terrorist financing.
viii. The availability of the foreign branch or office records in Nigeria.

In some jurisdictions, financial secrecy and other laws may prevent or severely limit Nigerian Bank Examiners or Nigerian head office staff from directly evaluating customers' transactions or records. In cases when an on-site examination cannot be conducted effectively, Examiners should consult with the relevant/appropriate regulatory authority. In such cases, regulatory authority personnel may contact the counterpart foreign supervisors to make appropriate information sharing or examination arrangements. In lower-risk situations when information is not restricted, Examiners may conduct Nigerian -based examinations.

In higher-risk situations when adequate examinations (on-site or otherwise) cannot be effected, the CBN alone or in conjunction with the relevant regulatory agency may require the head office to take action to address the situation, which may include closing the foreign office.

Nigerian- based examinations

Nigerian-based but off-site the foreign office examinations generally require greater confidence in the AML/CFT program at the foreign branch or office as well as the ability to access sufficient records.

Such off-site examinations should include discussions with the senior financial institution management at the head and foreign office. These discussions are crucial to the understanding of the foreign branches' or offices' operations, AML/CFT risks and its programs. Also, the examination of the foreign branch or office should include a review of the Nigerian financial institution's involvement in managing or monitoring the foreign branch's operations, internal control systems (e.g., policies, procedures and monitoring reports) and, where available, the host country supervisors' examination findings, audit findings and work-papers. As with all AML/CFT examinations, the extent of transaction testing and activities where it is performed is based on various factors including the Examiner's judgment of risks, controls and the adequacy of the independent testing.

Host jurisdiction-based examinations

On-site work in the host jurisdiction enables Examiners not only to better understand the role of the Nigerian financial institution in relation to its foreign branch or office but also, perhaps more importantly, permit the Examiners to determine the extent to which the global policies, procedures and processes are being followed locally.
The standard scoping and planning process will determine the focus of the examination and the resource needs. There may be some differences in the examination process conducted abroad. The host supervisory authority may send an Examiner to join the Nigerian team or request attendance at meetings at the beginning and at the conclusion of the examination. AML/CFT reporting requirements also are likely to be different, as they will be adjusted to local regulatory requirements.

For both Nigerian-based and host-based examinations of foreign branches and offices, the procedures used for specific products, services, customers and entities are those found in this **AML/CFT Risk-Based Manual.** For example, if an Examiner is looking at pouch activities at foreign branches and offices, he or she should use the applicable expanded examination procedures.

41. EXAMINATION PROCEDURES OF FOREIGN BRANCHES AND OFFICES OF NIGERIAN FINANCIAL INSTITUTIONS

Objective

Assess the adequacy of the Nigerian financial institution's systems to manage the risks associated with its foreign branches and offices, and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to foreign branches and offices to evaluate their adequacy given the activity in relation to the institution's risk, and assess whether the controls are adequate to reasonably protect the institution from money laundering and terrorist financing.
2. On the basis of a review of MIS and internal risk rating factors, determine whether the Nigerian financial institution's head office effectively identifies and monitors foreign branches and offices, particularly those conducting higher-risk transactions or located in higher-risk jurisdictions.
3. Determine whether the Nigerian financial institution's head office system for monitoring foreign branches and offices and detecting unusual or suspicious activities at those branches and offices is adequate given the institution's size, complexity, location and types of customer relationships. Determine whether the host country requires filing STRs. If permitted and available, review those reports. Determine whether the information provided to the Nigeria financial institution's head office filters into the institution-wide or, if appropriate, the organization-wide assessment of STRs.
4. Review the financial institution's organizational structure reports, which should include a list of all legal entities and the countries in which they are registered. Determine the locations of foreign branches and offices, including the foreign regulatory environment and the degree of access by Nigerian regulators for on-site examinations and customer records.
5. Review any partnering or outsourcing relationships of foreign branches and offices. Determine whether the relationship is consistent with the institution's AML/CFT Program.
6. Determine the type of products, services, customers, entities and geographic locations served by the foreign branches and offices. Review the risk assessments of the foreign branches and offices.
7. Review the management, compliance and audit structure of the foreign branches and offices. Identify the decisions that are made at the financial institution's Nigerian head office level versus those that are made at the foreign branch or office.

8. Determine the involvement of the Nigerian financial institution's head office in managing and monitoring foreign branches and offices. Conduct a preliminary evaluation of the foreign branches or offices through discussions with senior management at the Nigerian financial institution's head office **(e.g., operations, customers, entities, jurisdictions, products, services, management strategies, audit programs, anticipated product lines, management changes, branch expansions, AML/CFT risks and its programs).** Similar discussions should occur with management of the foreign branches and offices, particularly those that may be considered higher risk.
9. Coordinate with the host country supervisor and, if applicable, the host FIU. Discuss their assessment of the foreign branches' and offices' compliance with the local laws and Nigerian laws and regulations like MLPA and CBN AML/CFT Regulation 2009. Determine whether there are any restrictions on materials that may be reviewed, copied, or taken out of the country.
10. If available, review the previous regulatory examination reports, host country's regulatory examination report, audit reports and supporting documentation, compliance reviews and supporting documentation.
11. If appropriate, refer to the core examination procedures.

Transaction testing

12. Make a determination whether transaction testing is feasible. If feasible, on the basis of the financial institution's risk assessment of its activity, prior examination and audit reports, select a sample of higher-risk foreign branch and office activity. Complete transaction testing from appropriate expanded examination procedures sections.
13. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with the Nigerian bank's foreign branches and offices.

42. OVERVIEW OF PARALLEL BANKING

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with parallel banking relationships and the management's ability to implement effective due diligence, monitoring and reporting systems.

A parallel financial institution exists when at least one Nigerian financial institution and one foreign financial institution are controlled either directly or indirectly by the same person or group of persons who are closely associated in their business dealings or otherwise acting together, but are not subject to consolidated supervision by a single home country supervisor. The foreign financial institution will be subject to different money laundering rules and regulations and a different supervisory oversight structure, both of which may be less stringent than Nigeria. The regulatory and supervisory

differences heighten the AML/CFT risk associated with parallel banking organizations.

Risk factors

Parallel banking organizations may have common management, share policies and procedures, cross-sell products, or generally be linked to a foreign parallel financial institution in a number of ways. The key money laundering concern regarding parallel banking organizations is that the Nigerian financial institution may be exposed to greater risk through transactions with the foreign parallel financial institution. Transactions may be facilitated and risks heightened because of the lack of arm's length dealing or reduced controls on transactions between financial institutions that are linked or closely associated. **For example, officers or directors may be common to both entities or may be different but nonetheless work together.**

Risk mitigation

The Nigerian financial institution's policies, procedures and processes for parallel banking relationships should be consistent with those of other foreign correspondent bank relationships. **In addition, parallel financial institutions should:**

i. Provide for independent lines of decision-making authority.
ii. Guard against conflicts of interest.
iii. Ensure independent and arm's-length dealings between related entities.

43. EXAMINATION PROCEDURES OF PARALLEL BANKING

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with parallel banking relationships, and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Determine whether parallel banking relationships exist through discussions with management or by reviewing inter-party activities involving the financial institution and another foreign financial institution. Review the policies, procedures and processes related to parallel banking relationships. Evaluate the adequacy of the policies, procedures and processes given the financial institution's parallel banking activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. Determine whether there are any conflicts of interest or differences in policies, procedures and processes between parallel banking relationships and other foreign correspondent bank/other financial institution relationships. Particular consideration should be given to funds transfer, pouch and payable through activities because these activities are more vulnerable to money laundering. If

the financial institution engages in any of these activities, Examiners should consider completing applicable expanded examination procedures that address each of these topics.

3. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors parallel banking relationships, particularly those that pose a higher-risk for money laundering.
4. Determine whether the financial institution's system for monitoring parallel banking relationships for STRs, and for reporting suspicious transaction is adequate given the FI's size, complexity, location and types of customer relationships.

Transaction testing

5. On the basis of the financial institution's risk assessment of its parallel banking activities, as well as prior examination and audit reports, select a sample of higher-risk activities from parallel banking relationships (e.g., foreign correspondent banking, funds transfer, payable through accounts and pouch).
6. Consider the location of the foreign parallel financial institution. If the jurisdiction is higher risk, Examiners should review a larger sample of transactions between the two institutions. Financial institutions doing business with parallel foreign banking organizations in countries not designated as higher risk may still require EDD, but that determination will be based on the size, nature and type of the transactions between the institutions.
7. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with parallel banking organizations. Focus on whether controls exist to ensure independent and arm's-length dealings between the two entities. If significant concerns are raised about the relationship between the two entities, recommend that this information be forwarded to the appropriate supervisory authorities.

44. EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PRODUCTS AND SERVICES

45. OVERVIEW OF CORRESPONDENT ACCOUNTS (DOMESTIC)

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with offering of domestic correspondent account relationships, and ability of the management to implement effective monitoring and reporting systems.

Financial institutions maintain correspondent relationships at other domestic financial institutions to provide certain services that can be performed more economically or

efficiently because of the other financial institution's size, expertise in a specific line of business or geographic location. **Such services may include:**

i. **Deposit accounts -** Assets known as "due from financial institution deposits" or "correspondent financial institution balances" may represent the financial institution's primary operating account.

ii. **Funds transfers -** A transfer of funds between financial institutions may result from the collection of cheques or other cash items, transfer and settlement of securities transactions, transfer of participating loan funds, purchase or sale of government funds, or processing of customer transactions.

iii. **Other services -** Services include processing of loan participations, facilitating secondary market loan sales, performing data processing and payroll services and exchanging foreign currency.

ML/FT Risk Factors

Because domestic financial institutions must follow the same regulatory requirements, ML/FT risks in domestic correspondent banking are minimal in comparison to other types of financial services, especially for proprietary accounts (i.e., the domestic financial institution is using the correspondent account for its own transactions). Each financial institution, however, has its own approach for conducting its AML/CFT Compliance Program, including customer due diligence, MIS, account monitoring, and reporting suspicious transactions. Furthermore, while a domestic correspondent account may not be considered higher risk, transactions through the account, which may be conducted on behalf of the respondent's customer, may be higher risk. AML/CFT risks can be heightened when a respondent financial institution allows its customers to direct or execute transactions through the correspondent account, especially when such transactions are directed or executed through an ostensibly proprietary account.

The correspondent financial institution also faces heightened risks when providing direct currency shipments for customers of respondent financial institution. This is not to imply that such activities necessarily entail money laundering, but these **direct currency shipments should be appropriately monitored for unusual and suspicious activity. Without such a monitoring system, the correspondent bank is essentially providing these direct services to an unknown customer.**

Risk Mitigation

Financial institutions that offer correspondent bank services to respondent banks should have policies, procedures and processes to manage the AML/CFT risks involved in these correspondent relationships and to detect and report suspicious activities. **Financial institution should ascertain whether domestic correspondent accounts are proprietary or allow third-party transactions.** When the respondent financial institution allows third-party customers to transact business through the correspondent account, t**he correspondent financial institution should ensure that it puts the necessary steps in understanding the due diligence and procedures of the**

monitoring applied by the respondent on its customers that will be utilizing the account.

The level of risk varies depending on the services provided and the types of transactions conducted through the account and the respondent financial institution's AML/CFT Compliance Program, products, services, customers, entities and geographic locations. Each financial institution should appropriately monitor transactions of domestic correspondent accounts relative to the level of assessed risk.

46. EXAMINATION PROCEDURES OF CORRESPONDENT ACCOUNTS (DOMESTIC)

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with offering domestic correspondent account relationships, and ability of the management to implement effective monitoring and reporting systems.

1. Review the policies, procedures, processes and any financial institution's service agreements related to domestic correspondent banking relationships. Evaluate the adequacy of the policies, procedures and processes given the financial institution's domestic correspondent accounts and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the bank has identified any domestic correspondent banking activities as higher risk.
3. Determine whether the financial institution's system for monitoring domestic correspondent accounts for suspicious transactions and for reporting such suspicious transactions are adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's review of respondent accounts with unusual or higher-risk activity, its risk assessment and prior examination and audit reports, select a sample of respondents' accounts. **From the sample selected, perform the following examination procedures:**

    i. Review financial institution statements for domestic correspondent accounts.
    ii. Review large or unusual transactions to determine their nature. As necessary, obtain and review copies of credit or debit advices and other supporting documentation

iii. Note any currency shipments or deposits made on behalf of a respondent financial institution's customer. Based on this information determine whether:
   a. Currency shipments are adequately documented.
   b. The respondent financial institution has performed due diligence on customers that conduct large currency transactions.
   c. CTRs are properly filed and transaction is commensurate with how it is expected.

5. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes that are associated with domestic correspondent financial institution's relationships.

47. OVERVIEW OF CORRESPONDENT ACCOUNTS (FOREIGN)

Objective

Assess the adequacy of the Nigerian financial institution's systems to manage the ML/FT risks associated with foreign correspondent banking and ability of the management to implement effective due diligence, monitoring and reporting systems. This section expands the earlier core review of statutory and regulatory requirements of foreign correspondent account relationships in order to provide a broader assessment of the ML/FT risks associated with this activity.

Foreign financial institutions maintain accounts at Nigerian financial institutions to gain access to the Nigerian financial system and to take advantage of services and products that may not be available in the foreign financial institution's jurisdiction. These services may be performed more economically or efficiently by the Nigerian financial institutions or may be necessary for other reasons, such as the facilitation of international trade.

International trade services

i. Cash management services, including deposit accounts.
ii. International funds transfers.
iii. Check clearing.
iv. Payable through accounts.
v. Pouch activities.
vi. Foreign exchange services.
vii. Overnight investment accounts (sweep accounts).
viii. Loans and letters of credit.

Contractual Agreements

Each relationship that a Nigerian financial institution has with a foreign correspondent financial institution should be governed by an agreement or a contract describing each party's responsibilities and other relationship details (e.g., products and services provided, acceptance of deposits, clearing of items, forms of payment and acceptable forms of endorsement). The agreement or contract should also consider the foreign financial institution's AML/CFT regulatory requirements, customer-base, due diligence procedures and permitted third-party usage of the correspondent account.

ML/FT Risk Factors

Some foreign financial institutions are not subject to the same or similar regulatory guidelines as Nigerian financial institutions; therefore, these foreign institutions may pose a higher money laundering and financing terrorists risk to their respective Nigerian financial institutions correspondent(s). Investigations have disclosed that in the past, foreign correspondent accounts were used to launder funds.

Shell companies are sometimes used in the layering process to hide the true ownership of accounts at foreign correspondent financial institutions. Because of the large amount of funds, multiple transactions, and the Nigerian financial institution's potential lack of familiarity with the foreign correspondent financial institution's customer, criminals and terrorists can more easily conceal the source and use of illicit funds. **Consequently, each Nigerian financial institution, including all overseas branches, offices and subsidiaries should closely monitor transactions related to foreign correspondent accounts.**

Nested Accounts

Nested accounts occur when one foreign financial institution gains access to the financial system in Nigeria by operating through the correspondent account belonging to another foreign financial institution.

If the Nigerian financial institution is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the Nigerian financial system. Behaviour indicative of nested accounts and other accounts of concern includes transactions in jurisdictions in which the foreign financial institution has no known business activities or interests and transactions in which the total volume and frequency significantly exceed expected activity for the foreign financial institution, considering its customer base or asset size.

Risk Mitigation

Nigerian financial institutions that offer foreign correspondent financial institution services should have policies, procedure, and processes to manage the ML/FT risks inherent with these relationships and should closely monitor transactions related to these accounts to detect and report suspicious transactions. The level of risk varies depending on the foreign financial institution's products, services, customers and geographic locations. **The Nigerian financial institutions' policies, procedures and processes should:**

i. Specify appropriate account-opening procedures and KYC requirements, which may include minimum levels of documentation to be obtained from prospective customers; an account approval process independent of the correspondent account business line for potential higher-risk customers; and a description of circumstances when the financial institution will not open an account.
ii. Assess the risks posed by a prospective foreign correspondent customer relationship utilizing consistent, well-documented risk-rating methodologies, and incorporate that risk determination into the financial institution's suspicious transaction monitoring system.
iii. Understand the intended use of the accounts and expected account activity (e.g., determine whether the relationship will serve as a payable through account).
iv. Understand the foreign correspondent financial institution's other correspondent relationships (e.g., determine whether nested accounts will be utilized).
v. Conduct adequate and ongoing due diligence on the foreign correspondent financial institution relationships, which may include periodic visits.
vi. Establish a formalized process for escalating suspicious information on potential and existing customers to an appropriate management level for review.
vii. Ensure that foreign correspondent financial institution relationships are appropriately included within the Nigerian financial institution's suspicious transaction monitoring and reporting systems.
viii. Ensure that appropriate due diligence standards are applied to those accounts determined to be higher risk.
ix. Establish criteria for closing the foreign correspondent financial institution account.

As a sound practice, Nigerian financial institutions are encouraged to communicate their AML/CFT-related expectations to their foreign correspondent financial institutions' customers. Moreover, the Nigerian financial institutions should generally understand the AML/CFT controls at the foreign correspondent financial institution, including customer due diligence practices and record keeping documentation.

48. EXAMINATION PROCEDURES OF CORRESPONDENT ACCOUNTS (FOREIGN)

Objective

Assess the adequacy of the Nigerian financial institution's systems to manage the ML/FT risks associated with foreign correspondent banking and ability of the management to implement effective due diligence, monitoring and reporting systems. This section expands the earlier core review of statutory and regulatory requirements of foreign correspondent account relationships in order to provide a broader assessment of the ML/FT risks associated with this activity.

1. Review the policies, procedures and processes related to foreign correspondent financial institution account relationships. Evaluate the adequacy of the policies, procedures and processes. Assess whether the controls are adequate to reasonably protect the Nigerian financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk-rating factors, determine whether the Nigerian financial system effectively identifies and monitors foreign correspondent financial institution account relationships, particularly those that pose a higher risk for money laundering.
3. If the Nigerian financial system has a standardized foreign correspondent agreement, review a sample agreement to determine whether each party's responsibilities, products and services provided and allowable third party usage of the correspondent account are covered under the contractual arrangement. If the Nigerian financial institution does not have a standardized agreement, refer to the transaction testing examination procedures.
4. Determine whether the Nigerian financial institution's system for monitoring foreign correspondent financial institution account relationships for suspicious transactions and for reporting such suspicious transactions are adequate given the Nigerian financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

5. On the basis of the Nigerian financial institution's risk assessment of its foreign correspondent activities as well as prior examination and audit reports, select a sample of higher-risk foreign correspondent financial institution account relationships. The higher-risk sample should include relationships with foreign financial institutions located in jurisdictions that do not cooperate with international AML/CFT efforts and in other jurisdictions that the Nigerian financial institution has determined to pose a higher risk. From the sample selected, perform the following examination procedures:

    i. Review a foreign correspondent agreement or contract that delineates each party's responsibilities and the products and services provided.
    ii. Review Nigerian financial institution's statements for foreign correspondent accounts and as necessary, specific transaction details. Compare expected transactions with actual activity.
    iii. Determine whether actual activity is consistent with the nature of the customer's business. Identify any unusual or suspicious transaction.
    iv. Review large or unusual transactions to determine their nature. As necessary, obtain and review copies of credit or debit advices, general ledger tickets and other supporting documentation.
    v. Analyze transactions to identify behavior indicative of nested accounts, intermediary or clearing agent services or other services for third-party foreign financial institutions that have not been clearly identified

5 On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with foreign correspondent financial institution relationships.

49. OVERVIEW OF BULK SHIPMENTS OF CURRENCY

Objective

Assess the adequacy of the Nigerian financial institution's systems to manage the risks associated with receiving bulk shipments of currency and management's implementation of effective monitoring and reporting systems.

Bulk shipments of currency entail the use of common, independent, or Postal Service's air/land/sea carriers to transport large volumes of bank notes (Nigeria or foreign) from sources either inside or outside Nigeria to a bank in Nigeria. Often, but not always, shipments take the form of containerized cargo.

Shippers may be **"Currency Originators" i.e., individuals or businesses that generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency).**

Shippers also may be **"intermediaries" that ship currency gathered from their customers who are Currency Originators.** Intermediaries may also ship currency gathered from other intermediaries. Intermediaries may be other financial institutions, central banks, non-deposit financial institutions or agents of these entities.

Financial institutions receive bulk shipments of currency directly when they take possession of an actual shipment. Financial institutions receive bulk shipments of currency indirectly when they take possession of the economic equivalent of a currency shipment, such as through a cash letter notification.

Risk Factors

Bulk shipments of currency to financial institutions from shippers that are presumed to be reputable may nevertheless originate from illicit activity. The monetary proceeds of criminal activities, for example, often reappear in the financial system as seemingly legitimate funds that have been placed and finally integrated by flowing through numerous intermediaries and layered transactions that disguise the origin of the funds. Layering can include shipments to or through other jurisdictions. **Accordingly, financial institutions that receive direct or indirect bulk shipments of currency risk becoming complicit in money laundering or terrorist financing schemes.**

In recent years, the smuggling of bulk currency has become a preferred method for moving illicit funds across borders. However, the activity of shipping currency in bulk is not necessarily indicative of criminal or terrorist activity. Many individuals and businesses, both domestic and foreign, generate currency from

legitimate cash sales of commodities or other products or services. Also, intermediaries gather and ship currency from single or multiple currency originators whose activities are legitimate. Financial institutions may legitimately offer services to receive such shipments. However, financial institutions should be aware of the potential misuse of their services by shippers of bulk currency. Financial institutions also should guard against introducing the monetary proceeds of criminal or terrorist activity into the financial system.

Risk Mitigation

Nigerian financial institutions that offer services to receive bulk shipments of currency should have policies, procedures and processes in place that mitigate and manage the ML/FT risks associated with the receipt of bulk currency shipments. Financial institutions should also closely monitor bulk currency shipment transactions to detect and report suspicious transaction, with particular emphasis on the source of funds and the reasonableness of transaction volumes from currency originators and intermediaries.

ML/FT risk mitigation begins with an effective risk assessment process that distinguishes relationships and transactions that present a higher risk of money laundering or terrorist financing. Risk assessment processes should consider currency originator's and intermediary's ownership, geographies and the nature, source, location and control of bulk currency.

Financial institution's policies, procedures and processes

i. Specify appropriate ML/FT risk-based relationship & account opening procedures which may include minimum levels of documentation to be obtained from prospective currency originators and intermediaries; specify relationship approval process that, for potential higher-risk relationships, is independent of the business line and may include a visit to the prospective shipper or shipping-preparation sites; and describe the circumstances under which the financial institution will not open a relationship.

ii. Determine the intended use of the relationship, the expected volumes, frequency of activity arising from transactions, sources of funds, reasonableness of volumes based on originators and shippers and any reporting requirements (CTRs, STRs, PEPs, etc).

iii. Identify the characteristics of acceptable and unacceptable transactions, including circumstances when the bank will or will not accept bulk currency shipments.

iv. Assess the risks posed by a prospective shipping relationship using consistent and well-documented risk-rating methodologies.

v. Incorporate risk assessments, as appropriate, into the financial institution's customer due diligence, EDD and suspicious transaction monitoring systems.

vi. Once the relationship is established, require adequate and ongoing due diligence which, as appropriate, may include periodic visits to the shipper and to shipping-preparation sites. As necessary, scrutinize for legitimacy the root source of cash shipments, using risk-based processes.

vii. Ensure that appropriate due diligence standards are applied to relationships determined to be higher risk.

viii. Include procedures for processing shipments, including employees' responsibilities, controls, reconciliation and documentation requirements, and employee/management authorizations.

ix. Establish a process for escalating suspicious information on potential and existing currency originator and intermediary relationships and transactions to an appropriate management level for review.

x. Refuse shipments that have questionable or suspicious origins.

xi. Ensure that shipping relationships and comparisons of expected and actual shipping volumes are included, as appropriate, within the Nigerian financial institution's systems for monitoring and reporting suspicious transaction.

xii. Establish criteria for terminating a shipment relationship.

As a sound practice, Nigerian financial institutions should inform currency originators and intermediaries of the AML/CFT-related requirements and expectations that apply to Nigerian financial institutions. Nigerian financial institutions also should understand the AML/CFT controls that apply to or are otherwise adopted by the currency originator or intermediary, including any customer due diligence and recordkeeping requirements or practices.

Other financial institutions' controls may also prove useful in protecting financial institution against illicit bulk shipments of currency. These may include effective controls over foreign correspondent banking activity, pouch activity, funds transfers, international automated clearing house transactions and remote deposit capture.

Contractual Agreements

Nigerian financial institutions should establish agreements or contracts with currency originators or intermediaries. The agreement or contract should describe each party's responsibilities and other relevant details of the relationship. The agreement or contract should reflect and be consistent with any AML/CFT considerations that apply to the financial institution, the currency originator or intermediary and the currency originator or intermediary's customers. The agreement or contract should also address expectations about due diligence and permitted third-party usage of the shipper's services. While agreements and contracts should provide for respective AML/CFT controls, obligations and considerations, Nigerian financial institutions cannot shift their AML/CFT responsibilities to others.

50. EXAMINATION PROCEDURES OF BULK SHIPMENTS OF CURRENCY

Objective

Assess the adequacy of the Nigerian financial institution's systems to manage the ML/FT risks associated with receiving bulk shipments of currency, and ability of the management to implement effective due diligence, monitoring and reporting systems.

1. Determine whether the financial institution receives shipments of bulk currency.
2. Review for adequacy the policies, procedures and processes related to receiving shipments of bulk currency, given the activity and the risks presented.
3. Review the list of currency originators and intermediaries that send bulk currency shipments to the financial institution.
4. Determine whether management has assessed the risks associated with receiving bulk currency shipments from particular currency originators and intermediaries. Consider the source of the currency originator's or intermediary's currency and the reasonableness of transaction volumes. Assess the adequacy of the risk-assessment methodology.
5. From a review of MIS and internal risk-rating factors, determine whether the financial institution effectively identifies and monitors relationships with currency originators and intermediaries, particularly those that pose a higher risk for money laundering or terrorist financing.
6. If the financial institution has a standardized agreement or contract with currency originators or intermediaries, review a sample agreement or contract to determine whether each party's responsibilities, products and services provided allow third-party usage of the relationship, including the parties' AML/CFT responsibilities are covered. If the financial institution does not have a standardized agreement or contract, refer to the transaction testing examination procedures below.
7. Determine whether the financial institution's system for monitoring and reporting suspicious transactions related to shipping relationships and transactions is adequate given the financial institution's size, complexity, location and types of customer relationships.
8. Determine whether the financial institution is monitoring expected or actual shipping volumes and taking action in response to unusual or inordinate increase in volumes.

Transaction Testing

9. Based on the financial institution's risk assessment of its relationships with currency originators and intermediaries, as well as prior examination and audit reports, select a sample of currency originators or intermediaries and recent bulk currency shipments. The sample should include relationships with currency originators and intermediaries located in or shipping from jurisdictions that may pose a higher risk

for money laundering and terrorist financing, or that participate in businesses that may pose a higher risk for money laundering and terrorist financing.

10. Preferably on an unannounced basis and over a period of several days, observe the process for accepting shipments of bulk currency. Review the records and the shipments for irregularities.

From the samples selected, perform the following examination procedures:

i. Review for completeness a relationship agreement or contract that delineates each party's responsibilities and the products and services provided.

ii. Review Nigeria bank's statements of accounts and, as necessary, specific transaction details.

iii. Review vault control records for bulk currency shipment transactions (in and out) to identify large denomination activity as a result of small denomination exchanges.

iv. Assess the reasonableness of customer due diligence and EDD information pertaining to the sampled currency originators and intermediaries.

v. Determine whether the nature, volume and frequency of activity is consistent with the expectations associated with the currency originator and intermediary. Discuss with financial institution management any inconsistencies identified. As necessary, obtain and review copies of credit or debit advices, general ledger tickets and other supporting documentation.

vi. Review unusual transactions and customer due diligence information to determine if transactions are potentially suspicious.

vii. Discuss preliminary findings and conclusions with the management of the financial institution.

11. If the currency originator or intermediary, or the referral agent who works for the currency originator or intermediary has an account with the financial institution, review a sample of account activity.

12. Based on the examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with the bulk shipment of currency.

51. OVERVIEW OF FOREIGN CURRENCY DENOMINATED DRAFTS

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with foreign currency denominated drafts and the management's ability to implement effective monitoring and reporting systems.

A foreign currency draft is a financial institution's drafts or cheque denominated in foreign currency and made available at foreign financial institution. These drafts are drawn on a Nigerian correspondent account by a foreign financial institution. Such drafts are frequently purchased to pay for commercial or personal transactions and to settle overseas obligations.

ML/FT Risk Factors

Most foreign currency denominated drafts are legitimate. However, such drafts have proven to be vulnerable to money laundering abuse. Schemes involving foreign currency drafts could involve the smuggling of currency to a foreign financial institution for the purchase of a cheque or draft denominated in another foreign currency. The foreign financial institution accepts the draft denominated in a particular foreign currency and issues another draft denominated in a different foreign currency. Once the currency is in the form of a bank draft, the money launderer can more easily conceal the source of funds. The ability to convert illicit proceeds to a bank draft at a foreign financial institution makes it easier for a money launderer to transport the instrument either back into the originating country or to endorse it to a third party in a jurisdiction where money laundering laws or compliance are lax. In any case, when the individual has succeeded in laundering his illicit proceeds, the draft or cheque would be returned ultimately for processing in the originating country.

Risk Mitigation

A Nigerian financial institution's policies, procedures and processes should include the following:

i. Outline criteria for opening a foreign currency denominated draft relationship with a foreign financial institution or entity (e.g., jurisdiction, products, services, target market, purpose of account and anticipated activity or customer history).
ii. Detail acceptable and unacceptable transactions (e.g., structuring transactions or the purchase of multiple sequentially numbered drafts for the same payee).
iii. Detail the monitoring and reporting of suspicious transaction associated with foreign currency denominated drafts.
iv. Discuss criteria for closing a foreign currency denominated draft relationships.

52. EXAMINATION PROCEDURES OF FOREIGN CURRENCY DENOMINATED DRAFTS

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with foreign currency denominated drafts, and management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to foreign currency denominated drafts. Evaluate the adequacy of the policies, procedures and processes given the financial institution's foreign currency denominated draft activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing. Determine whether policies address the following:

    i. Criteria for allowing a financial institution to issue foreign currency denominated drafts (e.g., jurisdiction, products, services and target markets, purpose of account and anticipated activity, customer history and other available information).

    ii. Identification of unusual transactions (e.g., structuring transactions or the purchase of multiple sequentially numbered foreign currency denominated drafts to the same payee).

    iii. Criteria for ceasing foreign currency denominated draft issuance through a foreign financial institution.

2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk foreign currency denominated draft accounts.

3. Determine whether the financial institution's system for monitoring foreign currency denominated draft accounts for suspicious transactions, and for reporting suspicious transactions is adequate given the financial institution's size, complexity, location and types of customer relationships.

4. Obtain a list the financial institution's correspondent accounts in which foreign currency denominated drafts are offered. Review the volume by number and currency amount of monthly transactions for each account. Determine whether management has appropriately assessed risk.

Transaction Testing

5. On the basis of the financial institution's risk assessment of its foreign currency denominated draft transactions as well as prior examination and audit reports, select a sample of foreign correspondent financial institution's accounts in which foreign currency denominated drafts are processed. In the sample selected, include accounts with a high volume of foreign currency denominated draft transactions. From the sample selected, perform the following examination procedures:

    i. Review transactions for sequentially numbered foreign currency denominated drafts to the same payee or from the same remitter. Research any unusual or suspicious foreign currency denominated draft transactions.

ii. Review the financial institution's contracts and agreements with foreign correspondent financial institutions. Determine the
iii. contracts address procedures for processing and clearing foreign currency denominated drafts.
iv. Verify that the financial institution has obtained and reviewed information about the foreign financial institution's home country AML/CFT regulatory requirements (e.g., customer identification and suspicious transaction reporting).

6. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with foreign currency denominated drafts.

53. OVERVIEW OF PAYABLE THROUGH ACCOUNTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with payable through accounts (PTA), and ability of the management to implement effective monitoring and reporting systems.

Foreign financial institutions use PTAs, also known as "pass-through" or "pass-by" accounts, to provide their customers with access to the Nigerian financial system. Some financial institutions in Nigeria also offer payable through accounts as a service to foreign financial institutions. The risk associated with money laundering/ financing of terrorism and other illicit activities is higher in PTAs that are not adequately controlled.

Generally, a foreign financial institution requests a PTA for its customers that want to conduct banking transactions in Nigeria through the foreign financial institution's account at financial institution in Nigeria. The foreign financial institution provides its customers, commonly referred to as **"sub accountholders," with cheques that allow them to draw funds from the foreign financial institution's account from a Nigerian financial institution.** The sub accountholders, which may number several hundred or in the thousands for one PTA, all become signatories on the foreign financial institution's account in a Nigerian financial institution. While payable through customers are able to write cheques and make deposits at a financial institution in Nigeria like any other accountholder, they might not be directly subject to the financial institution's account opening requirements in Nigeria.

PTA activities should not be confused with traditional international correspondent banking relationships in which a foreign financial institution enters into an agreement with a Nigerian financial institution to process and complete transactions on behalf of the foreign financial institution and its

customers. Under the latter correspondent arrangement, the foreign financial institution's customers do not have direct access to the correspondent account at the Nigerian financial institution, but they do transact business through the Nigerian financial institution. This arrangement differs significantly from a PTA with sub accountholders who have direct access to the Nigerian financial system by virtue of their independent ability to conduct transactions with the Nigerian financial system through the PTA.

ML/FT Risk Factors

PTAs may be prone to higher risk because Nigerian financial institutions do not typically implement the same due diligence requirements for PTAs that they require of domestic customers who want to open current and other accounts.

Foreign financial institutions' use of PTAs, coupled with inadequate oversight by Nigerian financial institutions, may facilitate unsound banking practices, including money laundering/ financing of terrorism and other related criminal activities. The potential for facilitating money laundering or terrorist financing, and other serious crimes increases when a Nigerian financial institution is unable to identify and adequately understand the transactions of the ultimate users (all or most of whom are outside of Nigeria) of its account with a foreign correspondent. **PTAs used for illegal purposes can cause financial institutions serious financial losses in criminal and civil fines and penalties, seizure or forfeiture of collateral and reputation damage.**

Risk Mitigation

Nigerian financial institutions offering PTA services should develop and maintain adequate policies, procedures and processes to guard against possible illicit use of these accounts. At a minimum, policies, procedures and processes should enable each Nigerian financial institution to identify the ultimate users of its foreign financial institution's PTA. T**his should include the financial institution's obtaining (or having the ability to obtain through a trusted third-party arrangement) substantially the same information on the ultimate PTA users as it obtains on its direct customers.**

Policies, procedures and processes should include a review of the foreign financial institution's processes to identify and monitor the transactions of its sub-account holders and to comply with any AML/CFT statutory and regulatory requirements existing in Nigeria (as the host country). **It should also review the foreign financial institution's master agreement with the Nigerian financial institutions on the PTAs.** In addition, Nigerian financial institutions should have procedures for monitoring transactions conducted in the foreign financial institutions' PTAs.

In an effort to address the risk inherent in PTAs, financial institutions in Nigeria should have a signed contract (i.e., master agreement) that includes:

i. Roles and responsibilities of each party.

ii. Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, cheque cashing).

iii. Restrictions on some types of sub accountholders (e.g., finance companies, funds remitters or other non-bank financial institutions).

iv. Prohibitions or restrictions on multi-tier sub accountholders.

v. Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.

Nigeria Financial institutions should consider closing the PTA in the following circumstances:

i. Insufficient information on the ultimate PTA users.

ii. Evidence of substantive or ongoing suspicious activity.

iii. Inability to ensure that the PTAs are not being used for money laundering or other illicit purposes.

54. EXAMINATION PROCEDURES OF PAYABLE THROUGH ACCOUNTSE

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with payable through accounts (PTA), and ability of the management to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to PTAs. Evaluate the adequacy of the policies, procedures and processes given the financial institution's PTA activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing. **Determine whether:**

    i. Criteria for opening PTA relationships with a foreign financial institution are adequate. **Examples of factors that may be used include jurisdiction, products, services, markets, purpose, anticipated activity, customer history, ownership, senior management, certificate of incorporation, banking license, certificate of good standing and demonstration of the foreign financial institution's operational capability to monitor account activity.**

ii. Appropriate information has been obtained and validated from the foreign financial institution concerning the identity of any persons having authority to direct transactions through the PTA.

iii. Information and EDD have been obtained from the foreign financial institution concerning the source and beneficial ownership of funds of persons who have authority to direct transactions through the PTA **(e.g., name, address, expected activity level, place of employment, description of business, related accounts, identification of foreign politically exposed persons, source of funds and articles of incorporation).**

iv. Sub-accounts are not opened before the Nigerian financial institution has reviewed and approved the customer information.

v. Master or sub-accounts can be closed if the information provided to the financial institution has been materially inaccurate or incomplete.

vi. The financial institution can identify all signatories on each sub-account.

2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors PTAs.

3. Determine whether the financial institution's system for monitoring PTAs for suspicious activities and reporting suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

4. To assess the volume of risk and determine whether adequate resources are allocated to the oversight and monitoring activity, obtain a list of foreign correspondent financial institution accounts in which PTAs are offered and request MIS reports that show**:**

    i. The number of subaccounts within each PTA; and

    ii. The volume and Naira amount of monthly transactions for each subaccount.

5. Verify that the financial institution has obtained and reviewed information concerning the foreign financial institution's home country AML/CFT regulatory requirements (e.g., customer identification requirements and suspicious transaction reporting) and considered these requirements when reviewing PTAs. Determine whether the financial institution has ensured that subaccount agreements comply with any AML/CFT statutory and regulatory requirements existing in the foreign financial institution's home country.

Transaction Testing

6. On the basis of the financial institution's risk assessment of its PTA activities as well as prior examination and audit reports, select a sample of PTAs. **From the sample, review the contracts or agreements with the foreign financial institution and determine whether the contracts or agreements:**

i. Clearly outline the contractual responsibilities of both the Nigerian financial institution and the foreign financial institution.
ii. Define PTA and subaccount opening procedures and require an independent review and approval process when opening the account.
iii. Require the foreign financial institution to comply with its Nigeria/local AML/CFT requirements.
iv. Restrict subaccounts from being opened by finance companies, funds remitters or other non-bank financial institutions.
v. Prohibit multi-tier sub accountholders.
vi. Provide for proper controls over currency deposits and withdrawals by sub accountholders and ensure that CTRs have been appropriately filed.
vii. Provide for Naira limits on each sub accountholder's transactions that are consistent with expected account activity.
viii. Contain documentation requirements that are consistent with those used for opening domestic accounts at the Nigerian financial system.
ix. Provide the Nigeria financial institution with the ability to review information concerning the identity of sub-accountholders (e.g., directly or through a trusted third party).
x. Require the foreign financial institution to monitor subaccount activities for unusual or suspicious activity and report findings to the Nigerian financial institution.
xi. Allow the Nigerian financial institution, as permitted by local laws, to audit the foreign financial institution's PTA operations and to access PTA documents.

7. Review PTA master-account of the financial institution's statements. The Examiner should determine the time period based upon the size and complexity of the financial institution. The statements chosen should include frequent transactions and those of large Naira amounts. Verify the statements to the general ledger and bank reconciliations. Note any currency shipments or deposits made at the Nigerian financial institution on behalf of an individual sub accountholder for credit to the customer's subaccount.

8. From the sample selected, review each sub accountholder's identifying information and related transactions for a period of time as determined by the Examiner. Evaluate PTA sub account holders' transactions. Determine whether the transactions are consistent with expected transactions or warrant further research. The sample should include sub account holders with significant dollar activity.

9. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with PTAs.

55. OVERVIEW OF POUCH ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with pouch activities and management's ability to implement effective monitoring and reporting systems.

Pouch activity entails the use of a carrier, courier (either independent or common) or a referral agent employed by the courier to transport currency, monetary instruments and other documents from foreign countries to financial institutions in Nigeria.

Pouches can be sent by financial institution or individuals. Pouch services are commonly offered in conjunction with foreign correspondent banking services. Pouches can contain loan repayments, transactions for demand deposit accounts or other types of transactions.

Risk Factors

Financial institutions should be aware that bulk amounts of monetary instruments purchased in Nigeria that appear to have been structured to avoid the AML/CFT-reporting requirements often have been found in pouches or cash letters received from foreign financial institutions. **The monetary instruments involved are frequently traveller's cheques and bank cheques that usually have one or more of the following characteristics in common:**

i. The instruments purchased on the same or consecutive days at different locations.
ii. The payee lines are left blank or made out to the same person (or to only a few people).
iii. They contain little or no purchaser information.
iv. They bear the same stamp, symbol or initials.
v. They are purchased in round denominations or repetitive amounts.
vi. The depositing of the instruments is followed soon after by a funds transfer out in the same dollar amount.

Risk Mitigation

Policies, procedures and processes related to pouch activity

i. Outline criteria for opening a pouch relationship with an individual or a foreign financial institution (e.g., customer due diligence requirements, type of institution or person, acceptable purpose of the relationship).
ii. Detail acceptable and unacceptable transactions (e.g., monetary instruments with blank payees, unsigned monetary instruments and a large number of consecutively numbered monetary instruments).
iii. Detail procedures for processing the pouch including employee responsibilities, dual control, reconciliation, documentation requirements, and employee sign off.
iv. Detail procedures for reviewing of unusual or suspicious transaction including elevating concerns to management. Contents of pouches may be subject to

CTR, Report of International Transportation of Currency or Monetary Instruments (CMIR).

v. Discuss criteria for closing pouch relationships.

The above factors should be included within an agreement or contract between the financial institution and the courier that details the services to be provided and the responsibilities of both parties.

56. EXAMINATION PROCEDURES OF POUCH ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with pouch activities and the management's ability to implement effective monitoring and reporting systems.

1. Determine whether the financial institution has incoming or outgoing pouch activity and whether the activity is via carrier or courier.
2. Review the policies, procedures and processes, and any contractual agreements related to pouch activities. Evaluate the adequacy of the policies, procedures, and processes given the financial institution's pouch activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
3. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors pouch activities.
4. Determine whether the financial institution's system for monitoring pouch activities for suspicious transactions and for reporting suspicious transactions is adequate given the financial institution's size, complexity, location and types of customer relationships.
5. Review the list of financial institution customers permitted to use pouch services (incoming and outgoing). Determine whether management has assessed the ML/FT risk of the customers permitted to use this service.

Transaction Testing

6. On the basis of the financial institution's ML/FT risk assessment of its pouch activities as well as prior examination and audit reports, and recent activity records, select a sample of daily pouches for review. Preferably on an unannounced basis and over a period of several days, not necessarily consecutive, observe the pouch opening and the data capture process for items contained in a sample of incoming pouches, and observe the preparation of outgoing pouches. Review the records and the pouch contents for currency, monetary instruments, bearer securities, prepaid cards, gems, art, illegal substances or contraband, or other items that should not ordinarily appear in a financial institution's pouch.

7. If the courier or the referral agent who works for the courier has an account with the financial institution, review an appropriate sample of his account activity.
8. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with pouch activity.

57. OVERVIEW OF ELECTRONIC BANKING

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with electronic banking (e-banking) customers including **Remote Deposit Capture (RDC) activity** and management's ability to implement effective monitoring and reporting systems.

E-banking systems which provide electronic delivery of banking products to customers include automated teller machine (ATM) transactions; online account opening; internet banking transactions; and telephone banking. For example, credit cards, deposit accounts, mortgage loans and funds transfers can all be initiated online without face-to-face contact. **Management needs to recognize this as a potentially higher-risk area and develop adequate policies, procedures and processes for customer identification and monitoring for specific areas of banking.**

ML/FT Risk Factors

Financial institutions should ensure that their monitoring systems adequately capture transactions conducted electronically. As with any account, they should be alert to anomalies in account behaviour. **Red flags may include the velocity of funds in the account or in the case of ATMs, the number of debit cards associated with the account.**

Accounts opened without face-to-face contact may be a higher risk

i. More difficult to positively verify the individual's identity.
ii. Customer may be out of the financial institution's targeted geographic area or country.
iii. Customer may perceive the transactions as less transparent.
iv. Transactions are instantaneous.
v. May be used by a "front" company or unknown third party.

Risk Mitigation

Financial institutions should establish AML/CFT monitoring, identification and reporting for unusual and suspicious transactions occurring through e-banking systems. **Useful MIS for detecting unusual transaction in higher-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change**

of internet address reports, Internet Protocol (IP) address reports and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses and tax identification numbers).

In determining the level of monitoring required for an account, financial institutions should include how the account was opened as a factor. Financial institutions engaging in transactional internet banking should have effective and reliable methods to authenticate a customer's identity when opening accounts online and should establish policies for when a customer should be required to open accounts on a face-to-face basis. Financial institutions may also institute other controls, such as establishing transaction dollar limits for large items that require manual intervention to exceed the pre-set limit.

Remote Deposit Capture

Remote Deposit Capture (RDC) is a deposit transaction delivery system that has made cheque and monetary instrument processing (e.g., traveller's cheques) more efficient.

In broad terms, RDC allows a financial institution's customers to scan a cheque or monetary instrument and then transmit the scanned or digitized image to the institution.

It should be noted that scanning and transmission activities can take place at remote locations including the financial institution's branches, ATMs, domestic and foreign correspondents, and locations owned or controlled by commercial or retail customers. By eliminating face-to-face transactions, RDC decreases the cost and volume of paper associated with physically mailing or depositing items. RDC also supports new and existing banking products and improves customers' access to their deposits.

ML/FT Risk Factors in Remote Deposit Capture

RDC may expose financial institutions to various risks including money laundering, financing of terrorists, fraud and information security. Fraudulent, sequentially numbered or physically altered documents, particularly money orders and traveler's cheques may be more difficult to detect when submitted by RDC and not inspected by a qualified person. Financial institutions may face challenges in controlling or knowing the location of RDC equipment because the equipment can be readily transported from one jurisdiction to another.

This challenge is increased as foreign correspondents and foreign money services businesses are increasingly using RDC services to replace pouch and certain instrument processing and clearing activities. Inadequate controls could result in intentional or unintentional alterations to deposit item data, re-submission of a data file, or duplicate presentment of cheques and images at one or multiple financial institutions. In addition, original deposit items are not typically forwarded to financial institutions, but instead the customer or the customer's service provider retains them. As a result, recordkeeping, data safety and integrity issues may increase.

Higher-risk customers may be defined by industry, incidence of fraud or other criteria. Examples of higher-risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order companies, online gambling operations, businesses located offshore and adult entertainment businesses.

Risk Mitigation

Management should develop appropriate policies, procedures and processes to mitigate the risks associated with RDC services and to effectively monitor for unusual or suspicious transactions. Examples of risk mitigants include:

i. Comprehensively identifying and assessing RDC risk prior to implementation. Senior management should identify AML/CFT operational, information security, compliance, legal, and reputation risks. Depending on the financial institution's size and complexity, this comprehensive risk assessment process should include staff from information technology and security, deposit operations, treasury or cash management sales, business continuity, audit, compliance, accounting and legal.
ii. Conducting appropriate CDD and EDD.
iii. Creating risk-based parameters that can be used to conduct Remote Deposit Capture (RDC) customer suitability reviews. Parameters may include a list of acceptable industries, standardized underwriting criteria (e.g., credit history, financial statements and ownership structure of business) and other risk factors. When the level of risk warrants, financial institutions' staff should consider visiting the customer's physical location as part of the suitability review. During these visits, the customer's operational controls and risk management processes should be evaluated.
iv. Conducting vendor due diligence when financial institutions use a service provider for RDC activities. Management should ensure implementation of sound vendor management processes.
v. Obtaining expected account activity from the RDC customer, such as the anticipated RDC transaction volume, and type (e.g., payroll cheques, third-party cheques, or traveller's cheques), comparing it to actual transaction and resolving significant deviations. Comparing expected activity to business type to ensure they are reasonable and consistent.
vi. Establishing or modifying customer Remote Deposit Capture transaction limits.
vii. Developing well-constructed contracts that clearly identify each party's role, responsibilities and liabilities, and detail record retention procedures for RDC data. These procedures should include physical and logical security expectations for access, transmission, storage and ultimate disposal of original documents. The contract should also address the customer's responsibility for properly securing RDC equipment and preventing inappropriate use, including establishing effective equipment security controls (e.g., passwords & dual control access). In addition, contracts should detail the RDC customer's obligation to provide original documents to the financial institution in order to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes. Contracts should clearly detail the

authority of the financial institution to mandate specific internal controls, conduct audits or terminate the RDC relationship.Implementing additional monitoring or review when significant changes occur in the type or volume of transactions, or when significant changes occur in the underwriting criteria, customer base, customer risk management processes or geographic location that the bank relied on when establishing RDC services.

viii. Ensuring that RDC customers receive adequate training. The training should include documentation that addresses issues such as routine operations and procedures, duplication and problem resolution.

ix. Using improved aggregation and monitoring capabilities as facilitated by the digitized data.

x. As appropriate, using technology to minimize errors (e.g., the use of franking to stamp or identify a deposit as being processed).

58. EXAMINATION PROCEDURES OF ELECTRONIC BANKING

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with electronic banking (e-banking) customers, including **Remote Deposit Capture (RDC) activity** and management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to e-banking. Evaluate the adequacy of the policies, procedures and processes given the financial institution's e-banking activities and the ML/FT risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk e-banking activities.
3. Determine whether the financial institution's system for monitoring e-banking for suspicious transactions and for reporting suspicious transactions is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its e-banking activities as well as prior examination and audit reports, select a sample of e-banking accounts. From the sample selected, perform the following procedures:
    i. Review account opening documentation and KYC requirements, ongoing CDD and transaction history.
    ii. Compare expected activity with actual activity.

iii. Determine whether the transaction is consistent with the nature of the customer's business. Identify any unusual or suspicious transaction.

5. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with e-banking relationships.

59. OVERVIEW OF FUNDS TRANSFERS

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with funds transfers and the management's ability to implement effective monitoring and reporting systems. This section expands the core review of the statutory and regulatory requirements of funds transfers to provide a broader assessment of ML/FT risks associated with this transaction.

Payment systems in Nigeria consist of numerous financial intermediaries, financial services companies and non-bank businesses that create, process and distribute payments. The domestic and international expansion of the financial industry services has increased the importance of electronic funds transfers, including funds transfers made through the wholesale payment systems.

Funds Transfer Services

The vast majority of the value of Naira payments or transfers in Nigeria is ultimately processed through wholesale payment systems which generally handle large-value transactions between financial institutions. Financial institutions conduct these transfers on their own behalf as well as for the benefit of other financial service providers and financial institution customers, both consumer and corporate.

Related retail transfer systems facilitate transactions such as automated clearing houses (ACH); automated teller machines (ATM); point-of-sales (POS); telephone bill paying; home banking systems; and credit, debit, and prepaid cards. Most of these retail transactions are initiated by customers rather than by financial institutions or corporate users. These individual transactions may then be batched in order to form larger wholesale transfers, which are the focus of this section.

The primary domestic wholesale payment system for interbank funds transfers is the **Nigerian Inter-Bank Settlement System (NIBSS).** The bulk of the Naira value of these payments is originated electronically to make large value, time-critical payments, such as the settlement of interbank purchases and sales of government funds, settlement of foreign exchange transactions, disbursement or repayment of loans; settlement of real estate transactions or other financial market transactions; and purchasing, selling or financing securities transactions. NIBSS and **Real Time Gross Settlement System (RTGS)** participants facilitate these transactions on their behalf and on behalf of their customers, including non-bank financial institutions, commercial businesses and correspondent banks that do not have direct access.

Two components to funds transfers

i. The instructions, which contain information on the sender and receiver of the funds; and
ii. The actual movement or transfer of funds.

The instructions may be sent in a variety of ways, including by electronic access to networks operated by the NIBSS payment systems; by access to financial telecommunications systems such as **Society for Worldwide Interbank Financial Telecommunication (SWIFT);** or e-mail, facsimile, telephone or telex.

NIBSS and RTGS are used to facilitate funds transfers between two domestic endpoints or the fund segment of international transactions. SWIFT is an international messaging service that is used to transmit payment instructions for the vast majority of international interbank transactions which can be denominated in numerous currencies.

Society for Worldwide Interbank Financial Telecommunication

The SWIFT network is a messaging infrastructure (not a payments system) which provides users with a private international communications-link among themselves.

The actual funds movements (payments) are completed through correspondent financial institution relationship. Movement of payments denominated in different currencies occurs through correspondent financial institution relationships or over funds transfer systems in the relevant country. In addition to customer and financial institution funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections and documentary credits.

Cover Payments

A typical funds transfer involves an originator instructing his financial institution (the originator's financial institution) to make payment to the account of a payee (the beneficiary) in the beneficiary's financial institution. **A cover payment occurs when the originator's financial institution and the beneficiary's financial institution do not have a relationship that allows them to settle the payment directly. In that case, the originator's financial institution instructs the beneficiary's financial institution to effect the payment and advises that transmission of funds to "cover" the obligation created by the payment order has been arranged through correspondent accounts at one or more intermediary financial institutions.**

Cross-border cover payments usually involve multiple financial institutions in multiple jurisdictions.

Informal Value Transfer System

An Informal Value Transfer System **(IVTS)** is used to describe a currency or value transfer system that operates informally to transfer money as a business. In countries

lacking a stable financial sector or with large areas not served by formal financial institutions, IVTS may be the only method for conducting financial transactions. Persons living in Nigeria may use IVTS to transfer funds to their home countries.

Payable Upon Proper Identification Transactions

One type of funds transfer transaction that carries particular ML/FT risk is the payable upon proper identification (PUPID) service. **PUPID transactions are funds transfers for which there are no specific account to deposit the funds into and the beneficiary of the funds is not a financial institution customer.**

For example, an individual may transfer funds to a relative or an individual who does not have an account relationship with the financial institution that receives the funds transfer. In this case, the beneficiary financial institution may place the incoming funds into a suspense account and ultimately release the funds when the individual provides proof of identity. In some cases, financial institutions permit non-customers to initiate PUPID transactions. **These transactions are considered extremely high risk and require strong controls.**

ML/FT Risk Factors in Funds Transfer

Funds transfers may present a heightened degree of ML/FT risk, depending on such factors as the number and Naira volume of transactions, geographic location of originators and beneficiaries, and whether the originator or beneficiary is a financial institution customer. The size and complexity of a financial institution's operation and the origin and destination of the funds being transferred will determine which type of funds transfer system the financial institution uses. The vast majority of funds transfer instructions are conducted electronically. However, Examiners need to be mindful that physical instructions may be transmitted by other informal methods, as described earlier.

Cover payments made through SWIFT pose additional risks for intermediary financial institutions that do not have facilities that identify the originator and beneficiary of the funds transfer. Without such facilities, the intermediary financial institution is unable to monitor or filter payment information. This lack of transparency limits the Nigerian intermediary financial institution's ability to appropriately assess and manage the risk associated with correspondent and clearing operations and monitor suspicious transaction.

The risks of PUPID transactions to the beneficiary financial institution are similar to other transactions in which the financial institution does business with non-customers. However, the risks are heightened in PUPID transactions if the financial institution allows a non-customer to access the funds transfer system by providing minimal or no identifying information. **Financial institutions that allow non-customers to transfer funds using the PUPID service pose significant risk to both the originating and beneficiary financial institution. In these situations, both financial institutions have minimal or no identifying information on the originator or the beneficiary.**

Risk Mitigation

Funds transfers can be used in the placement, layering and integration stages of money laundering. Funds transfers purchased with currency are an example of the placement stage. Detecting unusual transaction in the layering and integration stages is more difficult for a financial institution because transactions may appear legitimate. In many cases, a financial institution may not be involved in the placement of the funds or in the final integration, only the layering of transactions. Financial institutions should consider all three stages of money laundering when evaluating or assessing funds transfer risks.

Financial institutions need to have sound policies, procedures and processes to manage the ML/FT risks of its funds transfer activities. Funds transfer policies, procedures and processes should address all foreign correspondent banking transactions, including transactions in which Nigerian branches and agencies of foreign financial institutions are intermediaries for their head offices.

Obtaining CDD information is an important mitigant of risk in providing funds transfer services. Because of the nature of funds transfers, adequate and effective CDD policies, procedures and processes are critical in detecting unusual and suspicious transactions. An effective risk-based suspicious transaction monitoring and reporting system is equally important. Whether this monitoring and reporting system is automated or manual, it should be sufficient to detect suspicious trends and patterns typically associated with money laundering.

Institutions involved in international payments transactions

i. Financial institutions should not omit, delete or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process;
ii. Financial institutions should not use any particular payment message for the purpose of avoiding detection of information by any other financial institution in the payment process;
iii. Subject to all applicable laws, financial institutions should cooperate as fully as practicable with other financial institutions in the payment process when requested to provide information about the parties involved; and
iv. Financial institutions should strongly encourage their correspondent financial institutions to observe these principles.

Effective monitoring processes for cover payments include:

i. Monitoring funds transfers processed through automated systems in order to identify suspicious transaction. This monitoring may be conducted after the transfers are processed, on an automated basis, and may use a risk-based approach; and

ii. Given the volume of messages and data for large Nigerian intermediary financial institutions, a manual review of every payment order may not be feasible or effective. However, intermediary financial institutions should have, as part of their monitoring processes, a risk-based method to identify incomplete fields or fields with meaningless data. **Nigerian financial institutions engaged in processing cover payments should have policies to address such circumstances, including those that involve systems other than SWIFT.**

Originating and beneficiary financial institutions should establish effective and appropriate policies, procedures and processes for PUPID transaction

i. Specifying the type of identification that is acceptable.
ii. Maintaining documentation of individuals consistent with the bank's recordkeeping policies.
iii. Defining which financial institution employees may conduct PUPID transactions
iv. Establishing limits on the amount of funds that may be transferred to or from the financial institution for non-customers.
v. Monitoring and reporting suspicious transactions.
vi. Providing enhanced scrutiny for transfers to or from certain jurisdictions.
vii. Identifying disbursement method for proceeds from a beneficiary financial institution.

60. EXAMINATION PROCEDURES OF FUNDS TRANSFERS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with funds transfers and the management's ability to implement effective monitoring and reporting systems.

This section expands the core review of the statutory and regulatory requirements of funds transfers to provide a broader assessment of ML/FT risks associated with this activity.

1. Review the policies, procedures and processes related to funds transfers. Evaluate the adequacy of the policies, procedures and processes given the financial institution's funds transfer activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors funds transfer activities.
3. Evaluate the financial institution's risks related to funds transfer activities by analyzing the frequency and currency volume of funds transfers, jurisdictions and the financial institution's role in the funds transfer process (e.g., whether it is the originator's bank or financial institution, intermediary financial institution or

beneficiary's financial institution). These factors should be evaluated in relation to the financial institution's size, its location and the nature of its customer and correspondent account relationships.

4. Determine whether an audit trail of funds transfer activities exists. Determine whether an adequate separation of duties or other compensating controls are in place to ensure proper authorization for sending and receiving funds transfers and for correcting postings to accounts.
5. Determine whether the financial institution's system for monitoring funds transfers and for reporting suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships. **Determine whether suspicious activity monitoring and reporting systems include:**
    i. Funds transfers purchased with currency.
    ii. Transactions in which the financial institution is acting as an intermediary.
    iii. All SWIFT message formats.
    iv. Transactions in which the financial institution is originating or receiving funds transfers from foreign financial institutions, particularly to or from jurisdictions with strict privacy and secrecy laws or those identified as higher risk.
    v. Frequent currency deposits or funds transfers and then subsequent transfers, particularly to a larger institution or out of the country.

Review the financial institution's procedures for cross-border funds transfers

i. Determine whether the financial institution processes its foreign correspondent banking activity with due diligence. Review and evaluate the transparency practices of the financial institution's correspondents in cross-border funds transfers through the bank (for example, whether correspondents are appropriately utilizing the MT message format).

ii. As applicable and if not already performed, review the financial institution's procedures to ensure compliance with the Travel Rule, including appropriate use of the MT format.

iii. Assess the financial institution's policies for cooperation with its correspondents when they request the bank or financial institution to provide information about parties involved in funds transfers.

iv. Assess the adequacy of the financial institution's procedures for addressing isolated as well as repeated instances where payment information received from a correspondent is missing, manifestly meaningless or incomplete or suspicious.

v. Determine the financial institution's procedures for payable upon proper identification (PUPID) transactions.

vi. Determine how the beneficiary bank or other financial institution disburses the proceeds (i.e., by currency or official cheques).

vii. Determine how the originating bank or other financial institution allows PUPID funds transfers for non-customers. Determine the type of funds accepted (i.e., by currency or official check).

Transaction Testing

On the basis of the financial institution's risk assessment of funds transfer activities as well as prior AML/CFT Bank Examination and Audit Reports, **select a sample of higher-risk funds transfer activities, which may include the following:**

i. Funds transfers purchased with currency.
ii. Transactions in which the financial institution is acting as an intermediary, such as cover payments.
iii. Transactions in which the financial institution is originating or receiving funds transfers from foreign financial institutions, particularly to or from jurisdictions with strict privacy and secrecy laws or those identified as higher risk.
iv. PUPID transactions.

From the sample selected, analyze funds transfers to determine whether the amounts, frequency and jurisdictions of origin or destination are consistent with the nature of the business or occupation of the customer.

In addition, for funds transfers processed using various message formats, review the sample of messages to determine whether the financial institution has used the appropriate message formats and has included complete originator and beneficiary information (e.g., no missing or meaningless information).

On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with funds transfer activity.

61. OVERVIEW OF AUTOMATED CLEARING HOUSE (ACH) TRANSACTIONS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with automated clearing house (ACH) and international ACH transactions (IAT) and the management's ability to implement effective monitoring and reporting systems.

The use of the ACH has grown markedly over the last several years due to the increased volume of electronic cheque conversion and one-time ACH debits, reflecting

the lower cost of ACH processing relative to cheque processing. Cheque conversion transactions as well as one-time ACH debits are primarily of low currency value used for consumer transactions for purchases of goods and services or payment of consumer bills. **ACH is primarily used for domestic payments.**

ACH Payment Systems

Traditionally, the ACH system has been used for the direct deposit of payroll and government benefit payments and for the direct payment of mortgages and loans. As noted earlier, the ACH has been expanding to include one-time debits and cheque conversion. ACH transactions are payment instructions to either credit or debit a deposit account. Examples of credit payment transactions include payroll direct deposit, social security, dividends and interest payments. Examples of debit transactions include mortgage, loan, insurance premium and a variety of other consumer payments initiated through merchants or businesses.

In the electronic cheque conversion process, merchants that receive a cheque for payment do not collect the cheque through the cheque collection system, either electronically or in paper form. Instead, merchants use the information on the cheque to initiate a type of electronic funds transfer known as an ACH debit to the cheque writer's account. The cheque is used to obtain the bank routing number, account number, cheque serial number and currency amount for the transaction. The cheque itself is not sent through the cheque collection system in any form as a payment instrument. Merchants use electronic cheque conversion because it can be a more efficient way for them to obtain payment than collecting the cheque.

RTGS is a central clearing facility for transmitting and receiving ACH payments and SWIFT/ Interswitch which sends cross-border ACH credits payments to some countries around the world plus debit payments.

Third-Party Service Providers

A Third-Party Service Provider **(TPSP)** is an entity other than an originator, Originating Depository Financial Institution (ODFI) or **Receiving Depository Financial Institution (RDFI)** that performs any functions on behalf of the Originator, the ODFI or the RDFI with respect to the processing of ACH entries.

Risk Factors

The ACH system was designed to transfer a high volume of domestic currency transactions which pose lower ML/FT risks. Nevertheless, the ability to send high international currency transactions through the ACH may expose banks to higher ML/FT risks. Banks/Other financial Institutions (OFIs) without a robust ML/FT monitoring

system may be exposed to additional risk particularly when accounts are opened over the internet without face-to face contact.

ACH transactions that are originated through a TPSP (that is, when the originator is not a direct customer of the ODFI) may increase ML/FT risks, therefore, making it difficult for an ODFI to underwrite and review originator's transactions for compliance with AML/CFT rules. Risks are heightened when neither the TPSP nor the ODFI performs due diligence on the companies for whom they are originating payments.

Certain ACH transactions, such as those originated through the internet or the telephone may be susceptible to manipulation and fraudulent use. Certain practices associated with how the banking industry processes ACH transactions may expose banks/OFIs to ML/FT risks. **These practices include:**

i. An Originating Depository Financial Institution (ODFI) authorizing a Third Party Service Provider (TPSP) to send ACH files directly to an ACH Operator, in essence by-passing the ODFI.
ii. ODFIs and Receiving Depository Financial Institutions (RDFIs) relying on each other to perform adequate due diligence on their customers.
iii. Batch processing that obscures the identities of originators.
iv. Lack of sharing of information on or about originators and receivers inhibits a bank's/OFIs' ability to appropriately assess, monitor, control/manage and mitigate the risk associated with correspondent and ACH processing operations, monitor for suspicious activity and screen for MLPA 2004 and CBN AML/CFT Regulation 2009 compliance.

Risk Mitigation

The BOFIA 1991 (as amended), MLPA 2004 and CBN AML/CFT Regulation 2009 require financial institutions to have AML/CFT Compliance Programs and appropriate policies, procedures and processes in place to monitor and identify unusual activity, including ACH transactions. Obtaining CDD information in all operations is an important mitigant to ML/FT risk in ACH transactions. Because of the nature of ACH transactions and the reliance that ODFIs and RDFIs place on each other for regulatory reviews and other necessary due diligence information, it is essential that all parties have a strong CDD program for regular ACH customers. For relationships with TPSPs, CDD on the TPSP can be supplemented with due diligence on the principals associated with the TPSP and, as necessary, on the originators.

Adequate and effective CDD policies, procedures and processes are critical in detecting a pattern of unusual and suspicious activities because the individual ACH transactions are typically not reviewed. Equally important is an effective risk-based suspicious activity monitoring and reporting system. In cases where a financial institution is heavily reliant upon the TPSP, the financial institution may want to review the TPSP's suspicious activity monitoring and reporting program, either through its own or an independent inspection. The ODFI may establish an agreement with the TPSP, which delineates general TPSP guidelines, such as compliance with ACH operating requirements and

responsibilities and meeting other applicable regulations. **Financial institutions may need to consider controls to restrict or refuse ACH services to potential originators and receivers engaged in questionable or deceptive business practices.**

ACH transactions can be used in the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. **Financial institutions should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer.**

The ODFI should be aware of IAT activity and evaluate the activity using a risk-based approach in order to ensure that suspicious activity is identified and monitored. The ODFI, if frequently involved in international transfers, may develop a separate process which may be automated for reviewing international transfers that minimizes disruption to general ACH processing, reconcililiation and settlement.

The potentially higher risk inherent in international transfers should be considered in the financial institution's ACH policies, procedures and processes. The financial institution should consider its current, potential roles and responsibilities when developing internal controls to monitor and mitigate the risk associated with international transfers and to comply with the financial institution's suspicious activity reporting obligations.

Considerations in processing of international transfers

i. Customers and transaction types and volume.
ii. Third-party payment processor relationships.
iii. Responsibilities, obligations and risks of becoming a **Gateway Operator (GO).**
iv. CIP, CDD and EDD standards and practices.
v. Suspicious activity monitoring and reporting.
vi. Appropriate MIS, including the potential necessity for systems upgrades or changes.
vii. Processing procedures (e.g., identifying and handling international transfers and handling non-compliant and rejected messages).
viii. Training programs for appropriate bank personnel (e.g., ACH personnel, operations, compliance audit, customer service, etc.).
ix. Legal agreements, including those with customers, third-party processors and vendors, and whether those agreements need to be upgraded or modified.

Financial institutions that have relationships with third-party service providers should assess the nature of those relationships and their related ACH transactions to ascertain the financial institution's level of ML/FT risk and to develop appropriate policies, procedures and processes to mitigate that risk.

62. EXAMINATION PROCEDURES OF AUTOMATED CLEARING HOUSE TRANSACTIONS

Objective

Assess the adequacy of the bank's/other financial institution's systems to manage the risks associated with automated clearing house (ACH), international ACH transactions (IAT) and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to ACH transactions including IATs. Evaluate the adequacy of the policies, procedures and processes given the financial institution's ACH transactions, including IATs and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk customers using ACH transactions, including IATs.
3. Evaluate the financial institution's risks related to ACH transactions including IATs by analyzing the frequency, volume and types of ACH transactions in relation to the financial institution's size, its location, the nature of its customer account relationships, and the location of the origin or destination of IATs relative to the financial institution's location.
4. Determine whether the financial institution's system for monitoring customers, including third-party service providers (TPSP) using ACH transactions and IATs for suspicious activities and for reporting of suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships. **Determine whether internal control systems include:**

    i. Identifying customers with frequent and large ACH transactions or IATs.

    ii. Monitor ACH detail activity when the batch-processed transactions are separated for other purposes (e.g., processing errors).

    iii. As appropriate, identify and apply increased due diligence to higher-risk customers who originate or receive IATs, particularly when a party to the transaction is located in a higher-risk geographic location.

    iv. Using methods to track, review and investigate customer complaints or unauthorized returns regarding possible fraudulent or duplicate ACH transactions, including IATs.

Transaction Testing

5. On the basis of the financial institution's risk assessment of customers with ACH transactions as well as prior AML/CFT Bank Examination and Audit Reports, **select**

a sample of higher-risk customers, including TPSPs with ACH transactions or IATs which may include the following:

i. Customers initiating ACH transactions, including IATs from the internet or via telephone, particularly from an account opened on the internet or via the telephone without face-to-face interaction.
ii. Customers whose business or occupation does not warrant the volume or nature of ACH or international transfer activity.
iii. Customers who have been involved in the origination or receipt of duplicate or fraudulent ACH transactions or international transfer.
iv. Customers or originators (clients of customers) that are generating a high rate or high volume of invalid account returns, consumer unauthorized returns or other unauthorized transactions.

6. From the sample selected, analyze ACH transactions including IATs to determine whether the amounts, frequency and jurisdictions of origin or destination are consistent with the nature of the business or occupation of the customer. A review of the account opening documentation including CIP documentation may be necessary in making these determinations. Identify any suspicious or unusual activity.

7. On the basis of the examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with ACH transactions and international transfers.

63. OVERVIEW OF ELECTRONIC CASH

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with electronic cash (e-cash) and the management's ability to implement effective monitoring and reporting systems.

E-cash (e-money) is a digital representation of money. E-cash comes in several forms including computer-based, mobile telephone-based and prepaid cards. Computer e-cash is accessed through personal computer hard disks via a modem or stored-in-an-online repository. Mobile telephone-based e-cash is accessed through an individual's mobile telephone. Prepaid cards, discussed in more detail below, are used to access funds generally held by issuing financial institutions in pooled accounts.

In the case of computer e-cash, monetary value is electronically deducted from the financial institution account when a purchase is made or funds are transferred to another person.

Risk Factors

Transactions using e-cash may pose unique risks

i. Funds may be transferred to or from an unknown third party.
ii. Customers may be able to avoid border restrictions as the transactions can become mobile and may not be subject to jurisdictional restrictions.
iii. Transactions may be instantaneous.
iv. Specific cardholder activity may be difficult to determine by reviewing activity through a pooled account.
v. The customer may perceive the transactions as less transparent.

Risk Mitigation

Financial institutions should establish AMLCFT monitoring, identification and reporting for unusual and suspicious activities occurring through e-cash. Useful MIS for detecting unusual activity on higher-risk accounts include **ATM activity reports (focusing on foreign transactions), funds transfer reports, new account activity reports, change of internet address reports, internet protocol (IP) address reports & reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses and taxpayer identification numbers).** The financial institution also may institute other controls, such as establishing transaction and account/currency limits that require manual intervention to exceed the preset limit.

Prepaid Cards/Stored Value Cards

Consistent with industry practice, the term **"prepaid card"** is primarily used in this document. Although some sources use the term **"stored value card"** more broadly, **it most commonly refers to cards where the monetary value is physically stored on the card.**

The term "prepaid card" generally refers to an access device linked to funds held in a pooled account, which is the type of product most frequently offered by banking organizations. Prepaid cards can cover a variety of products, functionalities and technologies. Prepaid cards operate within either an "open" or "closed" system.

Open-system prepaid cards can be used for purchases at any merchant or to access cash at any automated teller machine (ATM) that connects to the affiliated global payment network. Examples of open system cards are payroll cards and gift cards that can be used anywhere a credit card can be used. Some prepaid cards may be reloaded, allowing the cardholder to add value.

Closed-system cards generally can only be used to buy goods or services from the merchant issuing the card or a select group of merchants or service providers that participate in a specific network. Examples of closed system cards include merchant-specific retail gift cards, mall cards and mass transit system cards.

Some prepaid card programs may combine multiple features, such as a flexible spending account card that can be used to purchase specific health services as well as products at a variety of merchants. These programs are often referred to as "hybrid" cards.

Prepaid cards provide a compact and transportable way to maintain and access funds. They also offer individuals without bank accounts an alternative to cash and money orders. As an alternate method of cross-border funds transmittal, prepaid card programs may issue multiple cards per account, so that persons in another country or jurisdiction can access the funds loaded by the original cardholder via ATM withdrawals of cash or merchant purchases.

Many banks that offer prepaid card programs do so as issuer or issuing bank. Most payment networks require that their branded prepaid cards be issued by a bank that is a member of that payment network. In addition to issuing prepaid cards, banks may participate in other aspects of a card program such as marketing and distributing cards issued by another financial institution. Banks often rely on multiple third parties to accomplish the design, implementation and maintenance of their prepaid card programs. These third parties may include program managers, distributors, marketers, merchants and processors. Under payment network requirements, the issuing bank or other financial institution may have due diligence and other responsibilities relative to these third parties.

Contractual Agreements

Each relationship that a Nigerian financial institution has with another financial institution or third party as part of a prepaid card program should be governed by an agreement or a contract describing each party's responsibilities and other relationship details, such as the products and services provided. The agreement or contract should also consider each party's AML/CFT compliance requirements, customer base, due diligence procedures and any payment network obligations. The issuing bank or financial institution maintains ultimate responsibility for AML/CFT compliance whether or not a contractual agreement has been established.

Risk Factors

Money laundering, terrorist financing and other criminal activities may occur through prepaid card programs if effective controls are not in place. **Investigations have found that some prepaid cardholders used false identification and funded their initial deposits with stolen credit cards or purchased multiple cards under aliases.** In the placement phase of money laundering, because many domestic and offshore financial institutions offer cards with currency access through ATMs internationally, criminals may load cash from illicit sources onto prepaid cards through unregulated load points and send the cards to their accomplices inside or outside the country. Investigations have disclosed that both open and closed system prepaid cards have been used in conjunction with, or as a replacement to bulk cash smuggling. Third parties involved in prepaid card programs may or may not be subject to regulatory requirements, oversight and supervision. In addition, these requirements may vary by party.

Prepaid card programs are extremely diverse in the range of products and services offered and the customer bases they serve. In evaluating the risk profile of a prepaid

card program, financial institutions should consider the program's specific features and functionalities. No single indicator is necessarily determinative of lower or higher ML/FT risk. Higher potential money laundering risk associated with prepaid cards results from the anonymity of the cardholder, fictitious cardholder information, cash access of the card (especially internationally) and the volume of funds that can be transacted on the card. Other risk factors include type and frequency of card loads and transactions, geographic location of card activity, relationships with parties in the card program, card value limits, distribution channels and the nature of funding sources.

Risk Mitigation

Banks/other financial institutions that offer prepaid cards or otherwise participate in prepaid card programs should have policies, procedures and processes sufficient to control and manage the related ML/FT risks. Customer due diligence is an important mitigant of ML/FT risk in prepaid card programs. **A financial institution's CDD program should provide for a risk assessment of all third parties involved in the prepaid card program, considering all relevant factors, including, as appropriate:**

i. The identity and location of all third parties involved in the prepaid card program, including any sub-agents.
ii. Corporate documentation, licences, references (including independent reporting services) and, if appropriate, documentation on principal owners.
iii. The nature of the third-parties' businesses and the markets and customer bases served.
iv. The information collected to identify and verify cardholder identity.
v. The type, purpose and anticipated activity of the prepaid card program.
vi. The nature and duration of the financial institution's relationship with third parties in the card program.
vii. The ML/FT risk obligations of third parties.

As part of their system of internal controls, financial institutions should establish a means for monitoring, identifying and reporting suspicious activity related to prepaid card programs. This reporting obligation extends to all transactions by, at or through the financial institution, including those in an aggregated form. Financial institutions may need to establish protocols to regularly obtain card transaction information from processors or other third parties. Monitoring systems should have the ability to identify foreign card activity, bulk purchases made by one individual and multiple purchases made by related parties. In addition, procedures should include monitoring for unusual activity patterns, such as cash card loads followed immediately by withdrawals of the full amount from another location.

Card features can provide important mitigation to the ML/FT risks inherent in prepaid card relationships and transactions and may include:

i. Limits or prohibitions on cash loads, access or redemption.
ii. Limits or prohibitions on amounts of loads and number of loads/reloads within a specific time frame (velocity or speed of fund use).

iii. Controls on the number of cards purchased by one individual.
iv. Maximum currency thresholds on ATM withdrawals and on the number of withdrawals within a specific time frame (velocity or speed of fund use).
v. Limits or prohibitions on certain usage (e.g., merchant type) and on geographic usage, such as outside Nigeria.
vi. Limits on aggregate card values.

64. Examination Procedures of Electronic Cash

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with electronic cash (e-cash), including prepaid cards and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to e-cash, including prepaid cards. Evaluate the adequacy of the policies, procedures and processes given the financial institution's e-cash activities, including prepaid cards and the risk they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk e-cash transactions, including prepaid card transactions.
3. Determine whether the financial institution's system for monitoring e-cash transactions, including prepaid card transactions for suspicious activities and for reporting suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its e-cash activities including prepaid card activities, as well as prior AML/CFT Bank Examination and Audit Reports, select a sample of e-cash transactions. **From the sample selected perform the following examination procedures:**

    i. Review account opening documentation, including CIP, ongoing CDD and transaction history.
    ii. Compare expected activity with actual activity.
    iii. Determine whether the activity is consistent with the nature of the customer's business.
    iv. Identify any unusual or suspicious activity.

5 On the basis of AML/CFT examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with e-cash relationships.

65. OVERVIEW OF THIRD-PARTY PAYMENT PROCESSORS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with its relationships with third-party payment processors and the management's ability to implement effective monitoring and reporting systems.

Non-bank or third-party payment processors (processors) are bank or other financial institution customers that provide payment-processing services to merchants and other business entities. Traditionally, processors primarily contract with retailers that have physical locations in order to process the retailers' transactions.

These merchant transactions primarily included credit card payments but also covered automated clearing house (ACH) transactions, **Remotely Created Cheques (RCCs),** debit and prepaid cards transactions. With the expansion of the internet, retail borders have been eliminated. Processors now provide services to a variety of merchant accounts, including conventional retail and internet-based establishments, prepaid travel, telemarketers and internet gaming enterprises.

Third-party payment processors often use their commercial bank accounts to conduct payment processing for their merchant clients. For example, the processor may deposit into its account RCCs generated on behalf of a merchant client, or act as a third-party sender of ACH transactions. In either case, the financial institution does not have a direct relationship with the merchant. The increased use by processor customers, particularly telemarketers of RCCs also raises the risk of fraudulent payments being processed through the processor's bank account.

Risk Factors

Processors generally are not subject to AML/CFT compliance and regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes and illicit transactions or transactions prohibited by MLPA 2004.

The financial institution's ML/FT risks when dealing with a processor account are similar to risks from other activities in which the financial institution's customer conducts transactions through the bank on behalf of the customer's clients. When the financial institution is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the financial institution and the likelihood of suspicious activity can increase. If a financial institution has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanction-able transactions.

Risk Mitigation

Financial institutions offering account services to processors should develop and maintain adequate policies, procedures and processes to address risks related to

these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. **A financial institution may assess the risks associated with payment processors by considering the following:**

i. Implementing a policy that requires an initial background check of the processor (using for example, state incorporation departments, internet searches and other investigative processes) and of the processor's underlying merchants on a risk-adjusted basis in order to verify their creditworthiness and general business practices.
ii. Reviewing the processor's promotional materials, including its Web site to determine the target clientele. A financial institution may develop policies, procedures and processes that restrict the types of entities for which it will allow processing services. These entities may include higher risk entities such as offshore companies, online gambling-related operations, telemarketers and online pay lenders. These restrictions should be clearly communicated to the processor at account opening stage.
iii. Determining whether the processor re-sells its services to a third party who may be referred to as an agent or provider of independent sales institution opportunities or internet service provider (gateway) arrangements.
iv. Reviewing the processor's policies, procedures and processes to determine the adequacy of its due diligence standards for new merchants.
v. Requiring the processor to identify its major customers by providing information such as the merchant's name, principal business activity and geographic location.
vi. Verifying directly or through the processor that the merchant is operating a legitimate business by comparing the merchant's identifying information against public record databases, fraud and financial institution check databases.
vii. Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
viii. Visiting the processor's business operations centre.

Financial institutions which provide account services to third-party payment processors should monitor their processor relationships for any significant changes in the processor's business strategies that may affect their risk profile. Financial institutions should periodically re-verify and update the processors' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. **To effectively monitor these accounts, the financial institution should have an understanding of the following processor information:**

i. Merchant base.
ii. Merchant activities.
iii. Average number of dollar/Naira volume and number of transactions.
iv. "Swiping" versus "keying" volume for credit card transactions.
v. Charge-back history, including rates of return for ACH debit transactions and Remotely Created Cheques (RCCs).

vi. Consumer complaints that suggest a payment processor's merchant clients are inappropriately obtaining personal account information and using it to create unauthorized RCCs or ACH debits.

With respect to account monitoring, a financial institution should thoroughly investigate high levels of returns and should not accept high levels of returns on the basis that the processor has provided collateral or other security to the financial institution. A financial institution should implement appropriate policies, procedures and processes that address compliance and fraud risks. High levels of RCCs or ACH debits returned for insufficient funds or as unauthorized can be an indication of fraud or suspicious activity.

66. EXAMINATION PROCEDURES OF THIRD-PARTY PAYMENT PROCESSORS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with its relationships with third-party payment processors, and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to third-party payment processors (processors). Evaluate the adequacy of the policies, procedures and processes given the financial institution's processor activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors processor relationships, particularly those that pose a higher risk for money laundering.
3. Determine whether the financial institution's system for monitoring processor accounts for suspicious activities and for reporting suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its processor activities as well as prior AML/CFT Bank Examination and Audit Reports, select a sample of higher-risk processor accounts. **From the sample selected:**
    i. Review account opening documentation and ongoing due diligence information.
    ii. Review account statements and, as necessary, specific transaction details to determine how expected transactions compare with actual activity.
    iii. Determine whether actual activity is consistent with the nature of the processor's stated activity.

iv. Assess the controls concerning identification of high rates of unauthorized returns and the process in place to address compliance and fraud risks.
v. Identify any unusual or suspicious activity.

5 .On the basis of the AML/CFT examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with processor accounts.

67. OVERVIEW OF PURCHASE AND SALE OF MONETARY INSTRUMENTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with monetary instrument and the management's ability to implement effective monitoring and reporting systems.

This section expands the core review of statutory and regulatory requirements for purchase and sale of monetary instruments in order to provide a broader assessment of the money laundering risks associated with this activity.

Monetary instruments are products provided by financial institutions and include cashier's cheques, traveller's cheques, and money orders. Monetary instruments are typically purchased to pay for commercial or personal transactions and, in the case of traveller's cheques, as a form of stored value for future purchases.

Risk Factors

The purchase or exchange of monetary instruments at the placement and layering stages of money laundering can conceal the source of illicit proceeds. As a result, financial institutions have been major targets in laundering operations because they provide and process monetary instruments through deposits. For example, customers or non-customers have been known to purchase monetary instruments in amounts below the reportable currency threshold to avoid having to provide adequate identification. Subsequently, monetary instruments are then placed into deposit accounts to circumvent the CTR filing threshold.

Risk Mitigation

Financial Institutions selling monetary instruments should have appropriate policies, procedures and processes in place to mitigate risk. **Policies should define:**

i. Acceptable and unacceptable monetary instrument transactions (e.g., non-customer transactions, monetary instruments with blank payees, unsigned monetary instruments, identification requirements for structured transactions, or

the purchase of multiple sequentially numbered monetary instruments for the same payee).

ii. Procedures for reviewing for unusual or suspicious activity, including elevating concerns to management.

iii. Criteria for closing relationships or refusing to do business with non-customers who have consistently or egregiously been involved in suspicious activity.

68. EXAMINATION PROCEDURES OF PURCHASE AND SALE OF MONETARY INSTRUMENTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with monetary instrument and the management's ability to implement effective monitoring and reporting systems.
This section expands the core review of statutory and regulatory requirements for purchase and sale of monetary instruments in order to provide a broader assessment of the money laundering risks associated with this activity.

1. Review the policies, procedures, and processes related to the sale of monetary instruments. Evaluate the adequacy of the policies, procedures and processes given the financial institution's monetary instruments activities and the risks they present. Assess whether controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From the volume of sales and the number of locations that monetary instruments are sold, determine whether the financial institution appropriately manages the risk associated with monetary instrument sales.
3. Determine whether the financial institution's system for monitoring monetary instruments for suspicious activities and for reporting suspicious activities is adequate given the financial institution's volume of monetary instrument sales, size, complexity, location and types of customer relationships. **Determine whether suspicious activity monitoring and reporting systems (either manual or automated) include a review of:**

    i. Sales of sequentially numbered monetary instruments from the same or different purchasers on the same day to the same payee.
    ii. Sales of monetary instruments to the same purchaser or sales of monetary instruments to different purchasers made payable to the same remitter.
    iii. Monetary instrument purchases by non-customers.
    iv. Common purchasers, payees, addresses, sequentially numbered purchases and unusual symbols.

Transaction Testing

4. On the basis of the financial institution's risk assessment, as well as prior RBS AML/CFT Bank Examination and Audit Reports, select a sample of monetary instrument transactions for both customers and noncustomers from:

    i. Monetary instrument sales records.
    ii. Copies of cleared monetary instruments purchased with currency.

5. From the sample selected, analyze transaction information to determine whether amounts, the frequency of purchases and payees are consistent with expected activity for customers or non-customers (e.g., payments to utilities or household purchases). Identify any suspicious or unusual activity.

6. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with monetary instruments.

69. OVERVIEW OF BROKERED DEPOSITS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with brokered deposit relationship and the management's ability to implement effective due diligence, monitoring and reporting systems.

The use of brokered deposits is a common funding source for many banks and other financial institutions. **Recent technology developments allow brokers to provide bankers with increased access to a broad range of potential investors who have no relationship with the bank and/or other financial institutions. Deposits can be raised over the internet through certificates of deposit listing services or through other advertising methods.**

Deposit brokers provide intermediary services for financial institutions and investors. This activity is considered higher risk because each deposit broker operates under its own guidelines for obtaining deposits. The level of regulatory oversight over deposit brokers varies, as the applicability of AML/CFT Regulatory requirements directly on the deposit broker varies. However, the deposit broker is subject to other statutory requirements regardless of its regulatory status. Consequently, the deposit broker may not be performing adequate customer due diligence. The financial institution accepting brokered deposits depends on the deposit broker to sufficiently perform required account opening procedures and to follow applicable AML/CFT Compliance Program requirements.

Risk Factors

Money laundering and terrorist financing risks arise because the financial institution may not know the ultimate beneficial owners or the source of funds. The deposit broker could represent a range of clients that may be of higher risk for money laundering and terrorist financing (e.g., non-resident or offshore customers, politically exposed persons (PEP) or foreign shell banks).

Risk Mitigation

Financial institutions which accept deposit broker accounts or funds should develop appropriate policies, procedures and processes that establish minimum CDD procedures for all deposit brokers providing deposits to the bank or other financial institution. The level of due diligence performed by a financial institution should be commensurate with its knowledge of the deposit broker and the deposit broker's known business practices and customer base.

In an effort to address the risk inherent in certain deposit broker relationships, financial institutions may want to consider having a signed contract that sets out the roles and responsibilities of each party and restrictions on types of customers (e.g., non-resident or offshore customers, PEPs or foreign shell banks). Financial institutions should conduct sufficient due diligence on deposit brokers, especially unknown, foreign, independent or unregulated deposit brokers. **To manage the ML/FT risks associated with brokered deposits, the financial institution should:**

i. Determine whether the deposit broker is a legitimate business in all operating locations where the business is conducted.
ii. Review the deposit broker's business strategies, including targeted customer markets (e.g., foreign or domestic customers) and methods for soliciting clients.
iii. Determine whether the deposit broker is subject to regulatory oversight.
iv. Evaluate whether the deposit broker's AML/CFT compliance policies, procedures, and processes are adequate (e.g., ascertain whether the deposit broker performs sufficient CDD including CIP procedures).
v. Evaluate the adequacy of the deposit broker's AML/CFT audits and ensure that they address compliance with applicable regulations and requirements.

Institutions to take particular care in their oversight of deposit brokers in adequately regulated entities

i. Are unknown to the financial institution.
ii. Conduct business or obtain deposits primarily in other jurisdictions.
iii. Use unknown businesses and financial institutions for references.
iv. Provide other services that may be suspect, such as creating shell companies for foreign clients.
v. Refuse to provide requested audit and due diligence information or insist on placing deposits before providing this information.
vi. Use technology that provides anonymity to customers.

Financial institutions should also monitor existing deposit broker relationships for any significant changes in business strategies that may influence the broker's risk profile. As

such, financial institutions should periodically re-verify and update each deposit broker's profile to ensure an appropriate risk assessment.

70. EXAMINATION PROCEDURES OF BROKERED DEPOSITS

Objective

Assess the adequacy of the bank's or other financial institution's systems to manage the risks associated with brokered deposit relationships and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the policies, procedures and processes related to deposit broker relationships. Evaluate the adequacy of the policies, procedures and processes given the financial institution's deposit broker activities and the risks that they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the bank effectively identifies and monitors deposit broker relationships, particularly those that pose a higher risk for money laundering.
3. Determine whether the financial institution's system for monitoring deposit broker relationships for suspicious activities and for reporting suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its brokered deposit activities as well as prior AML/CFT Bank Examination and Audit Reports, select a sample of higher-risk deposit broker accounts. **When selecting a sample, Examiners should consider the following:**

i. New relationships with deposit brokers.
ii. The method of generating funds (e.g., internet brokers).
iii. Types of customers (e.g., non-resident or offshore customers, politically exposed persons or foreign shell banks or other financial institution).
iv. A deposit broker that has appeared in the financial institution's STRs.
v. Subpoenas served on the financial institution for a particular deposit broker.
vi. Foreign funds providers.
vii. Unusual activity.

5. Review the customer due diligence information on the deposit broker. For deposit brokers who are considered higher risk (e.g., they solicit foreign funds or market via the internet or are independent brokers) assess whether the following information is available:

i. Background and references.

ii. Business and marketing methods.
iii. Client-acceptance and due diligence practices.
iv. The method for or basis of the broker's compensation or bonus program.
v. The broker's source of funds.
vi. Anticipated activity or transaction types and levels (e.g., funds transfers).

6 On the basis of RBS AML/CFT examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with deposit brokers.

71. OVERVIEW OF NON-DEPOSIT INVESTMENT PRODUCTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with both networking and in-house non-deposit investment products (NDIP) and the management's ability to implement effective monitoring and reporting systems.

NDIP include a wide array of investment products (e.g., securities, bonds and fixed or variable annuities). Sales programs may also include cash management sweep accounts to retail and commercial clients; these programs are offered by the bank directly. Banks and other financial institutions offer these investments to increase fee income and provide customers with additional products and services. The manner in which the NDIP relationship is structured and the methods with which the products are offered substantially affect the bank's/other financial institution's ML/FT risks and responsibilities.

In-House Sales and Proprietary Products

The financial institution is fully responsible for in-house NDIP transactions completed on behalf of its customers either with or without the benefit of an internal broker/dealer employee. In addition, the bank or other financial institution may also offer its own proprietary NDIPs which can be created and offered by the bank or other financial institution, its subsidiary or affiliate.

With in-house sales and proprietary products, the entire customer relationship and all ML/FT risks may need to be managed by the financial institution, depending on how the products are sold.

Risk Factors

ML/FT risks arise because NDIP can involve complex legal arrangements, large amounts and the rapid movement of funds. NDIP portfolios managed and controlled directly by

clients pose a greater money laundering risk than those managed by the bank or other financial services provider. Sophisticated clients may create ownership structures to obscure the ultimate control and ownership of these investments. For example, customers can retain a certain level of anonymity by creating Private Investment Companies (PIC), offshore trusts or other investment entities that hide the customer's ownership or beneficial interest.

Risk Mitigation

Management should develop risk-based policies, procedures and processes that enable the bank/other financial institution to identify unusual account relationships and circumstances, questionable assets and sources of funds and other potential areas of risk (e.g., offshore accounts, agency accounts and unidentified beneficiaries). Management should be alert to situations that need additional review or research.

Networking Arrangements

Before entering into a networking arrangement, financial institutions should conduct an appropriate review of the broker/dealer. The review should include an assessment of the broker/dealer's financial status, management experience, Securities Dealers status, reputation and ability to fulfil its AML/CFT compliance responsibilities as regards the financial institution's customers. Appropriate due diligence would include a determination that the broker/dealer has adequate policies, procedures and processes in place to enable the broker/dealer meet its legal obligations. The financial institution should maintain documentation on its due diligence of the broker/dealer. Furthermore, detailed written contracts should address the AML/CFT responsibilities, including suspicious activity monitoring and reporting of the broker/dealer and its registered representatives.

A financial institution may also want to mitigate risk exposure by limiting certain investment products offered to its customers. Investment products such as PICs, offshore trusts or offshore hedge funds (may involve international funds transfers) are offered to customers as a way to obscure ownership interests.

Financial institution management should develop and put in place structure that can update due diligence information on the broker/dealer. Such structures should include a periodic review of information on the broker/dealer's compliance with its AML/CFT responsibilities, verification of the broker/dealer's record in meeting testing requirements and a review of consumer complaints. Financial institution management is also encouraged, when possible, to review AML/CFT reports generated by the broker/dealer. This review could include information on account openings, transactions, investment products sold and suspicious activity monitoring and reporting.

In-House Sales and Proprietary Products

Assess risk on the basis of a variety of factors such

i. Type of NDIP purchased and the size of the transactions.
ii. Types and frequency of transactions.
iii. Country of residence of the principals or beneficiaries, the country of incorporation or the source of funds.
iv. Accounts and transactions that are not usual and customary for the customer or for the financial institution.

For customers that management considers higher risk for money laundering and terrorist financing, more stringent documentation, verification and transaction monitoring procedures should be established. **EDD may be appropriate in the following situations:**

i. Financial institution is entering into a relationship with a new customer.
ii. Non-discretionary accounts have a large asset size or frequent transactions.
iii. Customer resides in a foreign jurisdiction.
iv. Customer is a PIC or other corporate structure established in a higher-risk jurisdiction.
v. Assets or transactions are typical for the customer.
vi. Investment type, size, assets or transactions are typical for the financial institution.
vii. International funds transfers are conducted, particularly from offshore funding sources.
viii. The identities of the principals or beneficiaries in investments or relationships are unknown or cannot be easily determined.
ix. Politically Exposed persons (PEPs) are parties to any investments or transactions.

72. EXAMINATION PROCEDURES OF NON-DEPOSIT INVESTMENT PRODUCTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with both networking and in-house non-deposit investment products (NDIP) and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to NDIP. Evaluate the adequacy of the policies, procedures and processes given the financial institution's NDIP activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. If applicable, review contractual arrangements with financial service providers. Determine the AML/CFT compliance responsibility of each party. Determine whether these arrangements provide for adequate AML/CFT oversight and control functions.

3. From a review of MIS reports (e.g., exception reports, funds transfer reports and activity monitoring reports) and internal risk rating factors, determine whether the financial institution effectively identifies and monitors NDIP, particularly those that pose a higher risk for money laundering.
4. Determine how the financial institution includes NDIP sales activities in its institution-wide AML/CFT aggregation systems.
5. Determine whether the financial institution's system for monitoring NDIP and for reporting suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

6. If the financial institution or its majority-owned subsidiary is responsible for the sale or direct monitoring of NDIP, then the E**xaminers should perform transaction testing procedures on customer accounts established by the financial institution.**

7. On the basis of the financial institution's risk assessment of its NDIP activities as well as prior AML/CFT Bank Examination and Audit Reports, select a sample of higher-risk NDIP. **From the sample selected, perform the following examination procedures:**

   i. Review appropriate documentation including CIP to ensure that adequate due diligence has been performed and appropriate records are maintained.
   ii. Review account statements and (as necessary) specific transaction details for:
      a. Expected transactions with actual activity.
      b. Holdings in excess of the customer's net worth.
      c. c. Irregular trading patterns (e.g., incoming funds transfers to purchase securities followed by delivery of securities to another custodian shortly thereafter).
   iii. Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account. Identify any unusual or suspicious activity.

8. On the basis of RBS AML/CFT examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with NDIP sales activities.

73. OVERVIEW OF INSURANCE PRODUCTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with the sale of covered insurance products and the management's ability to implement effective monitoring and reporting systems.

1. Financial institutions engage in insurance sales to increase their profitability, mainly through expanding and diversifying fee-based income. Insurance products are typically sold to financial institution customers through networking arrangements with an affiliate, an operating subsidiary or other third-party insurance providers.

2. Financial institutions are also interested in providing cross-selling opportunities for customers by expanding the insurance products they offer. Typically, financial institutions take a role as a third-party agent selling covered insurance products. The types of insurance products sold may include life, health, property & casualty, and fixed or variable annuities.

AML/CFT Compliance Programs and Suspicious Transaction Reporting Requirements for Insurance Companies

The insurance regulations apply only to insurance companies, there are no independent obligations for brokers and agents. However, the insurance company is responsible for the conduct and effectiveness of its AML/CFT Compliance Program, which includes agent and broker activities. The insurance regulations only apply to a limited range of products that may pose a higher risk of abuse by money launderers and terrorist financiers. **A covered product for the purposes of an AML/CFT Compliance Program includes:**

i. A permanent life insurance policy other than a group life insurance policy.
ii. Any annuity contract other than a group annuity contract.
iii. Any other insurance product with features of cash value or investment.

When an insurance agent or broker is already required to establish an AML/CFT Compliance Program under a separate requirement of the regulations issued by National Insurance Corporation of Nigeria (NAICOM) (e.g., financial institution or securities broker requirements), the insurance company generally may rely on that Compliance Program to address issues at the time of sale of the covered product. However, the financial institution may need to establish specific policies, procedures and processes for its insurance sales in order to submit information to the insurance company for the insurance company's AML/CFT compliance.

Risk Factors

Insurance products can be used to facilitate money laundering. For example, currency can be used to purchase one or more life insurance policies, which may subsequently and quickly be cancelled by a policyholder (also known as "early surrender") for a penalty. The insurance company refunds the money to the purchaser in the form of a cheque. Insurance policies without cash value or investment features are lower risk, but can be used to launder money or finance terrorism through the submission by a policyholder of inflated or false claims to its insurance carrier, which if paid, would enable the insured to recover a part or all of the originally invested payments.

Other ways insurance products can be used to launder money

i. Borrowing against the cash surrender value of permanent life insurance policies.
ii. Selling units in investment-linked products (such as annuities).
iii. Using insurance proceeds from an early policy surrender to purchase other financial assets.
iv. Buying policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer (e.g., second-hand endowment and bearer insurance policies).
v. Purchasing insurance products through unusual methods such as currency or currency equivalents.
vi. Buying products with insurance termination features without concern for the product's investment performance.

Risk Mitigation

To mitigate money laundering risks the financial institution should adopt policies, procedures and processes that include:

i. The identification of higher-risk accounts.
ii. Customer due diligence, including EDD for higher-risk accounts.
iii. Product design & use, types of services offered and unique aspects or risks of target markets.
iv. Employee compensation and bonus arrangements that are related to sales.
v. Monitoring, including the review of early policy terminations and the reporting of unusual and suspicious transactions (e.g., a single, large premium payment, a customer's purchase of a product that appears to fall outside the customer's normal range of financial transactions, early redemptions, multiple transactions, payments to apparently unrelated third parties and collateralized loans).
vi. Recordkeeping requirements.

74. EXAMINATION PROCEDURES OF INSURANCE PRODUCTS

Objective

Assess the adequacy of the financial institution's systems to manage the ML/FT risks associated with the sale of covered insurance products and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to insurance sales. Evaluate the adequacy of the policies, procedures and processes given the financial institution's insurance sales activities, its role in insurance sales and the risks the insurance sales present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. Review the contracts and agreements for the financial institution's networking arrangements with affiliates, operating subsidiaries or other third-party insurance

providers conducting sales activities on financial institution premises on behalf of the financial institution.

3. Depending on the financial institution's responsibilities as set forth in the contracts and agreements, review MIS reports (e.g., large and unusual transaction reports, single premium payments, early policy cancellation records, premium overpayments and assignments of claims) and internal risk rating factors. Determine whether the financial institution effectively identifies and monitors covered insurance product sales.
4. Depending on the financial institution's responsibilities as set forth in the contracts and agreements, determine whether the financial institution's system for monitoring covered insurance products for suspicious activities and for reporting suspicious transactions is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

If the financial institution or its majority-owned subsidiary is responsible for the sale or direct monitoring of insurance, then Bank Examiners should perform the transaction testing procedures.

5. On the basis of the financial institution's risk assessment of its insurance sale transactions as well as prior examination and audit reports, select a sample of covered insurance products. **From the sample selected, perform the following examination procedures:**

i. Review account opening documentation (KYC requirements) and on-going due diligence information.
ii. Review account activity. Compare anticipated transactions with actual transactions.
iii. Determine whether activity is unusual or suspicious.

6. On the basis of the completed examination procedures including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with insurance sales.

75. OVERVIEW OF CONCENTRATION ACCOUNTS

Objective

Assess the adequacy of the financial institution's systems to manage the AML/CFT risks associated with concentration accounts and the management's ability to implement effective monitoring and reporting systems.

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the financial institution, usually on the same day. These accounts may also be **known as special-use, omnibus, suspense, settlement, intra-day, sweep, or collection accounts.** Concentration accounts are frequently **used to**

facilitate transactions for private banking, trust & custody accounts, funds transfers and international affiliates.

Risk factors

Money laundering risk can arise in concentration accounts if the customer-identifying information such as name, transaction amount and account number are separated from the financial transaction. If separation occurs, the audit trail is lost and accounts may be misused or administered improperly. Financial institution that use concentration accounts should implement adequate policies, procedures and processes covering the operation and recordkeeping for these accounts. Policies should establish guidelines to identify, measure, monitor and control the risks.

Risk mitigation

Because of the risks involved, management should be familiar with the nature of their customers' businesses and with the transactions flowing through the financial institution's concentration accounts. Additionally, the monitoring of concentration account transactions is necessary to identify and report unusual or suspicious transactions.
Internal controls are necessary to ensure that processed transactions include the identifying customer information. Retaining complete information is crucial for compliance with regulatory requirements as well as ensuring adequate transaction monitoring. **Adequate internal controls may include:**

i. Maintaining a comprehensive system that identifies (institution-wide) the general ledger accounts used as concentration accounts, as well as the departments and individuals authorized to use those accounts.
ii. Requiring dual signatures on general ledger tickets.
iii. Prohibiting direct customer access to concentration accounts.
iv. Capturing customer transactions in the customer's account statements.
v. Prohibiting customer's knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
vi. Retaining appropriate transaction and customer identifying information.
vii. Frequent reconciling of the accounts by an individual who is independent from the transactions.
viii. Establishing timely discrepancy resolution process.
ix. Identifying recurring customer names.

76. EXAMINATION PROCEDURES OF CONCENTRATION ACCOUNTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with concentration accounts and the management's ability to implement effective monitoring and reporting systems.

1. Review the policies, procedures and processes related to concentration accounts. Evaluate the adequacy of the policies, procedures and processes in relation to the financial institution's concentration account activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors concentration accounts.

3. Review the general ledger and identify any concentration accounts. After discussing concentration accounts with management and conducting any additional research needed, obtain and review a list of all concentration accounts and the financial institution's most recent reconciliation statements.

4. Determine whether the financial institution's system for monitoring concentration accounts for STRs and for reporting of STRs is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction testing

5. On the basis of the financial institution's risk assessment of its concentration accounts as well as prior examination and audit reports, select a sample of concentration accounts. **From the sample selected, perform the following examination procedures:**

i. Obtain account activity reports for selected concentration accounts.
ii. Evaluate the activity and select a sample of transactions passing through different concentration accounts for further review.
iii. Focus on higher-risk activity (e.g., funds transfers or monetary instruments purchases) and transactions from higher-risk jurisdictions.

6. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with concentration accounts.

77. OVERVIEW OF LENDING ACTIVITY

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with lending activities and the management's ability to implement effective due diligence, monitoring and reporting systems.

Lending activities include, but are not limited to real estate, trade finance, cash-secured, credit card, consumer, commercial and agricultural. Lending activities can include multiple parties (e.g., guarantors, signatories, principals, or loan participants).

Risk factors

The involvement of multiple parties may increase the risk of money laundering or terrorist financing when the source and use of the funds are not transparent. This lack of transparency can create opportunities in any of the three stages of money laundering or terrorist financing schemes. **These schemes could include the following:**

i. To secure a loan, an individual purchases a certificate of deposit with illicit funds.
ii. Loans are made for an ambiguous or illegitimate purpose.
iii. Loans are made or paid for a third party.
iv. The bank or the customer attempts to sever the paper trail between the borrower and the illicit funds.
v. Loans are extended to persons located outside Nigeria, particularly to those in higher-risk jurisdictions and geographic locations. Loans may also involve collateral located outside the country.

Risk mitigation

All loans are required to meet purposes that are compliant with the KYC regulations. For loans that may pose a higher risk of money laundering and terrorist financing, including the loans listed above, the financial institution should complete due diligence on related account parties (i.e., guarantors, signatories or principals). **Due diligence beyond what is required for a particular lending activity will vary according to the ML/FT risks present, but could include performing reference checks, obtaining credit references, verifying the source of collateral and obtaining tax or financial statements on the borrower and any or all of the various parties involved in the loan.**

The bank should have policies, procedures and processes to monitor, identify and report unusual and suspicious activities. The sophistication of the systems used to monitor lending account activity should conform to the size and complexity of the bank's lending business. **For example, the bank can review loan reports such as early payoffs, past dues, fraud or cash-secured loans.**

78. EXAMINATION PROCEDURES OF LENDING ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with lending activities and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the policies, procedures and processes related to lending activities. Evaluate the adequacy of the policies, procedures and processes given the financial institution's lending activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk loan accounts.

3. Determine whether the financial institution's system for monitoring loan accounts for suspicious transactions and for reporting of suspicious transactions is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction testing

4. On the basis of the financial institution's risk assessment of its lending activities as well as prior examination and audit reports, select a sample of higher-risk loan accounts. **From the sample selected, perform the following examination procedures:**

   i. Review account opening documentation including CIP to ensure that adequate due diligence has been performed and that appropriate records are maintained.
   ii. Review as necessary the loan history.
   iii. Compare expected transactions with actual activity.
   iv. Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the loan. Identify any unusual or suspicious transaction.

5. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with lending relationships.

79. OVERVIEW OF TRADE FINANCE ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with trade finance activities and the management's ability to implement effective due diligence, monitoring and reporting systems.

Trade finance typically involves short-term financing to facilitate the import and export of goods. These operations can involve payment if documentary requirements are met (e.g., letter of credit) or may instead involve payment, if the original obligor defaults on the commercial terms of the transactions (e.g., guarantees or standby letters of credit). In both cases, a financial institution's involvement in trade finance minimizes payment risk to importers and exporters. The nature of trade finance activities, however, requires the active involvement of multiple parties on both sides of the transaction. In addition to the basic exporter or importer relationship at the center of any particular trade activity, relationships may exist between the exporter and its suppliers and between the importer and its customers.

Both the exporter and importer may also have other banking relationships. Furthermore, many other intermediary financial and non-financial institutions may provide conduits and services to expedite the underlying documents and payment flows associated with trade transactions. Financial institutions can participate in trade financing by, among other things, providing pre-export financing, helping in the collection process, confirming or issuing letters of credit, discounting drafts and acceptances or offering fee-based services such as providing credit and country information on buyers. Although most trade financing is short-term and self-liquidating in nature, medium-term loans (one to five years) or long-term loans (more than five years) may be used to finance the import and export of capital goods such as machinery and equipment.

Transactions covered by letters of credit

Applicant - The buyer or party who requests the issuance of a letter of credit.

Issuing Bank - The bank that issues the letter of credit on behalf of the applicant and advises it to the beneficiary either directly or through an advising financial institution. The applicant is the issuing bank's customer.

Confirming Bank – Typically, is in the home country of the beneficiary and at the request of the issuing bank. It is the financial institution that adds its commitment to honour draws made by the beneficiary, provided the terms and conditions of the letter of credit are met.

Advising Bank - The bank that advises the credit at the request of the issuing bank. The issuing bank sends the original credit to the advising bank for onward forwarding to the beneficiary. The advising bank authenticates the credit and advises it to the beneficiary. There may be more than one advising bank in a letter of credit transaction. The advising bank may also be a confirming bank.

Beneficiary - The seller or party to whom the letter of credit is addressed.

Negotiation - The purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) or documents under a complying presentation by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank.

Nominated Bank - The bank with which the credit is available or any bank in which the credit is available.

Accepting Bank - The bank that accepts a draft, providing a draft is called for by the credit. Drafts are drawn on the accepting bank that dates and signs the instrument.

Discounting Bank - The bank that discounts a draft for the beneficiary after it has been accepted by the accepting bank. The discounting bank is often the accepting bank.

Reimbursing Bank - The bank authorized by the issuing bank to reimburse the paying bank submitting claims under the letter of credit.

Paying Bank - The bank that makes payment to the beneficiary of the letter of credit. As an example, in a letter of credit arrangement, a bank can serve as the issuing bank, allowing its customer (the buyer) to purchase goods locally or internationally, or the bank can act as an advising bank, enabling its customer (the exporter) to sell its goods locally or internationally. The relationship between any two banks may vary and could include any of the roles listed above.

Risk factors

The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection. The involvement of **multiple parties on both sides** of any international trade transaction can make the process of due diligence more difficult. Also, because trade finance can **be more document-based than other banking activities, it can be susceptible to documentary fraud** which can be linked to money laundering, terrorist financing or the **circumvention of sanctions or other restrictions** (such as export prohibitions, licensing requirements or controls).

While financial institutions should be alert to transactions involving higher-risk goods (e.g., trade in weapons or nuclear equipment), they need to be aware that goods may be over or undervalued in an effort to evade AML/CFT requirements or customs regulations, or to move funds or value across national borders. For example, an importer may pay a large sum of money from the proceeds of an illegal activity for goods that are essentially worthless and are subsequently discarded. Alternatively, trade documents such as invoices may be fraudulently altered to hide the scheme. Variations on this theme include inaccurate or double invoicing, partial shipment of goods (short shipping) and the use of fictitious goods. Illegal proceeds transferred in such transactions thereby appear sanitized and enter the realm of legitimate commerce. Moreover, many suspect trade finance transactions also involve collusion between buyers and sellers.

The applicant's true identity or ownership may be disguised by the use of certain corporate forms such as shell companies or offshore front companies. The use of these types of entities results in a lack of transparency, effectively hiding the identity of the purchasing party and thus increasing the risk of money laundering and terrorist financing.

Risk Mitigation

Sound CDD procedures are needed to gain a thorough understanding of the customer's underlying business and locations served. The financial institutions in the letter of credit process need to undertake varying degrees of due diligence depending upon their role in the transaction. For example, issuing bank should conduct sufficient due diligence on a prospective customer before establishing the letter of credit. The due diligence should include gathering sufficient information on the applicants and beneficiaries including their identities, nature of business and sources of funding. This may require the use of background checks or investigations, particularly in higher-risk jurisdictions. As such, financial institutions should conduct a thorough review and reasonably know their customers prior to facilitating trade-related activity and should have a thorough understanding of trade finance documentation.

Likewise, guidance provided by the Financial Action Task Force (FATF) on money laundering has helped in setting important industry standards and is a resource for financial institutions that provide trade finance services. The Wolfsberg Group also has published suggested industry standards and guidance for financial institutions that provide trade finance services.

Financial institutions taking other roles in the letter of credit process should complete due diligence that is commensurate with their roles in each transaction. Financial institutions need to be aware that because of the frequency of transactions in which multiple banks are involved, issuing banks may not always have correspondent relationships with the advising or confirming bank.

To the extent feasible, financial institutions should review documentation, not only for compliance with the terms of the letter of credit, but also for anomalies or red flags that

could indicate unusual or suspicious transaction. Reliable documentation is critical in identifying potentially suspicious transaction. When analyzing trade transactions for unusual or suspicious transaction, financial institutions should consider obtaining copies of official Nigerian or foreign government import and export forms to assess the reliability of documentation provided. These anomalies could appear in shipping documentation, obvious under or over-invoicing, government licences (when required) or discrepancies in the description of goods on various documents. Identification of these elements may not, in itself, require the filing of STRs, but may suggest the need for further research and verification. In circumstances where STRs are warranted, the financial institution is not expected to stop trade or discontinue processing the transaction. However, stopping the trade may be required to avoid a potential violation of the Money Laundering (Prohibition) Act and its sanctions.

Trade finance transactions frequently use **Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages.** Nigerian financial institutions must comply with relevant regulations and when necessary, provide funding in advance of consummating the deal involved. Financial institutions should monitor the names of the parties contained in these messages and compare the names against terrorist lists. Financial institutions with a high volume of SWIFT messages should determine whether their monitoring efforts are adequate to detect suspicious transaction, particularly if the monitoring mechanism is not automated.
Policies, procedures and processes should also require a thorough review of all applicable trade documentation (e.g., customs declarations, trade documents, invoices, etc) to enable the financial institution to monitor and report unusual and suspicious transactions based on the role played by the financial institution in the letter of credit process. The sophistication of the documentation review process and MIS should be commensurate with the size and complexity of the financial institution's trade finance portfolio and its role in the letter of credit process. **The monitoring process should give greater scrutiny to:**

i. Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products or an information technology company that starts dealing in bulk pharmaceuticals).
ii. Customers conducting business in higher-risk jurisdictions.
iii. Customers shipping items through higher-risk jurisdictions including transit through non -cooperative countries.
iv. Customers involved in potentially higher-risk activities including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil).
v. Obvious over or under-pricing of goods and services.
vi. Obvious misrepresentation of quantity or type of goods imported or exported.
vii. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
viii. Customer directs payment of proceeds to an unrelated third party.
ix. Shipment locations or description of goods not consistent with letter of credit.

x. Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Unless customer behaviour or transaction documentation appears unusual, the financial institution should not be expected to spend undue time or effort reviewing all information. The examples above, particularly for an issuing bank, may be included as part of its routine CDD process. Financial institution with robust CDD programs may find that less focus is needed on individual transactions as a result of their comprehensive knowledge of the customer's activities.

80. EXAMINATION PROCEDURES OF TRADE FINANCE ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with trade finance activities and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the policies, procedures and processes related to trade finance activities. Evaluate the adequacy of the policies, procedures and processes governing trade finance-related activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. Evaluate the adequacy of the due diligence information the financial institution obtains for the customer's files. Determine whether the financial institution has processes in place for obtaining information at account opening in addition to ensuring current customer information is maintained.
3. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors the trade finance portfolio for suspicious or unusual activities, particularly those that pose a higher risk for money laundering.
4. Determine whether the financial institution's system for monitoring trade finance activities for suspicious activities and for reporting of suspicious activities is adequate, given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

5. On the basis of the financial institutions' risk assessment of its trade finance portfolio as well as prior examination and audit reports, select a sample of trade finance accounts. From the sample selected, review customer due diligence documentation to determine whether the information is commensurate with the customer's risk. Identify any unusual or suspicious activities.
6. Verify whether the financial institution monitors the trade finance portfolio for potential violations and unusual transactional patterns and conducts and records the results of any due diligence.

7. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with trade finance activities.

81. OVERVIEW OF PRIVATE BANKING ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with private banking activities and the management's ability to implement effective due diligence, monitoring and reporting systems.
This section expands the core review of the statutory and regulatory requirements of private banking in order to provide a broader assessment of the ML/FT risks associated with this activity.

Private banking activities are generally defined as providing personalized services to higher net worth customers (e.g., estate planning, financial advice, lending, investment management, bill paying, mail forwarding and maintenance of a residence). Private banking has become an increasingly important business line for large and diverse banking organizations and a source of enhanced fee income.

Nigerian financial institution manage private banking relationships for both domestic and international customers. Typically, thresholds of private banking service are based on the amount of assets for management and on the need for specific products or services (e.g., real estate management, closely held company oversight, money management). **The fees charged are ordinarily based on asset thresholds and the use of specific products and services.**

Private banking arrangements are typically structured to have a central point of contact (i.e., relationship officer/manager) that acts as a liaison between the client and the financial institution and facilitates the client's use of the financial institution's financial services and products.

Typical products and services offered in a private banking relationship

i. Cash management (e.g., cheque-accounts, overdraft privileges, cash sweeps and bill-paying services).
ii. Funds transfers.
iii. Asset management (e.g., trust, investment advisory, investment management and custodial and brokerage services).
iv. The facilitation of shell companies and offshore entities (e.g., private investment companies (PIC), international business corporations (IBC) and trusts).
v. Lending services (e.g., mortgage loans, credit cards, personal loans and letters of credit).

vi. Financial planning services including tax and estate planning.
vii. Custody services.
viii. Other services as requested (e.g., mail services).

Privacy and confidentiality are important elements of private banking relationships. Although customers may choose private banking services simply to manage their assets, they may also seek a confidential, safe and legal haven for their capital. When acting as a fiduciary, financial institution have statutory, contractual and ethical obligations to uphold.

Risk Factors

Private banking services can be vulnerable to money laundering schemes and past money laundering prosecutions have demonstrated that vulnerability. **Vulnerabilities to money laundering include the following:**

i. Private bankers as client advocates.
ii. Powerful clients including politically exposed persons, industrialists and entertainers.
iii. Culture of confidentiality and the use of secrecy jurisdictions or shell companies
iv. Private banking culture of lax internal controls.
v. Competitive nature of the business.
vi. Significant profit potential for the financial institution.

Risk Mitigation

Effective policies, procedures and processes can help protect financial institutions from becoming conduits for or victims of money laundering, terrorist financing and other financial crimes that are perpetrated through private banking relationships. Illicit activities through the private banking unit could result in significant financial costs and reputational risk to the financial institution. Financial impacts could include regulatory sanctions and fines, litigation expenses, the loss of business, reduced liquidity, asset seizures and freezes, loan losses and remediation expenses.

Customer Risk Assessment in Private Banking

Financial institutions should assess the risks its private banking activities pose on the basis of the scope of operations and the complexity of the financial institution's customer relationships. Management should establish a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities.

Factors to consider when identifying risk characteristics of private banking customers

i. Nature of the customer's wealth and the customer's business - The source of the customer's wealth, the nature of the customer's business and the extent to which the customer's business history presents an increased risk for money laundering

and terrorist financing. This factor should be considered for private banking accounts opened for politically exposed persons (PEP).

ii. **Purpose and anticipated activity -** The size, purpose, types of accounts, products and services involved in the relationship, and the anticipated activity of the account.

iii. **Relationship -** The nature and duration of the financial institution's relationship (including relationships with affiliates) with the private banking customer.

iv. **Customer's corporate structure** - Type of corporate structure (Private, public, **holding, etc).**

v. **Geographic location and jurisdiction -** The geographic location of the private banking customer's domicile and business (domestic or foreign). The review should consider the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or conversely, is considered to have robust AML/CFT standards.

vi. **Public information -** Information known or reasonably available to the financial institution about the private banking customer. The scope and depth of this review should depend on the nature of this relationship and the risks involved.

Customer Due Diligence

Customer Due Diligence (CDD) is essential when establishing any customer relationship and it is critical for private banking clients. Financial institutions should take reasonable steps to establish the identity of their private banking clients and as appropriate, the beneficial owners of accounts. Adequate due diligence should vary based on the risk factors identified previously. Policies, procedures and processes should define acceptable CDD for different types of products, services and account holders. As due diligence is an ongoing process, a financial institution should take measures to ensure account profiles are current and monitoring should be risk-based. Financial institutions should consider whether risk profiles should be adjusted or suspicious transaction reported when the activity is inconsistent with the profile.

For purposes of the customer identification program (CIP), the financial institution is not required to search the private banking account to verify the identities of beneficiaries. Instead, it is required to verify the identity of the named account holder only. However, the **CIP rule also provides that** based on the financial institution's risk assessment of a new account opened by a customer that is not an individual (e.g., private banking accounts opened for a PIC), the institution may need "to obtain information about" individuals with authority or control over such an account, including signatories in order to verify the customer's identity to determine whether the account is maintained for non-Nigerians.

Information from the private banking clients before opening account

i. Purpose of the account.
ii. Type of products and services to be used.

iii. Anticipated account activity.
iv. Description and history of the source of the client's wealth.
v. Client's estimated net worth, including financial statements.
vi. Current source of funds for the account.
vii. References or other information to confirm the reputation of the client.

Bearer Shares of Shell Companies

Some shell companies issue bearer shares. **Bearer shares allow their ownership to be vested on their bearer and the ownership of the company to therefore be conveyed by simply transferring of the physical possession of the shares.** Risk mitigation of shell companies that issue bearer shares may include maintaining control of the bearer shares, entrusting the shares with a reliable independent third party or requiring periodic certification of ownership. Financial institutions should assess the risks these relationships pose and determine the appropriate controls. For example, in most cases, financial institutions should choose to maintain (or have an independent third party maintain) bearer shares for their customers. In rare cases that involve lower-risk, well-known, long-time customers, financial institutions may find that periodically re-certifying of the beneficial ownership is effective. A strong CDD program is an effective underlying control through which financial institutions can determine the nature, purpose and expected use of shell companies and apply appropriate monitoring and documentation standards.

Board of Directors and Senior Management Oversight of Private Banking Activities

The board of directors' and senior management's active oversight of private banking activities and the creation of an appropriate corporate governance oversight culture are crucial elements of a sound risk management and control environment. **The purpose and objectives of the institution's private banking activities should be clearly identified and communicated by the board and senior management.** Well-developed goals and objectives should describe the target client base in terms of minimum net worth, investable assets, types of products and services sought. Goals and objectives should also specifically describe the types of clients the financial institution will and will not accept and should establish appropriate levels of authorization for new-client acceptance. Board and senior management should also be actively involved in establishing control and risk management goals for private banking activities, including effective audit and compliance reviews. Each financial institution should ensure that its policies, procedures and processes for conducting private banking activities are evaluated and updated regularly and ensure that roles, responsibilities and accountability are clearly delineated.

Employee compensation plans are often based on the number of new accounts established or on an increase in the managed assets. Board and senior management should ensure that compensation plans do not create incentives for employees to ignore appropriate due diligence and account opening procedures or possible suspicious

activity relating to the account. Procedures that require various levels of approval for accepting new private banking accounts can minimize such opportunities.
Given the sensitive nature of private banking and the potential liability associated with it, financial institutions should thoroughly investigate the background of newly hired private banking relationship managers. During the course of employment, any indications of inappropriate activities should be promptly investigated by the financial institution.

Additionally, when private banking relationship managers change employers, their customers often move with them. Financial institutions bear the same potential liability for the existing customers of newly hired officers as they do for any new, private banking relationship. Therefore, those accounts should be promptly reviewed using the financial institution's procedures for establishing new account relationships.

MIS and reports are also important in effectively supervising and managing private banking relationships and risks. Board and senior management should review relationship manager compensation reports, budget or target comparison reports and applicable risk management reports. Private banker MIS reports should enable the relationship manager to view and manage the whole client and any related client relationships.

82. EXAMINATION PROCEDURES OF PRIVATE BANKING ACTIVITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with private banking activities and the management's ability to implement effective due diligence, monitoring and reporting systems.

This section expands the core review of the statutory and regulatory requirements of private banking in order to provide a broader assessment of the ML/FT risks associated with this activity.

1. Review the policies, procedures and processes related to private banking activities. Evaluate the adequacy of the policies, procedures and processes given the financial institution's private banking activities and the risks they represent. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS reports (e.g., customer aggregation, policy exception and missing documentation, customer risk classification, unusual accounts activity and client concentrations) and internal risk rating factors, determine whether the financial institution effectively identifies and monitors private banking relationships, particularly those that pose a higher risk for money laundering.
3. Determine whether the financial institution's system for monitoring private banking relationships for suspicious activities and for reporting of suspicious activities is

adequate given the financial institution's size, complexity, location and types of customer relationships.

4. Review the private banking compensation program. Determine whether it includes qualitative measures that are provided to employees to comply with account opening and suspicious transaction monitoring and reporting requirements.
5. Review the monitoring program the financial institution's uses to oversee the private banking relationship manager's personal financial condition and to detect any inappropriate activities.

Transaction Testing

6. On the basis of the financial institution's risk assessment of its private banking activities as well as prior examination and audit reports, select a sample of private banking accounts. **The sample should include the following types of accounts:**

   i. Politically exposed persons (PEP).
   ii. Private investment companies (PIC), international business corporations (IBC) and shell companies.
   iii. Offshore entities.
   iv. Cash-intensive businesses.
   v. Import or export companies.
   vi. Customers from or doing business in a higher-risk geographic location.
   vii. Customers listed on unusual activity monitoring reports.
   viii. Customers who have large currency transactions and frequent funds transfers.

7. From the sample selected, **perform the following examination procedures:**
   i. Review the account opening documentation and ongoing due diligence information.
   ii. Review account statements and as necessary, specific transaction details.
   iii. Compare expected transactions with actual activity.
   iv. Determine whether actual activity is consistent with the nature of the customer's business.
   v. Identify any unusual or suspicious activity.

8. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with private banking relationships.

9. Update Risk Assessment Summary and Knowledge of Business of the financial institution.

83. OVERVIEW OF TRUST AND ASSET MANAGEMENT SERVICES

Objective

Assess the adequacy of the financial institution's policies, procedures, processes and systems to manage the ML/FT risks associated with trust and asset management services and the management's ability to implement effective due diligence, monitoring and reporting systems.

Trust accounts are generally defined as a legal arrangement in which one party (the trustor or grantor) transfers ownership of assets to a person or bank/other financial institution (the trustee) to be held or used for the benefit of others. These arrangements include the broad categories of court-supervised accounts (e.g., executorships and guardianships), personal trusts (e.g., living trusts, trusts established under a will, charitable trusts) and corporate trusts (e.g., bond trusteeships).

Agency accounts are established by contract and governed by contract law. Assets are held under the terms of the contract and legal title or ownership does not transfer to the financial institution as agent. **Agency accounts include custody, escrow, investment management and safekeeping relationships.** Agency products and services may be offered in a traditional trust department or through other financial institution departments.

Customer Identification Program

Customer identification program (CIP) rules apply to all financial institutions' accounts. **The CIP rule defines an "account" to include cash management, safekeeping, custodian and trust relationships but excludes employee benefit accounts.**

For purposes of the CIP, the financial institution is not required to search the trust, escrow or similar accounts to verify the identities of beneficiaries. Instead, it is required to verify the identity of the named accountholder (the trust) only. In the case of a trust account, the customer is the trust whether or not the financial institution is the trustee for the trust. However, the CIP rule also provides that, based on the financial institution's ML/FT risk assessment of a new account opened by a customer that is not an individual, the financial institution may need "to obtain information about" individuals with authority or control over such an account, including the signatories in order to verify the customer's identity.

For example, in certain circumstances involving revocable trusts, the financial institution may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee and who thus have authority or control over the account in order to establish the true identity of the customer.

In the case of an escrow account, if a financial institution establishes an account in the name of a third party such as a real estate agent (who is acting as agent) then, the financial institution's customer is the escrow agent.

If the financial institution is the escrow agent, then the person who establishes the account is the financial institution's customer. For example, if the purchaser of real estate directly opens an escrow account and deposits funds to be paid to the seller upon satisfaction of specified conditions, the financial institution's customer will be the purchaser. Further, if a company in formation establishes an escrow account for investors to deposit their subscriptions pending receipt of a required minimum amount, the financial institution's customer will be the company in formation (or if not yet a legal entity, the person opening the account on its behalf).

However, the CIP rule also provides that, based on the financial institution's ML/FT risk assessment of a new account opened by a customer that is not an individual, the financial institution may need "to obtain information about" individuals with authority or control over such an account including the signatories in order to verify the customer's identity.

Money Laundering and Financing of Terrorism (ML/FT) Risk Factors

Trust and asset management accounts including agency relationships present ML/FT concerns similar to those of deposit taking, lending and other traditional financial institution's activities. Concerns are primarily due to the unique relationship structures involved when the financial institution handles trust and agency activities, such as:

i. Personal and court-supervised accounts.
ii. Trust accounts formed in the private banking department.
iii. Asset management and investment advisory accounts.
iv. Global and domestic custody accounts.
v. Securities lending.
vi. Employee benefit and retirement accounts.
vii. Corporate trust accounts.

Transfer agent accounts

As in any account relationship, money laundering risk may arise from trust and asset management activities. When misused, trust and asset management accounts can conceal the sources and uses of funds as well as the identity of beneficial and legal owners. Customers and account beneficiaries may try to remain anonymous in order to move illicit funds or avoid scrutiny.

For example, customers may seek a certain level of anonymity by creating private investment companies offshore trusts or other investment entities that hide the true ownership or beneficial interest of the trust.

Risk Mitigation

Management should develop policies, procedures and processes that enable the financial institution to identify unusual account relationships & circumstances,

questionable assets & sources of assets and other potential areas of ML/FT risk (e.g., offshore accounts, PICs, asset protection trusts (APT), agency accounts and unidentified beneficiaries). While the majority of traditional trust and asset management accounts will not need EDD, management should be alert to those situations that need additional review or research.

Customer Comparison Against Various Lists

The financial institution must maintain required CIP information and complete the required one-time check of trust account names against VIS search requests. The financial institution should also be able to identify customers who may be politically exposed persons (PEP), doing business with or located in a jurisdiction designated as "primary money laundering concern. The financial institution should also determine the identity of other parties that may have control over the account, such as grantors or co-trustees.

Circumstances Warranting Enhanced Due Diligence

i. Management should assess account risk on the basis of a variety of factors which may include:

a. Type of trust or agency account and its size.
b. Types and frequency of transactions.
c. Country of residence of the principals or beneficiaries or the country where established or source of funds.
d. Accounts and transactions that are not usual and customary for the customer or for the financial institution.
e. Stringent documentation, verification and transaction monitoring procedures should be established for accounts that the management considers as higher risk. Typically, employee benefit accounts and court-supervised accounts are among the lowest ML/FT risks.

ii. Circumstance in which EDD may be appropriate:

The financial institution is entering into a relationship with a new customer.

a. Account principals or beneficiaries reside in a foreign jurisdiction or the trust or its funding mechanisms are established offshore.
b. Assets or transactions are not typical for the type and character of the customer.
c. Account type, size, assets or transactions are atypical for the financial institution.
d. International funds transfers are conducted particularly through offshore funding sources.
e. Accounts are funded with easily transportable assets such as gemstones, precious metals, coins, artwork, rare stamps or negotiable instruments.
f. Accounts or relationships are maintained in way that the identities of the principals, beneficiaries, sources of funds are unknown or cannot be easily determined.

g. Accounts transactions are for the benefit of charitable organizations or other non-governmental organizations (NGOs) that may be used as a conduit for illegal activities.
h. Interest on lawyers' trust accounts (IOLTA) holding are processing significant currency/dollar amounts.
i. Account assets that include PICs.
j. PEPs are parties to the accounts or transactions.

84. EXAMINATION PROCEDURES OF TRUST AND ASSET MANAGEMENT SERVICES

Objective

Assess the adequacy of the financial institution's policies, procedures, processes and systems to manage the ML/FT risks associated with trust and asset management services and the management's ability to implement effective due diligence, monitoring and reporting systems.

For examination of stand-alone trusts, the Examiners should cover additional areas such as training, the CCO, independent review and follow-up items.

1. Review the policies, procedures and processes related to trust and asset management services. Evaluate the adequacy of the policies, procedures and processes given the financial institution's trust and asset management activities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. Review the bank's procedures for gathering additional identification information, when necessary, about the settlor, grantor, trustee or other persons with authority to direct a trustee and who thus have authority or control over the account in order to establish a true identity of the customer.
3. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors trust and asset management relationships, particularly those that pose a higher risk for money laundering.
4. Determine how the financial institution includes trust and asset management relationships in an institution-wide AML/CFT aggregation systems.
5. Determine whether the financial institution's system for monitoring trust and asset management relationships for suspicious transactions and for reporting of such transactions is adequate, given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

6. On the basis of the financial institution's ML/FT risk assessment of its trust and asset management relationships as well as prior examination and audit reports, select a sample of higher-risk trust and asset management services relationships. Include

relationships with grantors and co-trustees if they have authority or control as well as any higher-risk assets such as private investment companies (PIC) or asset protection trusts. **From the sample selected, perform the following examination procedures:**

i. Review account opening documentation, including the CIP, to ensure that adequate due diligence has been performed and that appropriate records are maintained.

ii. Review account statements and (as necessary) specific transaction details. Compare expected transactions with actual activity.

iii. Determine whether actual activity is consistent with the nature of the customer's business and the stated purpose of the account.

iv. Identify any unusual or suspicious activity.

7. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with trust and asset management relationships.

8. Update the section Notes, Risk Assessment Summary and Knowledge of Business of the financial institution.

85. OVERVIEW OF EXPANDED EXAMINATION AND PROCEDURES FOR PERSONS AND ENTITIES

86. OVERVIEW OF NON-RESIDENT ALIENS AND FOREIGN INDIVIDUALS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with transactions involving accounts held by non-resident aliens (NRA) and foreign individuals and the management's ability to implement effective due diligence, monitoring and reporting systems.

Foreign individuals maintaining relationships with Nigerian financial institutions can be divided into two categories of **resident aliens and non-resident aliens.**

For definitional purposes, a NRA is a non-Nigerian citizen who: (i) is not a lawful permanent resident of Nigeria during the calendar year and who does not meet the substantial presence test or (ii) has not been issued an alien registration permit. The FIRS determines the tax liabilities of a foreign person and officially defines the person as a "resident" or "non-resident."

Although NRAs are not permanent residents, they may have a legitimate need to establish an account relationship with a Nigerian financial institution. NRAs can use

bank products and services for asset preservation (e.g., mitigating losses due to exchange rates), business expansion and investments.

Risk Factors of an Account Holder

Financial institutions may find it more difficult to verify and authenticate an NRA accountholder's identification, source of funds and source of wealth which may result in ML/FT risks. The NRA's home country may also heighten the account risk, depending on the secrecy laws of that country. Because the NRA is expected to reside outside of Nigeria, funds transfers or the use of foreign automated teller machines (ATM) may be more frequent. The ML/FT risk may be further heightened if the NRA is a politically exposed person (PEP).

Risk Mitigation

Financial institutions should establish policies, procedures and processes that provide for sound due diligence and verification practices, adequate risk assessment of NRA accounts, ongoing monitoring and reporting of unusual or suspicious activities. **The following factors are to be considered when determining the risk level of an NRA account:**

i. Account-holder's home country.
ii. Types of products and services used.
iii. Forms of identification.
iv. Source of wealth and funds.
v. Unusual account activity.

The financial institution's CIP should detail the identification requirements for opening an account for a non-Nigerian person, including a NRA. The program should include the use of documentary and non-documentary methods to verify a customer. In addition, financial institutions must maintain due diligence procedures for private banking accounts for non-Nigerian persons, including those held for PEPs or senior foreign political figures.

87. EXAMINATION PROCEDURES OF NON-RESIDENT ALIENS AND FOREIGN INDIVIDUALS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with transactions involving accounts held by non-resident aliens (NRA) and foreign individuals, and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the financial institution's policies, procedures and processes related to NRA and foreign individual accounts. Evaluate the adequacy of the policies, procedures and processes given the financial institution's non-resident alien and foreign individual activities and the risks they represent. Assess whether the controls are

adequate to reasonably protect the financial institution from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk NRA and foreign individual accounts.

3. Determine whether the financial institution's system of monitoring NRA and foreign individual accounts for suspicious activities and for reporting of suspicious activities is adequate based on the complexity of the financial institution's NRA and foreign individual relationships, the types of products used by NRAs & foreign individuals, the home countries of the NRAs, and the source of funds and wealth for NRAs and foreign individuals.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its NRA and foreign individual accounts as well as prior examination and audit reports, select a sample of higher-risk NRA accounts. **Include the following risk factors:**

   i. Account for resident or citizen of a higher-risk jurisdiction.
   ii. Account activity which is substantially currency based.
   iii. NRA or foreign individual who uses a wide range of bank services, particularly correspondent services.
   iv. NRA or foreign individual for whom the financial institution has filed a STR.

4. From the sample selected, perform the following examination procedure

   i. Review the customer due diligence information, including CIP information, if applicable.
   ii. Review account statements and (as necessary) transaction details to determine whether actual account activity is consistent with expected activity. Assess whether transactions appear unusual or suspicious.
   iii. Review transaction activity and identify patterns that indicate Nigerian resident status or indicate other unusual and suspicious activity.

6. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with NRA accounts.

88. OVERVIEW OF POLITICALLY EXPOSED PERSONS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with senior local/foreign political figures, often referred to as "politically exposed persons" (PEP) and the management's ability to implement effective risk-based due diligence, monitoring and reporting systems.

Financial institution should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior local/foreign political figures, their families and associates. Because the risks presented by PEPs will vary by customer, product, service, country and industry, identifying, monitoring and designing controls for these accounts and transactions should be risk-based.

The term "politically exposed persons" generally include individuals who are or have been entrusted with prominent public functions in Nigeria and/or foreign countries and people/entities associated with them. **As specified in the CBN AML/CFT Regulation 2009, examples of PEPs include but not limited to:**

i. Heads of State or government;
ii. State Governors;
iii. Local Government Chairmen;
iv. Senior Politicians;
v. Senior government officials;
vi. Judicial or military officials;
vii. Senior executives of state owned corporations;
viii. Important political party officials;
ix. Family members or close associates of PEPs; and
x. Members of Royal Families.

In addition to performing CDD measures, financial institutions are required to put in place appropriate risk management systems and procedures that include reasonable steps to determine and ascertain whether a potential customer or existing customer or the beneficial-owner is a politically exposed person. Risk will vary depending on other factors such as products and services used and size or complexity of the account relationship. **Financial institutions also should consider various factors when determining if an individual is a PEP, including:**

i. Official responsibilities of the individual's office.
ii. Nature of the title (e.g., honorary or salaried).
iii. Level and nature of authority or influence over government activities or other officials.
iv. Access to significant government assets or funds.

Financial institutions are also required to obtain senior management approval before they establish business relationships with a PEP and to render monthly returns on all their transactions with PEPs to the CBN **(refer to pages B1402 – B1403 of the CBN AML/CFT Regulation 2009, for guidance).**

In determining the acceptability of higher-risk accounts, a financial institution should be able to obtain sufficient information to determine whether an individual is or is not a PEP. For example, when conducting due diligence on a higher-risk account, it would be usual for a financial institution to review a customer's income sources, financial information and professional background. These factors would likely require some review of past and present employment as well as general references that may identify a customer's status as a PEP. Moreover, a financial institution should always keep in mind that identification of a customer's status as a PEP should not automatically result in a higher-risk determination. **It is not only one factor that the institution should consider in assessing the risk of such a relationship.**

Ascertaining whether a customer has a close association with a senior local/foreign political figure could be difficult. Moreover, focusing on the relationships that are "widely and publicly known" may also provide a reasonable limitation on expectation to identify close associates of PEPs. However, financial institution that has actual knowledge of close associations of its customer should consider such a customer as PEP, even if such association is not otherwise widely or publicly known. Financial institutions are expected to follow reasonable steps to ascertain the status of an individual. The regulatory agencies recognize that these steps may not uncover all close associations of PEPs.

Risk Factors

In high-profile cases over the past few years, PEPs have used financial institutions as conduits for their illegal activities, including corruption, bribery and money laundering. However, not all PEPs present the same level of risk. This risk will vary depending on numerous factors, including the PEP's geographic location, industry, sector, position and level or nature of influence or authority. Risk may also vary depending on factors such as the purpose of the account, the actual or anticipated activity, products and services used, and size or complexity of the account relationship.

As a result of these factors, some PEPs may be of lower risk and some may be of higher risk for local/foreign corruption or money laundering. Financial institutions that conduct business with dishonest PEPs face substantial reputational risk, additional regulatory scrutiny and possible supervisory action. Financial institution also should be alert to a PEP's access to, control of or influence over government or corporate accounts; the level of involvement of intermediaries, vendors, suppliers, and agents in the industry or sector in which the PEP operates; and the improper use of corporate vehicles and other legal entities to obscure ownership.

Risk Mitigation

Section 1.10.5 of the CBN AML/CFT Regulation 2009, requires "financial institutions to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs". Financial institutions should exercise reasonable judgment in designing and implementing policies, procedures and processes regarding PEPs. Financial institution should obtain risk-based due diligence information on PEPs and establish policies, procedures and processes that provide for appropriate scrutiny and monitoring. It is critical and in order to have appropriate risk-based account opening procedures for big ticket transaction or higher-risk products and services. The opening of an account is the prime opportunity for the financial institution to gather information for all customers, including PEPs. **Commensurate with the identified level of risk, due diligence procedures should include, but are not necessarily limited to, the following:**

i. Identify the account-holder and beneficial owner, including the nominal and beneficial owners of companies, trusts, partnerships, private investment companies, or other legal entities that are accountholders.
ii. Seek information directly from the account holder and beneficial owner regarding possible PEP status.
iii. Identify the accountholder's and beneficial owner's country (ies) of residence and the level of risk for corruption and money laundering associated with these jurisdictions.
iv. Obtain information regarding employment including industry and sector, and the level of risk for corruption associated with the industries and sectors.
v. Check references (as appropriate) to determine whether the account holder and beneficial owner is or has been a PEP.
vi. Identify the account holder's and beneficial owner's source of wealth and funds.
vii. Obtain information on immediate family members or close associates that have the account.
viii. Determine the purpose of the account, the expected volume and nature of account activity.
ix. Make reasonable efforts to review public sources of information. These sources will vary depending upon each situation. However, financial institutions should check the account-holder and any beneficial owners of legal entities against reasonably accessible public sources of information (e.g., government databases, major news publications, commercial databases and other databases available on the internet, as appropriate).

PEP accounts are not limited to large or internationally focused financial institutions. **A PEP can open an account at any financial institution, regardless of its size or location.** Financial institutions should have risk-based procedures for identifying PEP accounts and assessing the degree of risks involved and the latter will vary. **Senior management should be involved in the decision to accept a PEP account. If management determines after-the-fact that an account is a PEP account, it should evaluate the risks and take appropriate steps. The financial institution should exercise additional, reasonable due diligence with regard to such accounts.**

For example, the financial institution may increase reference inquiries, obtain additional background information on the PEP from branches or correspondents operating in the client's home country, and make reasonable efforts to consult publicly available information sources. **On-going risk-based monitoring of PEP accounts is critical to ensuring that the accounts are being used as anticipated.**

89. EXAMINATION PROCEDURES OF POLITICALLY EXPOSED PERSONS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with senior local/foreign political figures, often referred to as "politically exposed persons" (PEP) and the management's ability to implement effective risk-based due diligence, monitoring and reporting systems.

1. Review the risk-based policies, procedures and processes related to PEPs. Evaluate the adequacy of the policies, procedures and processes given the financial institution's PEP accounts and the risks they present. Assess whether the risk-based controls are adequate to reasonably protect the financial institution from being used as a conduit for money laundering, corruption and terrorist financing.
2. Review the procedures for opening PEP accounts. Identify senior management's role in the approval and ongoing risk-based monitoring of PEP accounts.
3. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors PEP relationships, particularly those that pose a higher risk for corruption, money laundering and terrorist financing.
4. Determine whether the financial institution's system for monitoring PEPs for suspicious activities and for reporting of suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

5. On the basis of the financial institution's risk assessment of its PEP relationships as well as prior examination and audit reports, select a sample of PEP accounts. **From the sample selected, perform the following examination procedures:**

    i. Determine compliance with regulatory requirements and with the financial institution's established policies, procedures and processes related to PEPs.
    ii. Review transaction activity for accounts selected. If necessary, request and review specific transactions.
    iii. If the analysis of activity and customer due diligence information raises concerns, hold discussions with the institution management.

6. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with PEPs.

90. OVERVIEW OF EMBASSY AND FOREIGN CONSULATE ACCOUNTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with transactions involving embassy and foreign consulate accounts and the management's ability to implement effective due diligence, monitoring and reporting systems.

Embassies contain the offices of the foreign ambassador, the diplomatic representative and their staff. The embassy, led by the ambassador, is a foreign government's official representation in the Nigeria (or other country).

Foreign consulate offices act as branches of the embassy and perform various administrative and governmental functions (e.g., issuing visas and handling immigration matters). Foreign consulate offices are typically located in major metropolitan areas. In addition, foreign ambassadors' diplomatic representatives, their families and associates may be considered politically exposed persons (PEP) in certain circumstances.

Embassies and foreign consulates in Nigeria require access to the banking system to meet many of their day-to-day financial responsibilities. Such services can range from account relationships for operational expenses (e.g., payroll, rent and utilities) to inter and intra-governmental transactions (e.g., commercial and military purchases). In addition to official embassy accounts, some financial institutions provide ancillary services or accounts to embassy staff, families and current or prior foreign government officials. Each of these relationships poses different levels of risk to the financial institution.

Embassy accounts, including those accounts for a specific embassy office such as a cultural or education ministry, a defence attaché or ministry, or any other account should have a specific operating purpose, stating the official function of the foreign government office. Consistent with established practices for business relationships, these embassy accounts should have written authorization by the foreign government.

Risk Factors

To provide embassy and foreign consulate services, **a Nigerian financial institution may need to maintain a foreign correspondent relationship with the embassy's or foreign consulate's financial institution.** Financial institutions conducting business with foreign embassies or consulates should assess and understand the potential risks of these accounts and should develop appropriate

policies, procedures and processes. **Embassy or foreign consulate accounts may pose a higher risk in the following circumstances:**

i. Accounts are from countries that have been designated as higher risk.
ii. Substantial currency transactions take place in the accounts.
iii. Account activity is not consistent with the purpose of the account (e.g., pouch activity or payable upon proper identification transactions).
iv. Accounts directly fund personal expenses of foreign nationals including but not limited to expenses for college students.
v. Official embassy business is conducted through personal accounts.

Risk Mitigation

Financial institutions should obtain comprehensive due diligence information on embassy and foreign consulate account relationships. For private banking accounts for non-Nigerian persons specifically, financial institutions must obtain due diligence information. The financial institution's due diligence related to embassy and foreign consulate account relationships should be commensurate with the risk levels presented. In addition, financial institutions are expected to establish policies, procedures and processes that provide for greater scrutiny and monitoring of all embassy and foreign consulate account relationships. Management should fully understand the purpose of the account and the expected volume and nature of account activity. On-going monitoring of embassy and foreign consulate account relationships is critical to ensuring that the account relationships are being used as anticipated.

91. EXAMINATION PROCEDURES OF EMBASSY AND FOREIGN CONSULATE ACCOUNTS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with transactions involving embassy and foreign consulate accounts and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the policies, procedures and processes related to embassy and foreign consulate accounts. Evaluate the adequacy of the policies, procedures and processes given the financial institution's embassy and foreign consulate accounts and the risks they present (e.g., number of accounts, volume of activity and geographic locations). Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. Identify senior management's role in the approval and ongoing monitoring of embassy and foreign consulate accounts. Determine whether the board is aware of embassy banking activities and whether it receives periodic reports on these activities.

3. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors embassy and foreign consulate accounts, particularly those that pose a higher risk for money laundering.
4. Determine whether the financial institution's system for monitoring embassy and foreign consulate accounts for suspicious activities and for reporting of suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

5. On the basis of the financial institution's risk assessment of its embassy and foreign consulate accounts as well as prior examination and audit reports, select a sample of embassy and foreign consulate accounts. **From the sample selected, perform the following examination procedures:**

    i. Determine compliance with regulatory requirements and with the financial institution's established policies, procedures and processes.
    ii. Review the documentation authorizing the ambassador or the foreign consulate to conduct banking in Nigeria.
    iii. Review transaction activity for accounts selected. If necessary, request and review specific transactions.

6. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with embassy and foreign consulate accounts.

92. OVERVIEW OF DESIGNATED NON-FINANCIAL INSTITUTIONS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with accounts of designated non- financial institutions (DNFI) and the management's ability to implement effective monitoring and reporting systems.

Common examples of NBFIs include but not limited to:

i. Casinos, hotels, supermarkets and card clubs.
ii. Dealers in cars, luxury goods, chartered accountants, audit firms, clearing and settlement companies, legal practitioners.
iii. Dealers in precious metals, stones or jewellery.

Some NBFIs are currently required to develop an AML/CFT program, comply with the reporting and recordkeeping requirements of the MLPA, and report suspicious activity to Federal Ministry of Commerce as the regulatory authority. DNFIs typically need access to banking services in order to operate. While financial institutions are expected to manage risk associated with all accounts including DNFI accounts, the institution will

not be held responsible for their customers' non-compliance with the MLPA and other relevant laws and regulations.

Risk Factors

DNFI industries are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component to their primary business (e.g., grocery store that offers cheque- cashing). The range of products and services offered and the customer bases served by DNFIs are equally diverse. As a result of this diversity, some DNFIs may be of lower risk and some may be of higher risk for money laundering. **Financial institutions that maintain account relationships with DNFIs may be exposed to a higher risk for potential money laundering activities because many DNFIs:**

i. Lack ongoing customer relationships and require minimal or no identification by customers.
ii. Maintain limited or inconsistent record-keeping on customers and transactions.
iii. Engage in frequent currency transactions.
iv. Are subject to varying levels of regulatory requirements and oversight.
v. Can quickly change their product mix or location and quickly enter or exit an operation.
vi. Sometimes operate without proper registration or licensing.

Risk Mitigation

Financial institutions that maintain account relationships with DNFIs should develop policies, procedures and processes to:

i. Identify DNFI relationships.
ii. Assess the potential risks posed by the DNFI relationships.
iii. Conduct adequate and ongoing due diligence on the DNFI relationships when necessary.
iv. iv Ensure DNFI relationships are appropriately considered within the financial institution's suspicious activity monitoring and reporting systems.

Risk assessment factors of financial institutions assess the risks posed by their DNFI customers and direct their resources most appropriately to those accounts that pose a more significant money laundering risk.
Risk factors may be used to help identify the relative risks within the DNFI portfolio. Nevertheless, management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer and to prioritize oversight resources. **Relevant risk factors include:**

i. Types of products and services offered by the DNFI.
ii. Locations and markets served by the DNFI.
iii. Anticipated account activity.
iv. Purpose of the account.

A financial institution's due diligence should be commensurate with the level of risk of the DNFI customer identified through its risk assessment. If a financial institution's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

Providing Banking Services to Money Services Businesses

Money Services Businesses (MSBs) are subject to the full range of MLPA regulatory requirements, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules and various other identification and record-keeping rules.

Regulatory expectations apply to financial institution with MSB customers:

i. The MLPA does not require financial institutions to serve as the de facto regulator of any type of DNFI industry or individual DNFI customer, including MSBs.
ii. While financial institutions are expected to manage risk associated with all accounts including MSB accounts, they will not be held responsible for the MSB not having AML/CFT Program.
iii. Not all MSBs pose the same level of risk and not all MSBs will require the same level of due diligence. Accordingly, if a financial institution's assessment of the risks of a particular MSB relationship indicates a lower risk of money laundering or other illicit activity, a financial institution is not routinely expected to perform further due diligence (such as reviewing information about an MSB's AML/CFT Program) beyond the minimum due diligence expectations. Unless indicated by the risk assessment of the MSB, financial institutions are not expected to routinely review an MSB's AML/CFT Program.

MSB Risk Assessment

An effective risk assessment should be a composite of multiple factors and depending upon the circumstances, certain factors may be given more weight than others. **The following factors may be used to help identify the level of risk presented by each MSB customer:**

i. Purpose of the account.
ii. Anticipated account activity (type and volume).
iii. Types of products and services offered by the MSB.
iv. Locations and markets served by the MSB.

Financial institution management may tailor these factors based on their customer base or the geographic locations in which the financial institution operates. Management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer. A bank's due diligence should be commensurate with the level of risk assigned to the MSB customer, after consideration of these factors. If

a bank's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, the bank will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

MSB Risk Mitigation

A financial institution's policies, procedures and processes should provide for sound due diligence and verification practices, adequate risk assessment of MSB accounts and ongoing monitoring and reporting of unusual or suspicious transactions. A financial institution that establishes and maintains accounts for MSBs should apply appropriate, specific risk-based and where necessary, EDD policies, procedures, and controls.

Factors that may reduce or mitigate the risk in some MSB accounts:

i. MSB is registered and licensed with the CBN.
ii. MSB confirms it is subject to examination for AML compliance.
iii. MSB affirms the existence of a written AML/CFT Program and provides its CCO's name and contact information.
iv. MSB has an established banking relationship and/or account activity consistent with expectations.
v. MSB is an established business with an operating history.
vi. MSB is a principal with one or few agents, or is acting as an agent for one principal.
vii. MSB provides services only to local residents.
viii. Most of the MSB's customers conduct routine transactions in not too much amounts.
ix. The expected (lower-risk) transaction activity for the MSB's business operations is consistent with information obtained by the financial institution at account opening. **Examples include the following:**
    a. Cheque-cashing activity is limited to payroll or government cheques.
    b. (b) Cheque-cashing service is not offered for third-party or out-of-state cheques.
x. Money-transmitting activities are limited to domestic entities (e.g., domestic bill payments).

MSB Due Diligence Expectations

Given the importance of licensing and registration requirements, a financial institution should file a STR if it becomes aware that a customer is operating in violation of the registration or licensing requirements. **The decision to maintain or close an account should be made by financial institution senior management under standards and guidelines approved by its board of directors.**

The extent to which the financial institution should perform further due diligence beyond the minimum due diligence obligations set forth below will be dictated by the level of risk posed by the individual MSB customer. Because not all MSBs present the same level of risk, not all MSBs will require further due diligence. For example, a local

grocer that also cashes payroll cheques for customers purchasing groceries may not present the same level of risk as a money transmitter specializing in cross-border funds transfers. Therefore, the customer due diligence requirements will differ based on the risk posed by each MSB customer. **Based on existing AML/CFT Regulation requirements applicable to financial institutions, the minimum due diligence expectations associated with opening and maintaining accounts for any MSB are:**

i. Apply the financial institution's CIP.
ii. Confirm registration renewal.
iii. Confirm compliance with licensing requirements, if applicable.
iv. Confirm agent status, if applicable.
v. Conduct a basic ML/FT risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

If the institution determines that the MSB customer presents a higher level of money laundering or terrorist financing risk, EDD measures should be conducted in addition to the minimum due diligence procedures. **Depending on the level of perceived risk, the size and sophistication of the particular MSB, banking organizations may pursue some or all of the following actions as part of an appropriate EDD review:**

i. Review the MSB's AML/CFT Program.
ii. Review results of the MSB's independent testing of its AMLCFT Program.
iii. Review written procedures for the operation of the MSB.
iv. Conduct on-site visits.
v. Review list of agents, including locations within or outside Nigeria which will be receiving services directly or indirectly through the MSB account.
vi. Review written agent management and termination practices for the MSB.
vii. Review written employee screening practices for the MSB.

93. EXAMINATION PROCEDURES OF DESIGNATED NON-FINANCIAL INSTITUTIONS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with accounts of designated non- financial institutions (DNFI) and the management's ability to implement effective monitoring and reporting systems.

1. Determine the extent of the financial institution's relationships with DNFIs and for financial institutions with significant relationships with DNFIs, review the financial institution's risk assessment of this activity.
2. Review the policies, procedures and processes related to DNFI accounts. Evaluate the adequacy of the policies, procedures and processes given the financial institution's DNFI activities and the risks they represent. Assess whether the controls

are adequate to reasonably protect the financial institution from money laundering and terrorist financing.

3. From review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors DNFI accounts.
4. Determine whether the financial institution's system for monitoring DNFI accounts for suspicious activities and for reporting of suspicious activities is adequate given the nature of the bank's customer relationships.

Money Services Businesses

5. Determine whether the financial institution has policies, procedures and processes in place for accounts opened or maintained for money services businesses (MSB) to:

   i. Confirm registration (if required) and that registration must be renewed as required.
   ii. Confirm status of the licence, if applicable.
   iii. Confirm agent status, if applicable.
   iv. Conduct a risk assessment to determine the level of risk associated with each account and whether further due diligence is required.

6. Determine whether the financial institution's policies, procedures and processes to assess risks posed by MSB customers effectively identify higher-risk accounts and the amount of further due diligence necessary.

Transaction Testing

7. On the basis of the financial institution's risk assessment of the DNFI as well as prior examination and audit reports, select a sample of higher-risk DNFI accounts. **From the sample selected, perform the following examination procedures:**

   i. Review account opening documentation and ongoing due diligence information.
   ii. Review account statements (as necessary) and specific transaction details. Compare expected transactions with actual activity.
   iii. Determine whether actual activity is consistent with the nature of the customer's business and identify any unusual or suspicious activity.

8. On a basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with DNFI relationships.

Overview of Professional Service Providers

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with professional service provider relationships and the management's ability to implement effective due diligence, monitoring and reporting systems.

A professional service provider acts as an intermediary between its client and the financial institution. Professional service providers include lawyers, accountants, investment brokers and other third parties that act as financial liaisons for their clients. These providers may conduct financial dealings for their clients. For example, an attorney may perform services for a client or arrange for services to be performed on the client's behalf. Such services include settlement of real estate transactions, asset transfers, management of client monies, investment services and trust arrangements.

Risk Factors

In contrast to escrow accounts that are set up to serve individual clients, professional service provider accounts allow for ongoing business transactions with multiple clients. Generally, a financial institution has no direct relationship with or knowledge of the beneficial owners of these accounts who may be a constantly changing group of individuals and legal entities.

As with any account that presents third-party risk, the financial institution could be more vulnerable to potential money laundering abuse. **Some potential examples of abuse could include:**

i. Laundering illicit currency.
ii. Structuring currency deposits and withdrawals.
iii. Opening any third-party account for the primary purpose of masking the underlying client's identity.

As such, the financial institution should establish an effective due diligence program for the professional service provider.

Risk Mitigation

When establishing and maintaining relationships with professional service providers, financial institutions should adequately assess account risk and monitor the relationship for suspicious or unusual activity. At account opening, the financial institution should have an understanding of the intended use of the account, including anticipated transaction volume, products and services used, and geographic locations involved in the relationship.

95. EXAMINATION PROCEDURES OF PROFESSIONAL SERVICE PROVIDERS

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with professional service provider relationships and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the policies, procedures and processes related to professional service provider relationships. Evaluate the adequacy of the policies, procedures and processes given the financial institution's relationships with professional service providers and the risks these relationships represent. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors professional service provider relationships. MIS reports should include information about the entire relationship. For example, an interest on lawyers' trust account (IOLTA) may be in the name of the law firm instead of an individual. However, the financial institution's relationship report should include the law firm's account and the names and accounts of lawyers associated with the IOLTA.
3. Determine whether the financial institution's system for monitoring professional service provider relationship's suspicious activities and for reporting of suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its relationships with professional service providers as well as prior examination and audit reports, select a sample of higher-risk relationships. **From the sample selected, perform the following examination procedures:**

i. Review account opening documentation and a sample of transaction activity.

ii. Determine whether determine whether actual account activity is consistent with anticipated (as documented) account activity. Look for trends in the nature, size or scope of the transactions, paying particular attention to currency transactions.

iii.Determine whether ongoing monitoring is sufficient to identify potentially suspicious activity.

5. On the basis of examination procedures conducted including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with professional service provider relationships.

96. OVERVIEW OF NON-GOVERNMENTAL ORGANIZATIONS AND CHARITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with accounts of non-governmental organizations (NGO) and charities and the management's ability to implement effective due diligence, monitoring and reporting systems.

NGOs are private non-profit organizations that pursue activities intended to serve the public good. NGOs may provide basic social services work to relieve suffering, promote the interests of the poor, bring citizen concerns to governments, encourage political participation, protect the environment, or undertake community development to serve the needs of citizens, organizations or groups in one or more of the communities that the NGO operates. An NGO can be any non-profit organization that is independent from government.

NGOs can range from large regional, national or international charities to community-based self-help groups. NGOs may also include research institutes, churches, professional associations and lobby groups. NGOs typically depend (in whole or in part) on charitable donations and voluntary service for support.

Risk Factors

Because NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. Guidelines will be issued to assist charities in adopting practices to reduce the risk of terrorist financing or abuse.

Risk Mitigation

To assess the risk of NGO customers, a financial institution should conduct adequate due diligence on the organization. **In addition to required CIP information, due diligence for NGOs should focus on other aspects of the organization, such as the following:**

i. Purpose and objectives of their stated activities.
ii. Geographic locations served including headquarters and operational areas.
iii. Organizational structure.
iv. Donor and volunteer base.
v. Funding and disbursement criteria including basic beneficiary information.
vi. Record keeping requirements.
vii. Its affiliation with other NGOs, governments or groups.

viii.Internal controls and audits.

For accounts that financial institution management considers to be higher risk, stringent documentation, verification and transaction monitoring procedures should be established. NGO accounts that are at higher risk for ML/FT concerns include those operating or providing services internationally, conducting unusual or suspicious activities or lacking proper documentation. **EDD for these accounts should include:**

i. Evaluating the principals.
ii. Obtaining and reviewing the financial statements and audits.
iii. Verifying the source and use of funds.
iv. Evaluating large contributors or grantors to the NGO.

97. EXAMINATION PROCEDURES OF NONGOVERNMENTAL ORGANIZATIONS AND CHARITIES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with accounts of non-governmental organizations (NGO) and charities and the management's ability to implement effective due diligence, monitoring, and reporting systems.

1. Review the policies, procedures and processes related to NGOs. Evaluate the adequacy of the policies, procedures and processes given the financial institution's NGO accounts and the risks they represent. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk NGO accounts.
3. Determine whether the financial institution's system for monitoring NGO accounts for suspicious activities and for reporting of suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of the NGO and charity account, as well as prior examination and audit reports, select a sample of higher-risk NGO accounts. **From the sample selected, perform the following examination procedures:**

i.Review account opening documentation and ongoing due diligence information.

ii.Review account statements (as necessary) and specific transaction details.

iii.Compare expected transactions with actual activity.

iv. Determine whether actual activity is consistent with the nature of the customer's business.

v. Identify any unusual or suspicious activity.

5. On the basis of examination procedures conducted including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with NGO accounts.

98. OVERVIEW OF BUSINESS BUSINESS ENTITIES (DOMESTIC AND FOREIGN)

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with transactions involving domestic and foreign business entities and the management's ability to implement effective due diligence, monitoring and reporting systems.

The term "business entities" refers to limited liability companies, corporations, trusts, and other entities that may be used for many purposes such as tax and estate planning. Business entities are relatively easy to establish. Individuals, partnerships and existing corporations establish business entities for legitimate reasons but the entities may be abused for money laundering and terrorist financing.

Domestic Business Entities

Nigeria has statutes governing the incorporation and operation of business entities, including limited liability companies, corporations, general partnerships, limited partnerships and trusts.

Shell companies registered in Nigeria are a type of domestic business entity that may pose heightened risks. Shell companies can be used for money laundering and other crimes because they are easy and inexpensive to form and operate. In addition, ownership and transactional information can be concealed from regulatory agencies and law enforcement in large part because it requires minimal disclosures of such information during the formation process.

The term "domestic" refers to entities formed or organized in Nigeria. These entities may have no other connection to Nigeria and ownership and management of the entities may reside abroad.

The term "shell company" generally refers to an entity without a physical presence in any country.

Shares of shell companies can be publicly traded or privately held. Although publicly traded shell companies can be used for illicit purposes, the vulnerability of the

shell company is compounded when it is privately held and beneficial ownership can more easily be obscured or hidden. Lack of transparency of beneficial ownership can be a desirable characteristic for some legitimate uses of shell companies, but it is also a serious vulnerability that can make some shell companies ideal vehicles for money laundering and other illicit financial activity. In some, only minimal information is required to register articles of incorporation or to establish and maintain "good standing" for business entities — increasing the potential for their abuse by criminal and terrorist organizations.

Foreign Business Entities

Frequently used foreign entities include trusts, investment funds and insurance companies. **Two foreign entities that can pose particular money laundering risk are international business corporations (IBC) and Private Investment Companies (PIC) opened in offshore financial centres (OFCs).** Many OFCs have limited organizational disclosure and record-keeping requirements for establishing foreign business entities, creating an opportune environment for money laundering.

International Business Corporations

IBCs are entities formed outside of a person's country of residence which can be used to maintain confidentially or hide assets. IBC ownership can, based on jurisdiction, be conveyed through registered or bearer shares. **There are a variety of advantages to using an IBC which include, but are not limited to, the following:**

i. Asset protection.
ii. Estate planning.
iii. Privacy and confidentiality.
iv. Reduction of tax liability.

Through an IBC, an individual is able to conduct the following:

i. Open and hold bank accounts.
ii. Hold and transfer funds.
iii. Engage in international business and other related transactions.
iv. Hold and manage offshore investments (e.g., stocks, bonds, mutual funds and certificates of deposit) many of which may not be available to "individuals" depending on their location of residence.
v. Hold corporate debit and credit cards, thereby allowing convenient access to funds.

Private Investment Companies

PICs are separate legal entities. They are essentially subsets of IBCs. Determining whether a foreign corporation is a PIC is based on identifying the purpose and use of the legal vehicle. **PICs are typically used to hold individual funds and**

investments, and ownership can be vested through bearer shares or registered shares. Like IBCs, PICs can offer confidentiality of ownership, hold assets centrally and may provide intermediaries between private banking customers and the potential beneficiaries of the PICs. Shares of a PIC may be held by a trust, which further obscures beneficial ownership of the underlying assets. **IBCs, including PICs, are incorporated frequently in countries that impose low or no taxes on company assets and operations or are bank secrecy havens.**

Risk Factors

Money laundering and terrorist financing risks arise because business entities can hide the true owner of assets or property derived from or associated with criminal activity. The privacy and confidentiality surrounding some business entities may be exploited by criminals, money launderers and terrorists. Verifying the grantors and beneficial owner(s) of some business entities may be extremely difficult, as the characteristics of these entities shield the legal identity of the owner. Few public records will disclose true ownership. Overall, the lack of ownership transparency; minimal or no record-keeping requirements, financial disclosures and supervision; and the range of permissible activities all increase money laundering risk.

While business entities can be established in most international jurisdictions, many are incorporated in OFCs that provide ownership privacy and impose few or no tax obligations. To maintain anonymity, many business entities are formed with nominee directors, office-holders and shareholders. In certain jurisdictions, business entities can also be established using bearer shares; ownership records are not maintained, rather ownership is based on physical possession of the stock certificates. Revocable trusts are another method used to insulate the grantor and beneficial owner and can be designed to own and manage the business entity, presenting significant barriers to law enforcement.

Indicators of potentially suspicious activity commonly associated with shell company activity

i. Insufficient or no information available to positively identify originators or beneficiaries of funds transfers (using internet, commercial database searches or direct inquiries to a respondent bank).
ii. Payments have no stated purpose, do not reference goods or services. They identify only a contract or invoice number.
iii. Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
iv. Transacting businesses share the same address, provide only a registered agent's address or other inconsistent addresses.
v. Many or all of the funds transfers are sent in large, round amounts.
vi. Unusually large number and variety of beneficiaries receiving funds transfers from one company.

vii. Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk OFCs.
viii. A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
ix. Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
ix.Purpose of the shell company is unknown or unclear.

Risk Mitigation

Management should develop policies, procedures and processes that enable the financial institution to identify account relationships in particular deposit accounts, with business entities and monitor the risks associated with these accounts in all the financial institution's departments. Business entity customers may open accounts within the private banking department, within the trust department, or at local branches. Management should establish appropriate due diligence at account opening and during the life of the relationship to manage risk in these accounts. The financial institution should gather sufficient information on the business entities and their beneficial owners to understand and assess the risks of the account relationship. Important information for determining the valid use of these entities includes the type of business, the purpose of the account, the source of funds and the source of wealth of the owner or beneficial owner.

The financial institution's CIP should detail the identification requirements for opening an account for a business entity. When opening an account for a customer that is not an individual, financial institution should obtain information about the individuals who have authority and control over such accounts in order to verify the customer's identity (the customer being the business entity). Required account opening information may include articles of incorporation, a corporate resolution by the directors authorizing the opening of the account, or the appointment of a person to act as a signatory for the entity on the account. Particular attention should be paid to articles of association that allow for nominee shareholders, board members and bearer shares.

If the financial institution, through its trust or private banking departments, is facilitating the establishment of a business entity for a new or existing customer, the money laundering risk to the financial statement is typically mitigated. Because the financial institution is aware of the parties (e.g., grantors, beneficiaries and shareholders) involved in the business entity, initial due diligence and verification is easier to obtain. Furthermore, in such cases, the financial institution frequently has ongoing relationships with the customers initiating the establishment of a business entity.

Risk assessments may include a review of the domestic or international jurisdiction where the business entity was established, the type of account (or accounts) and expected versus actual transaction activities, the types of products that will be used, and whether the business entity was created in-house or externally. If ownership is held in bearer share form, financial institution should assess the risks these relationships

pose and determine the appropriate controls. In most cases, financial institutions should choose to maintain (or have an independent third party maintain) bearer shares for customers. In rare cases involving lower-risk, well-known, established customers, financial institutions may find that periodically re-certifying beneficial ownership is effective. The financial institution's risk assessment of a business entity customer becomes more important in complex corporate formations. For example, a foreign IBC may establish a series of layered business entities with each entity naming its parent as its beneficiary.

On-going account monitoring is critical to ensure that the accounts are reviewed for unusual and suspicious activity. The financial institution should be aware of higher-risk transactions in these accounts, such as activity that has no business or apparent lawful purpose, funds transfer activity to and from higher-risk jurisdictions, currency intensive transactions and frequent changes in the ownership or control of the non-public business entity.

99. EXAMINATION PROCEDURES OF BUSINESS ENTITIES (DOMESTIC AND FOREIGN)

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with transactions involving domestic and foreign business entities and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the financial institution's policies, procedures and processes related to business entities. Evaluate the adequacy of the policies, procedures and processes given the financial institution's transactions with business entities and the risks they present. Assess whether the controls are adequate to reasonably protect the financial institution from money laundering and terrorist financing.
2. Review the policies and processes for opening and monitoring accounts with business entities. Determine whether the policies adequately assess the risk between different account types.
3. Determine how the financial institution identifies (as necessary) and completes additional due diligence on business entities. Assess the level of due diligence the financial institution performs when conducting its risk assessment.
4. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors higher-risk business entity accounts.
5. Determine whether the financial institution's system for monitoring business entities for suspicious activities and for reporting of suspicious activities is adequate given the activities associated with business entities.

Transaction Testing

6. On the basis of the financial institution's risk assessment of its accounts with business entities as well as prior examination and audit reports, select a sample of these accounts. **Include the following risk factors:**

   i. An entity organized in a higher-risk jurisdiction.
   ii. Account activity that is substantially currency based.
   iii. An entity whose account activity consists primarily of circular-patterned funds transfers.
   iv. A business entity whose ownership is in bearer shares, especially bearer shares that are not under bank or trusted third-party control.
   v. An entity that uses a wide range of bank services, particularly trust and correspondent services.
   vi. An entity owned or controlled by other non-public business entities.
   vii. Business entities for which the financial institution has filed STRs.

7. From the sample selected, obtain a relationship report for each selected account. It is critical that the full relationship, rather than only an individual account, be reviewed.

8. Review the due diligence information on the business entity. Assess the adequacy of that information.

8. Review account statements (as necessary) and specific transaction details. Compare expected transactions with actual activity. Determine whether actual activity is consistent with the nature and stated purpose of the account and whether transactions appear unusual or suspicious. Areas that may pose a higher risk, such as funds transfers, private banking, trust, and monetary instruments should be a primary focus of the transaction review.

9. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with business entity relationships.

100. OVERVIEW OF CASH-INTENSIVE BUSINESSES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with cash-intensive businesses and entities, and the management's ability to implement effective due diligence, monitoring and reporting systems.

Cash-intensive businesses and entities cover various industry sectors. Most of these outfits conduct legitimate business. However, some aspects of these businesses may be susceptible to money laundering or terrorist financing. **Common examples include but are not limited to, the following:**

   i. Convenience stores.
   ii. Restaurants.
   iii. Retail stores.

iv. iv Liquor stores.
v. Cigarette distributors.
vi. Privately owned automated teller machines (ATM).
vii. Vending machine operators.
viii. Parking garages.

Risk Factors

Some businesses and entities may be misused by money launderers to legitimize their illicit proceeds. For example, a criminal may own a cash-intensive business such as a restaurant and use it to launder currency from illicit criminal activities. The restaurant's currency deposits with its bank do not, on the surface, appear unusual because the business is legitimately a cash-generating entity. However, the volume of currency in a restaurant used to launder money will most likely be higher in comparison with similar restaurants in the area. The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause these businesses to be considered higher risk.

Risk Mitigation

When establishing and maintaining relationships with cash-intensive businesses, financial institution should establish policies, procedures and processes to identify higher-risk relationships; assess ML/FT risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity. At the time of account opening, the financial institution should have an understanding of the customer's business operations; the intended use of the account including anticipated transaction volume, products and services used; and the geographic locations involved in the relationship.

When conducting a risk assessment of cash-intensive businesses, financial institution should direct their resources to those accounts that pose the greatest risk of money laundering or terrorist financing. **The following factors may be used to identify the risks:**

i. Purpose of the account.
ii. Volume, frequency and nature of currency transactions.
iii. Customer history (e.g., length of relationship, CTR and STR filings).
iv. Primary business activity, products and services offered.
v. Business or business structure.
vi. Geographic locations and jurisdictions of operations.
vii. Availability of information and cooperation of the business in providing information. For those customers deemed to be particularly higher risk, management may consider implementing sound practices such as periodic on-site visits, interviews with the business's management or closer reviews of transactional activity.

101. EXAMINATION PROCEDURES OF CASH-INTENSIVE BUSINESSES

Objective

Assess the adequacy of the financial institution's systems to manage the risks associated with cash-intensive businesses and entities, and the management's ability to implement effective due diligence, monitoring and reporting systems.

1. Review the policies, procedures and processes related to cash-intensive businesses. Evaluate the adequacy of policies, procedures and processes given the financial institution's cash-intensive business activities in relation to the financial institution's cash-intensive business customers and the risks that they represent. Assess whether the controls are adequate to reasonably protect the bank from money laundering and terrorist financing.

2. From a review of MIS and internal risk rating factors, determine whether the financial institution effectively identifies and monitors cash-intensive businesses and entities.

3. Determine whether the financial institution's system for monitoring cash-intensive businesses for suspicious activities and for reporting of suspicious activities is adequate given the financial institution's size, complexity, location and types of customer relationships.

Transaction Testing

4. On the basis of the financial institution's risk assessment of its cash-intensive business and entity relationships as well as prior examination and audit reports, select a sample of cash-intensive businesses. **From the sample selected, perform the following examination procedures:**

   i. Review account opening documentation including CIP information, if applicable, and a sample of transaction activity.

   ii. Determine whether actual account activity is consistent with anticipated account activity.

   iii. Look for trends in the nature, size or scope of the transactions, paying particular attention to currency transactions.

   iv. Determine whether ongoing monitoring is sufficient to identify potentially suspicious activity.

5. On the basis of examination procedures completed including transaction testing, form a conclusion about the adequacy of policies, procedures and processes associated with cash-intensive businesses and entities.

APPENDIX A

AML/CFT Laws and Regulations

Statutes on Money Laundering

i. Money Laundering (Prohibition) Act, 2004 (MLP Act)
ii. The Economic and Financial Crimes Commission Act, 2004 (EFCC Act)
iii. The National Drug Law Enforcement Agency Act (NDLEA) 1989 as
iv. amended; and
v. The Independent Corrupt Practices (and Other Related Offences) Commission, (ICPC) Act, 2000.

Terrorist Financing

Section 15 of the EFCC (Establishment) Act, 2004 is the only attempt by Nigeria to criminalize the financing of terrorism. It states that "any person who willfully provides or collects by any means, directly or indirectly any money from any other person with intent or knowledge that the money shall be used for any act of terrorism is guilty of an offence and liable on conviction to life imprisonment".
Terrorism is defined in Section 46 of the EFCC Act. However, there is no clear definition of what constitutes terrorist organization, terrorist funds and assets. It covers the attempt to commit terrorist acts, aiding and abetting the commission of terrorism by any person who makes funds, financial assets or economic resources or other related services available for use by any person to commit or attempt to commit, facilitate or participate in the commission of a terrorist act. The applicable sanction for attempt to commit terrorism or the commission of a terrorist offence is imprisonment for life.

ANTI-TERRORIST ACT, 2010

Regulations

•CBN AML/CFT Regulation, 2009

APPENDIX B

AML/CFT Directives by the Central Bank of Nigeria

Supervisory and Regulatory Circulars are issued by the CBN to address significant policy and procedural matters related to its AML/CFT supervisory responsibilities. The circulars are issued by the various departments in CBN as important means of disseminating AML/CFT information to financial institutions. The applicable CBN AML/CFT Circulars are available at www.cenbank.gov.ng web site.

APPENDIX C

AML/CFT references web sites

Central Bank of Nigeria: www.cenbank.gov.ng

Nigerian Financial Intelligence Unit:

Nigerian Deposit Insurance Corporation:

Economic and Financial Crimes Commission:

National Drug Law Enforcement Agency:

Independent Corrupt Practices Commission:

Board of Governors of the Federal Reserve System: www.federalreserve.gov
Federal Deposit Insurance Corporation
www.fdic.gov

National Credit Union Administration: www.ncua.gov

Office of the Comptroller of the Currency: www.occ.treas.gov

Office of Thrift Supervision : www.ots.treas.gov

Financial Crimes Enforcement Network: www.fincen.gov

Office of Foreign Assets Control: www.treasury.gov/offices/enforcement/ofac

Federal Financial Institutions Examination Council : www.ffiec.gov

Manuals or Handbooks

Central Bank of Nigeria AML/CFT RBS On-Site Bank Examination Manual For Bank Examination

Central Bank of Nigeria Bank Examiners' Code of Conduct for Bank Examiners

Other Materials

Federal Government of Nigeria

Interagency Committee on Anti Money Laundering/Combating Financing of Terrorism Annual Report

National Focal Point Periodic and Annual Reports

Nigeria Financial Intelligence Unit (NFIU)

NFIU's web site contains the following materials:

i. AML/CFT Statutory Material, Regulations, and Notices — Links to legislation and regulations, as well as to proposed regulations.

ii. AML/CFT Reporting Formats — Links to AML/CFT reporting forms and corresponding preparation and filing instructions.

iii. AML/CFT Guidance — NFIU issues interpretations of AML/CFT regulations as well as guidance to financial institutions on complying with the same.

iv. Reports — NFIU periodically initiates and develops reports and publications covering AML issues, including the STR Activity Review.

v. Advisories — NFIU issues advisories to financial institutions concerning money laundering or terrorist financing threats and vulnerabilities, for the purpose of enabling financial institutions to guard against such threats.

vi. Enforcement actions — NFIU issues releases involving the assessment of civil money penalties against financial institutions for systemic non-compliance with the AML/CFT.

Basel Committee on Banking Supervision (BCBS)

The BCBS Web site (on the Bank for International Settlements' Web site, www.bis.org) contains the following publications:

i. Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers

ii. Consolidated Know Your Customer Risk Management

iii. Sharing of Financial Records between Jurisdictions in Connection with the Fight Against Terrorist Financing

iv. General Guide to Account Opening and Customer Identification

v. Customer Due Diligence for Banks

vi. Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering

vii. Banking Secrecy and International Cooperation in Banking Supervision

Financial Action Task Force on Money Laundering (FATF)

FATF's Web site (www.fatf-gafi.org) contains the following publications:

i. Forty Recommendations to Combat Money Laundering and Terrorism

ii. Special Recommendations Against Terrorist Financing

iii. Interpretive Notes to FATF Recommendations

iv. Non-cooperative Countries or Territories

v. Typologies on Money Laundering Risk

vi. Trade Based Money Laundering

vii. New Payment Methods

viii. The Misuse of Corporate Vehicles, Including Trust and Company Service Providers

ix. Complex Money Laundering Techniques — Regional Perspectives Report

The Nigerian Electronic Payments Association

The NACHA's Web site (www.nacha.org) contains the following:

i. "The Next Generation ACH Task Force: Future Vision of the ACH Network"

ii. NACHA Operating Rules

The Wolfsberg Group

The Wolfsberg Group's Web site (www.wolfsberg-principles.com) contains the following:

i. Wolfsberg AML Principles on Private Banking

ii. Wolfsberg Statement on the Suppression of the Financing of Terrorism

iii. Wolfsberg Statement on Payment Message Standards

iv. Wolfsberg AML Principles for Correspondent Banking

v. Wolfsberg Statement on Monitoring Screening and Searching

vi. Wolfsberg Guidance on Risk Based Approach for Managing Money Laundering Risks

vii. Wolfsberg FAQs on Correspondent Banking

viii. Wolfsberg Trade Finance Principles

ix. Wolfsberg Statement on AML Screening, Monitoring and Searching 2009

APPENDIX D

Statutory Definition of Financial Institution

The term "financial institution" includes the following:

i. Discount house.
ii. Insurance institutions.
iii. Debt factorization and conversion firms.
iv. Bureau de change.
v. Finance company.
vi. Money brokerage firms.
vii. Deposit Money Banks.
viii. Micro-finance Banks.
ix. Finance Companies.

x. Primary Mortgage Institutions.
xi. A licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system.

APPENDIX E

International Organizations

Money laundering and terrorist financing have a widespread international impact. Money launderers have been found to transfer funds and maintain assets on a global level, which makes tracing funds through various countries a complex and challenging process. Most countries support the fight against money laundering and terrorist funding. However, because of the challenges in creating consistent laws or regulations between countries, international groups have developed model recommendations for governments and financial institutions. The two key international bodies in this area are as follows:

i. The Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body established for the development and promotion of policies to combat money laundering and terrorist financing. The FATF has developed recommendations on various money laundering and terrorist financing issues published in the "FATF 40 (forty) Recommendations" and the Nine (9) "Special Recommendations on Terrorist Financing."

ii. The Basel Committee on Banking Supervision is a committee of central banks and bank supervisors and regulators from numerous jurisdictions that meets at the

Bank for International Settlements (BIS) in Basel, Switzerland to discuss issues related to prudential banking supervision. The Basel Committee formulates broad standards and guidelines and makes recommendations regarding sound practices, including those on customer due diligence.

In addition, other global organizations are becoming increasingly involved in combating money laundering. The International Monetary Fund (IMF) and the World Bank have integrated AML and counter-terrorist financing issues into their financial sector assessments, surveillance and diagnostic activities. Furthermore, various FATF-style regional bodies exist. These groups participate as observers in FATF meetings; assess their members against the FATF standards; and, like FATF members, frequently provide input to the IMF and World Bank assessment program.

APPENDIX F

Money Laundering and Terrorist Financing "Red Flags"

The following are examples of potentially suspicious activities or "red flags" for both money laundering and terrorist financing. Although these lists are not all-inclusive, they may help banks and Examiners to recognize possible money laundering and terrorist financing schemes. Management's primary focus should be on reporting suspicious activities, rather than on determining whether the transactions are in fact linked to money laundering, terrorist financing or a particular crime.

The following examples are red flags that, when encountered, may warrant additional scrutiny. The mere presence of a red flag is not by itself evidence of criminal activity. Closer scrutiny should help to determine whether the activity is suspicious or one for which there does not appear to be a reasonable business or legal purpose.

Potentially Suspicious Activity That May Indicate Money Laundering

1. Customers Who Provide Insufficient or Suspicious Information -

i. A customer uses unusual or suspicious identification documents that cannot be readily verified.

ii. A customer provides an individual tax identification number after having previously used a Social Security number.

iii. A customer uses different tax identification numbers with variations of his or her name.

iv. A business is reluctant when establishing a new account to provide complete information about the nature and purpose of its business, anticipated account activity, prior banking relationships, the names of its officers and directors or information on its business location.

v. A customer's home or business telephone is disconnected.

vi. The customer's background differs from that which would be expected on the basis of his or her business activities.

vii. A customer makes frequent or large transactions and has no record of past or present employment experience.

viii. A customer is a trust, shell company or Private Investment Company that is reluctant to provide information on controlling parties and underlying beneficiaries. Beneficial owners may hire nominee incorporation services to establish shell companies and open bank accounts for those shell companies while shielding the owner's identity.

2. Efforts to Avoid Reporting or Record-keeping Requirement -

i. A customer or group tries to persuade a bank employee not to file required reports or maintain required records.

ii. A customer is reluctant to provide information needed to file a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.

iii. A customer is reluctant to furnish identification when purchasing negotiable instruments in recordable amounts.

iv. A business or customer asks to be exempted from reporting or recordkeeping requirements.

v. A person customarily uses the automated teller machine to make several bank deposits below a specified threshold.

vi. A customer deposits funds into several accounts, usually in amounts of less than USA $10,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as non-cooperative countries and territories).

vii. A customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency or accesses a safe deposit box before making currency deposits structured at or just under USA $10,000, to evade CTR filing requirements.

3. Funds Transfers -

i. Many funds transfers are sent in large and rounded amounts.

ii. Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.

iii. Many small, incoming transfers of funds are received, or deposits are made using cheques and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer's business or history.

iv. Large, incoming funds transfers are received on behalf of a foreign client with little or no explicit reason.

v. Funds transfer activity is unexplained, repetitive or shows unusual patterns.

vi. Payments or receipts with no apparent links to legitimate contracts, goods or services are received.

vii. Funds transfers are sent or received from the same person to or from different accounts.

viii. Funds transfers contain limited content and lack related party information.

4. Activity Inconsistent with the Customer's Business -

i. The currency transaction patterns of a business show a sudden change inconsistent with normal activities.

ii. A large volume of cashier's cheques, money orders, or funds transfers is deposited into or purchased through an account when the nature of the accountholder's business would not appear to justify such activity.

iii. A retail business has dramatically different patterns of currency deposits from similar businesses in the same general location.

iv. Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.

v. The owner of both retail business and a cheque-cashing service does not ask for currency when depositing cheues, possibly indicating the availability of another source of currency.

vi. Goods or services purchased by the business do not match the customer's stated line of business.

vii. Payments for goods or services are made by cheques, money orders, or bank drafts not drawn from the account of the entity that made the purchase.

5. Lending Activity -

i. Loans secured by pledged assets are held by third parties unrelated to the borrower.

ii. Loan secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.

iii. Borrower defaults on a cash-secured loan or any loan that is secured by assets which are readily convertible into currency.

iv. Loans are made for or are paid on behalf of a third party with no reasonable explanation.

v. To secure a loan, the customer purchases a certificate of deposit using an unknown source of funds, particularly when funds are provided via currency or multiple monetary instruments.

vi. Loans that lack a legitimate business purpose, provide the bank with significant fees for assuming little or no risk, or tend to obscure the movement of funds (e.g., loans made to a borrower and immediately sold to an entity related to the borrower).

6. Changes in Bank-to-Bank Transactions -

i. The size and frequency of currency deposits increase rapidly with no corresponding increase in non-currency deposits.

ii. A bank is unable to track the true account-holder of correspondent or concentration account transactions.

iii. The turnover in large-denomination bills is significant and appears uncharacteristic, given the bank's location.

iv. Changes in currency-shipment patterns between correspondent banks are significant.

7. Trade Finance -

i. Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).

ii. Customers conducting business in higher-risk jurisdictions.

iii. Customers shipping items through higher-risk jurisdictions, including transit through non-cooperative countries.

iv. Customers involved in potentially higher-risk activities, including activities that may be subject to export/import restrictions (e.g., equipment for

military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil).

v. Obvious over or under-pricing of goods and services.

vi. Obvious misrepresentation of quantity or type of goods imported or exported.

vii. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.

viii. Customer requests payment of proceeds to an unrelated third party.

ix. Shipment locations or description of goods not consistent with letter of credit.

x. Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment. Any changes in the names of parties should prompt additional review.

8. Privately Owned Automated Teller Machines -

i. Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations.

ii. Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armoured car contracts, lending arrangements, or other appropriate documentation.

9. Insurance -

i. A customer purchases products with termination features without concern for the product's investment performance.

ii. A customer purchases insurance products using a single, large premium payment, particularly when payment is made through unusual methods such as currency or currency equivalents.

iii. A customer purchases a product that appears outside the customer's normal range of financial wealth or estate planning needs.

iv. A customer borrows against the cash surrender value of permanent life insurance policies, particularly when payments are made to apparently unrelated third parties.

v. Policies are purchased that allow for the transfer of beneficial ownership interests without the knowledge and consent of the insurance issuer. This would include second-hand endowment and bearer insurance policies.

vi. A customer is known to purchase several insurance products and uses the proceeds from an early policy surrender to purchase other financial assets.

vii. A customer uses multiple currency equivalents (e.g., cashier's cheques and money orders) from different banks and money services businesses to make insurance policy or annuity payments.

10. Shell Company Activity -

i. A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using internet, commercial database searches or direct inquiries to a respondent bank).

ii. Payments to or from the company have no stated purpose, do not reference goods or services or identify only a contract or invoice number.

iii. Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.

iv. Transacting businesses share the same address, provide only a registered agent's address or have other address inconsistencies.

v. Unusually large number and variety of beneficiaries are receiving funds transfers from one company.

vi. Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centres.

vii. A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.

viii. Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.

ix. Purpose of the shell company is unknown or unclear.

11. Embassy and Foreign Consulate Accounts -

i. Official embassy business is conducted through personal accounts.

ii. Account activity is not consistent with the purpose of the account, such as pouch activity or payable upon proper identification transactions.

iii. Accounts are funded through substantial currency transactions.

iv. Accounts directly fund personal expenses of foreign nationals without appropriate controls, including, but not limited to, expenses for college students.

12. Employees -

i. Employee exhibits a lavish lifestyle that cannot be supported by his or her salary.

ii. Employee fails to conform to recognized policies, procedures and processes, particularly in private banking.

iii. Employee is reluctant to take a vacation.

13. Other Unusual or Suspicious Customer Activity -

i. Customer frequently exchanges small-dollar denominations for large-dollar denominations.

ii. Customer frequently deposits currency wrapped in currency straps or currency wrapped in rubber bands that is disorganized and does not balance when counted.

iii. Customer purchases a number of cashier's cheques, money orders, or traveller's cheques for large amounts under a specified threshold.

iv. Customer purchases a number of open-end prepaid cards for large amounts. Purchases of prepaid cards are not commensurate with normal business activities.

v. Customer receives large and frequent deposits from online payments systems yet has no apparent online or auction business.

vi. Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.

vii. Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.

viii. Deposits are structured through multiple branches of the same bank or by groups of people who enter a single branch at the same time.

ix. Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.

x. Customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.

xi. Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area, despite the availability of such services at an institution closer to them.

xii. Customer repeatedly uses a bank or branch location that is geographically distant from the customer's home or office without sufficient business purpose.

xiii. Customer exhibits unusual traffic patterns in the safe deposit box area or unusual use of safe custody accounts. For example, several individuals arrive together, enter frequently, or carry bags or other containers that could conceal large amounts of currency, monetary instruments, or small valuable items.

xiv. Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high-value assets awaiting conversion to currency, for placement into the banking system. Similarly, a customer establishes multiple safe custody accounts to park large amounts of securities awaiting sale and conversion into currency, monetary instruments, outgoing funds transfers, or a combination thereof, for placement into the banking system.

xv. Unusual use of trust funds in business transactions or other financial activity.

xvi. Customer uses a personal account for business purposes.

xvii. Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.

xviii. Customer makes multiple and frequent currency deposits to various accounts that are purportedly unrelated.

xix. Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.

xx. Customer makes high-value transactions not commensurate with the customer's known incomes.

14. Potentially Suspicious Activity That May Indicate Terrorist Financing-

The following examples of potentially suspicious activity that may indicate terrorist financing are primarily based on guidance provided by the FATF. FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels to combat money laundering and terrorist financing.

15. Activity Inconsistent With the Customer's Business -

i. Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as non-cooperative countries and territories).

ii. The stated occupation of the customer is not commensurate with the type or level of activity.

iii. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed or self-employed).

iv. Regarding non-profit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

v. A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.

16. Funds Transfers -

i. A large number of incoming or outgoing funds transfers take place through a business account and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.

ii. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

iii. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.

iv. Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

v. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.

17. Other Transactions That Appear Unusual or Suspicious -

i. Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.

ii. Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.

iii. A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.

iv. Banks from higher-risk locations open accounts.

v. Funds are sent or received via international transfers from or to higher-risk locations.

vi. Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

APPENDIX G

Structuring

Structuring transactions to evade AML/CFT reporting and certain record keeping requirements can result in civil and criminal penalties under the MLPA, 2004.

Structuring is when "a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of other persons, conducts or attempts to conduct one or more transactions in currency in any amount at one or more financial institutions on one or more days, in any manner for the purpose of evading the CTR filing requirements."

Bank employees should be aware of and alert to structuring schemes. For example, a customer may structure currency deposit or withdrawal transactions, so that each is less than the USA $10,000 CTR filing threshold; use currency to purchase official bank cheques, money orders, or traveller's cheques with currency in amounts less than USA $10,000 (and possibly in amounts less than the $5,000 recordkeeping threshold for the currency purchase of monetary instruments to avoid having to produce identification in the process); or exchange small bank notes for large ones in amounts less than USA $10,000.

However, two transactions slightly under the USA $10,000 threshold conducted days or weeks apart may not necessarily be structuring. For example, if a customer deposits USA $9,900 in currency on Monday and deposits USA $9,900 in currency on Wednesday, it should not be assumed that structuring has occurred. Instead, further review and research may be necessary to determine the nature of the transactions, prior account history and other relevant customer information to assess whether the activity is suspicious. Even if structuring has not occurred, the bank should review the transactions for suspicious activity.
In addition, structuring may occur before a customer brings the funds to a bank. In these instances, a bank may be able to identify the aftermath of structuring. Deposits of

monetary instruments that may have been purchased elsewhere might be structured to evade the CTR filing requirements or the record-keeping requirements for the currency purchase of monetary instruments. These instruments are often numbered sequentially in groups totaling less than USA $10,000 or USA $5,000; bear the same handwriting (for the most part) and often the same small mark, stamp, or initials; or appear to have been purchased at numerous places on the same or different days.

APPENDIX H

Request Letter Items for Core/Expanded Examination Procedures

As part of the examination planning process, the Examiner should prepare a request letter. The list below includes materials that Examiners may request or request access to in a financial institution during AML/CFT examination. This list should be tailored for the specific financial institution's risk profile and the planned examination scope. Additional materials may be requested as needed.

1. AML/CFT Compliance Program

i. Name and title of the designated CCO and (if different) the name and title of the person responsible for monitoring AML/CFT compliance.

   a. Organization charts showing direct and indirect reporting lines.

   b. Copies of résumés and qualifications of new person(s) to the financial institution serving in AML/CFT Compliance Program oversight capacities.

ii. Make available copies of the most recent written AML/CFT Compliance Program approved by board of directors (or the statutory equivalent of such a program for foreign-owned financial institutions operating in Nigeria) including CIP requirements with date of approval noted in the board minutes.

iii. Make available copies of the policy and procedures relating to all the reporting and recordkeeping requirements including STR filing.

iv. Correspondence addressed between the financial institution, its personnel or agent, and its branches, FIRS, CBN, NFIU or law enforcement authorities since the previous AML/CFT examination. For example, please make available NFIU correspondence related to CTR errors or omissions.

2. Independent Testing

i. Make available copies of the results of any internally or externally sourced independent audits or tests performed since the previous AML/CFT examination including the scope or engagement letter, management's responses and access to the work-papers.

ii. Make available access to the auditor's risk assessment, audit plan (schedule), and program used for the audits or tests.

3. Training

i. Training documentation (e.g., materials used for training since the previous AML/CFT examination).

ii. AML/CFT training schedule with dates, attendees and topics. A list of persons in positions for which the financial institution typically requires AML/CFT training but who did not participate in the training.

4. Risk Assessment

i. Make available copies of management's AML/CFT risk assessment of products, services, customers and geographic locations.

ii. List of financial institutions identified as having higher-risk accounts.

5. Customer Identification Program

i. List of accounts without taxpayer identification numbers (TIN).

ii. File of correspondence requesting TINs for bank customers.

iii. A copy of any account opening forms (e.g., for loans, deposits or other accounts) used to document CIP/Customer Due Diligence information.

iv. Written description of the financial institution's rationale for CIP exemptions for existing customers who open new accounts.

v. List of new accounts covering all product lines (including accounts opened by third parties) and segregating existing customer accounts from new customers for the period between..... &..... The Examiner should indicate by inserting the period of time appropriate for the size and complexity of the financial institution.

vi. List of any accounts opened for a customer that provides an application for a TIN.

vii. List of any accounts opened in which verification has not been completed or any accounts opened with exceptions to the CIP.

viii. List of customers or potential customers for whom the financial institution took adverse action on the basis of its CIP.

ix. List of all documentary and non-documentary methods the bank uses to verify a customer's identity.

x. Make available customer notices and a description of their timing and delivery by product.

xi. List of the financial institutions on which the bank/ financial institution is relying on for identification purpose, if the bank/financial institution is using the "reliance provision." The list should note if the relied-upon financial institutions are subject to a rule requiring the implementation of the AML/CFT Compliance Program of MPLA and AML/CFT Regulation issued by the CBN.

xii. Provide the following:
   a. Copies of any contracts signed between the parties.
   b. Copies of the CIP or procedures used by the other party.
   c. Any certifications made by the other party.

xiii. Copies of contracts with financial institutions and with third parties that perform all or any part of the financial institution's CIP.

6. Suspicious Transaction Reporting

i. Provide access to STRs filed with NFIU during the review period and the supporting documentation. Include copies of any filed STRs that were related to requests for information or to information sharing requests.

ii. Any analysis or documentation of any activity for which a STR was considered but not filed, or for which the financial institution is actively considering filing a STR.

iii. Description of expanded monitoring procedures applied to higher-risk accounts.

iv. Determination of whether the bank uses a manual or an automated account monitoring system, or a combination of the two. If an automated system is used, determine whether the system is proprietary or vendor supplied. If the system was provided by an outside vendor, request (i) a list that includes the vendor, (ii) application names, and (iii) installation dates of any automated account monitoring system provided by an outside vendor. Request a list of the algorithms or rules used by the systems and copies of the independent validation of the software against these rules.

v. Make available copies of reports used for identification of and monitoring for suspicious transactions. These reports include, but are not limited to suspected kiting reports, CTRs, monetary instrument records and funds transfer reports. These reports can be generated from specialized AML/CFT software, the financial institution's general data processing systems or both.

vi. If not already provided, copies of other reports that can pinpoint unusual transactions warranting further review. Examples include non-sufficient funds (NSF) reports, account analysis fee income reports and large item reports.

vii. Provide name, purpose, parameters and frequency of each report.

viii. Correspondence received from law enforcement authorities concerning the disposition of accounts reported for suspicious activity.

ix. Make available copies (or a log) of criminal subpoenas received by the financial institution since the previous examination or inspection.

x. Make available copies of policies, procedures and processes used to comply with all criminal subpoenas related to MPLA & AML/CFT Regulation.

7. Currency Transaction Reporting

i. Provide information on and access to CTR filed for the review period.

ii. Provide information on & access to internal reports used to identify reportable currency transactions for the review period.

iii. Make the list of products or services that may involve currency transactions.

8. Currency Transaction Reporting Exemptions (Not Applicable)

i. Access to filed Designation of Exempt Person form(s) for current exemptions.

ii. List of customers exempted from CTR filing and the documentation to support the exemption (e.g., currency transaction history or, as applicable, risk-based analysis).

iii. Access to documentation of required annual reviews for CTR exemptions.

9. Information Sharing

i. Make available documentation demonstrating that required searches have been performed.

ii. Make available any vendor-confidentiality agreements, if applicable.

iii. Make available copies of policies, procedures and processes for complying with Information Sharing Between Law Enforcement Agencies and Financial Institutions.

iv. If applicable, a copy of the financial institution's most recent notification form to voluntarily share information with other financial institutions - Voluntary Information Sharing Among Financial Institutions, or a copy of the most recent correspondence received from NFIU or CBN that acknowledges receipt of the financial institution's notice to voluntarily share information with other financial institutions.

v. If applicable, make available copies of policies, procedures and processes for complying.

10. Purchase and Sale of Monetary Instruments

Access to records of sales of monetary instruments in amounts between N2 million and N5 million (if maintained with individual transactions, provide samples of the record made in connection with the sale of each type of monetary instrument).

11. Funds Transfers Record-keeping

Access to records of funds transfers, including incoming, intermediary and outgoing transfers of N10 million or more.

12. Foreign Correspondent Account Recordkeeping and Due Diligence

i. List of all foreign correspondent bank accounts, including a list of foreign financial institutions for which the financial institution provides or provided regular services and the date on which the required information was received (either by completion of a certification or by other means).

ii. If applicable, documentation to evidence compliance - Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process and Summons or Subpoena of Foreign Bank Records; Termination of Correspondent Relationship for foreign correspondent bank accounts and shell banks.

iii. List of all payable through relationships with foreign financial institutions.

iv. Access to contracts or agreements with foreign financial institutions that have payable through accounts.

v. List of the bank's foreign branches and the steps the financial institution has taken to determine whether the accounts with its branches are not used to indirectly provide services to foreign shell banks.

vi. List of all foreign correspondent bank accounts and relationships with foreign financial institutions that have been closed or terminated in compliance with the conditions (service to foreign shell banks, records of owners and agents).

vii. List of foreign correspondent bank accounts that have been the subject of Information Sharing Between Law Enforcement Agencies and Financial Institutions or any other information request from law enforcement officers for information regarding foreign correspondent bank accounts and evidence of compliance.

viii. Any directive/notice to close foreign correspondent bank accounts from the CBN.

ix. Ix. List of all the bank's embassy or consulate accounts, or other accounts maintained by foreign government, foreign embassy, or foreign political figure.

x. List of all account-holders and borrowers domiciled outside Nigeria, including those with Nigeria power of attorney.

13. Currency-Shipment Activity

Make available records reflecting currency shipped to and received from the CBN or correspondent banks or reflecting currency shipped between branches and the bank's central currency vaults for the previous _____ months. Examiner is to insert a period of time appropriate for the size and complexity of the financial institution.

14. Other MPLA Reporting and Record-keeping Requirements

i. Record retention schedule and procedural guidelines.

ii. File of Reports of International Transportation of Currency or Monetary Instruments (CMIR)

iii. Records of Report of Foreign Bank and Financial Accounts.

15. Expanded Examination Procedures

As part of the examination planning process, the Examiner should prepare a request letter. The listing below includes materials that may be requested for a financial institution AML/CFT examination. This list should be tailored for the specific institution profile and the planned examination scope. Additional materials may be requested as needed.

16. Correspondent Accounts (Domestic)

i. Make available copies of policies, procedures and processes specifically for correspondent bank accounts, including procedures for monitoring for suspicious activity.

ii. Make available a list of domestic correspondent bank accounts.

iii. Provide a list of STRs filed relating to domestic correspondent bank accounts.

17. Correspondent Accounts (Foreign)

i. Make available copies of policies, procedures and processes specifically for foreign correspondent financial institution accounts, including procedures for monitoring for suspicious activity.

ii. Make available a list of foreign correspondent financial institution accounts.

iii. Provide risk assessments covering foreign correspondent financial institution account relationships.

iv. Provide a list of STRs filed relating to foreign correspondent financial institution accounts.

18. Bulk Shipments of Currency

i. Make available copies of policies, procedures and processes related to receiving shipments of bulk currency. Describe expanded monitoring procedures applied to currency originators and intermediaries.

ii. Make available a list of currency originators, intermediaries, including referral agents, and foreign and domestic customers that send bulk currency shipments to the financial institution.

iii. Provide a list of all foreign and domestic correspondent bank accounts, including a list of foreign financial institutions from which the financial institution receives or sends bulk currency shipments.

iv. Provide a copy of management's risk assessment of relationships and transactions of currency originators and intermediaries.

v. Make available copies of reports used for identification of and monitoring for suspicious transactions related to currency originators and intermediaries. Make available agreements or contracts with currency originators or intermediaries. Provide a list of STRs filed related to shipping relationships and transactions.

19. Nigeria Naira Drafts

i. Make available copies of policies, procedures and processes specifically for Naira drafts including procedures for monitoring for suspicious activity.

ii. Make available a list of foreign correspondent bank accounts that offer Naira drafts. If possible, include the volume by number and Naira amount of monthly transactions for each account.

iii. Provide a list of STRs filed relating to Nigeria Naira drafts.

20. Payable Through Accounts

i. Make available copies of policies, procedures and processes specifically for payable through accounts (PTA) including procedures for monitoring for suspicious activity.

ii. Make available a list of foreign correspondent bank accounts with PTAs. Include a detailed summary (number and monthly naira volume) of sub-account-holders for each PTA.

iii. Provide a list of STRs filed relating to PTAs.

21. Pouch Activities

i. Make available copies of pouch activity policies, procedures and processes including procedures for monitoring for suspicious activity.

ii. Provide a list of customer accounts permitted to use pouch services.

iii. Provide a list of CTRs, CMIRs or STRs filed relating to pouch activity.

iv. As needed, provide a copy of pouch logs.

22. Foreign Branches and Offices of Nigerian Banks

i. Make available copies of policies, procedures and processes specific to the foreign branch or office, if different from the parent's policies, procedures and processes.

ii. Provide most recent management reports received on foreign branches and offices.

iii. Make available copies of the bank's tiering or organizational structure report.

iv. Provide AML/CFT audit reports, compliance reports and supporting documentation for the foreign branches and offices.

v. Provide a list of the types of products and services offered at the foreign branches and offices and information on new products or services offered by the foreign branch, including those that are not already offered by the parent financial institution.

vi. Provide a description of the method for aggregating each customer relationship across business units and geographic locations throughout the organization.

vii. Provide the code of ethics for foreign branches or offices, if it is different from the financial institution's standard policy.

viii. When testing will be performed, provide a list of accounts originated or serviced in the foreign branch or office. Examiners should try to limit this request and focus on accounts for specific products or services, higher-risk accounts only, or accounts for which exceptions or audit concerns have been noted.

ix. Provide a list of the locations of foreign branches and offices, including, if possible, the host country regulatory agency and contact information.

x. Provide the organizational structure of the foreign branches and offices, including reporting lines to the Nigerian financial institution level.

23. Parallel Banking

i. Provide a list of any parallel banking relationships.

ii. Make available copies of policies, procedures and processes specifically for parallel banking relationships, including procedures relating to higher-risk money laundering activities. Such policies and procedures should include those that are specific to the relationship with the parallel entity.

iii. Provide a list of STRs filed relating to parallel banking relationships.

iv. Make available documents that specify limits or procedures that should be followed when dealing with the parallel entity.

v. Provide a list of directors or officers of the financial institution who are also associated with the foreign parallel bank.

24. Electronic Banking

i. Make available copies of any policies and procedures related directly to electronic banking (e-banking) that are not already included in the AML/CFT policies.

ii. Provide management reports that indicate the monthly volume of e-banking activity.

iii. Provide a list of business customers regularly conducting e-banking transactions, including the number and Naira volume of transactions.

iv. Make available a list of service providers related to Remote Deposit Capture (RDC) activities.

v. Make available copies of contracts related to RDC activities.

25. Funds Transfers

i. Provide funds transfer activity logs, including funds transfers that involved cover payments, including transfers into and out of the financial institution. Include the number and Naira volume of funds transfer activity for the month.

ii. Provide a list of funds transfers purchased with currency over a specified time period.

iii. Provide a list of non-customer transactions over a specified time period.

iv. If not already included in the AML/CFT policies, make available copies of any policies, procedures and processes related to funds transfers, including transfers that involve cover payments or payable upon proper identification (PUPID).

v. Provide a list of suspense accounts used for PUPID proceeds.

vi. Provide a list of PUPID transactions completed by the financial institution, either as the beneficiary financial institution or as the originating financial institution.

26. Automated Clearing House Transactions

i. Make available copies of any policies and procedures related directly to automated clearing house (ACH) and international ACH transactions (IAT) that are not already included in the AML/CFT policies.

ii. Make available copies of management reports that indicate the monthly volume of ACH activity, including IATs.

iii. Make available a list of large or frequent ACH transactions or IATs.

iv. Make available a list of IATs (both those originated from or received by the financial institution).

v. Make available a list of customer complaints regarding ACH transactions and IATs.

27. Electronic Cash

i. Make available copies of any policies and procedures related directly to electronic cash (e-cash), including prepaid cards that are not already included in the AML/CFT policies.

ii. Provide management reports that indicate the monthly volume of e-cash activity, including prepaid cards.

iii. Provide a list of business customers regularly conducting e-cash transactions, including prepaid cards, the number and Naira volume of transactions.

28. Third-Party Payment Processors

i. If not already included in the AML/CFT policies, make available copies of any policies, procedures and processes related to third-party payment processors.

ii. Provide a list of third-party payment processor relationships. Include the number and Naira volume of payments processed per relationship.

iii. Provide a list of STRs filed on third-party payment processor relationships.

29. Purchase and Sale of Monetary Instruments

i. If not already included in the AML/CFT policies, make available copies of any policies, procedures and processes related to the sale of monetary instruments for currency. In particular, include policies, procedures and processes related to the monitoring sales of monetary instruments in order to detect unusual activities.

ii. Provide monetary instrument logs or other MIS reports used for the monitoring and detection of unusual or suspicious activities relating to the sales of monetary instruments.

iii. Provide a list of non-customer transactions over a specified period of time.

iv. Provide a list of monetary instruments purchased with currency over a specified time period.

v. Provide a list of STRs filed related to the purchase or sale of monetary instruments.

30. Brokered Deposits

i. Make available copies of specific policies and procedures specifically for brokered

ii. Deposits, including procedures for monitoring for suspicious activity.

iii. Provide risk assessment covering brokered deposits.

iv. Provide internal audits covering brokered deposits.

v. Provide a list of approved deposit brokers.

vi. Provide management reports covering non-relationship funding programs (including reports on balances, concentrations, performance or fees paid).

vii. Provide STRs and subpoenas related to brokered deposit relationships.

viii. Provide a copy of account documentation or agreements for deposit broker arrangements.

31. Privately Owned Automated Teller Machines

i. Provide a risk assessment covering privately owned automated teller machines (ATM) and Independent Sales Organizations (ISO) including a list of higher-risk privately owned ATM relationships.

ii. Make available copies of policies, procedures and processes for privately owned ATM and ISO account acceptance, due diligence and ongoing monitoring.

iii. Provide a list of ISO clients and balances.

iv. Provide STRs and subpoenas related to privately owned ATMs and ISOs.

32. Non-deposit Investment Products

i. Make available copies of policies, procedures and processes relating to non-deposit investment products (NDIP) and relationships with any independent NDIP providers.

ii. Provide internal audits covering NDIP sales and provider relationships.

iii. Provide a risk assessment covering NDIP customers and transactions.

iv. If available, provide a list of NDIP clients and balances.

v. Provide a list of suspense, concentration or omnibus accounts used for NDIP. Describe the purpose for and controls surrounding each account.

vi. Provide management reports covering 25 to 50 of the largest most active and most profitable NDIP customers.

vii. Provide STRs and subpoenas related to NDIP customers.

viii. Make available a copy of account opening documentation or agreements for NDIP.

ix. Make available a copy of contracts or agreements between the bank and third-party NDIP providers for the completion of CIP, due diligence and ongoing monitoring of NDIP customers.

33. Insurance

i. Make available copies of AML/CFT policies and procedures related to the sale of insurance.

ii. Provide risk assessment covering insurance products.

iii. Make available MIS reports related to the sales of insurance products. Reports may include large transaction reports, single premium payments, early cancellation, premium overpayments and assignments of claims.

iv. Make available a copy of contracts or agreements between the financial institution and insurance providers for the completion of CIP, due diligence and ongoing monitoring of insurance customers.

v. Provide a list of insurance products approved for sale at the financial institution.

vi. Provide management reports covering insurance products (including large transactions, funds transfers, single premium payments and early cancellations).

vii. Provide STRs or subpoenas related to insurance clients.

viii. Provide a copy of account documentation requirements and applications for insurance products.

34. Concentration Accounts

i. Make available copies of AML/CFT policies, procedures and processes that are specific to concentration accounts (also known as special-use, omnibus, suspense, settlement, intraday, sweep or collection accounts).

ii. Provide a list of all concentration accounts and each account's most recent reconciliation statements.

iii. Provide account activity reports for concentration accounts for _____. Examiner to insert a period of time appropriate for the size and complexity of the financial institution.

35. Lending Activities

i. Make available copies of AML/CFT policies and procedures specific to lending.

ii. Provide a risk assessment relating to the lending function, including a list of any higher-risk lending relationships identified by the financial institution.

iii. For loans secured by cash collateral, marketable securities or cash surrender value of life insurance products:

a. Provide a list of all loans that have defaulted since the previous AML/CFT examination including those that were charged off. Provide a list of all loans that have been extended since the previous AML/CFT examination.

36. Trade Finance Activities

i. Make available copies of AML/CFT policies and procedures specific to trade finance activities.

ii. Provide a risk assessment relating to trade finance activities including a list of any higher-risk trade finance transactions, accounts or relationships identified by the financial institution.

iii. Provide a list of customers involved in transactions with higher-risk geographic locations or for whom the financial institution facilitates trade finance activities with higher-risk geographic locations.

37. Private Banking

i. Make available copies of policies, procedures and controls used to manage AML/CFT risks in the private banking department.

ii. Make available business or strategic plans for the private banking department.

iii. Provide the most recent version of management reports on private banking activity such as customer aggregation reports, policy exception reports, client concentrations, customer risk classification reports and unusual account activity.

iv. Provide recent private banking reports from compliance, internal audit, risk management and external auditors or consultants that cover AML/CFT.

v. Provide a list of products and services offered to private banking clients. Information on new products and services offered to private banking clients and the financial institution's process for approving new activities.

vi. Provide a description of the method for aggregating customer holdings and activities across business units throughout the organization.

vii. Provide a description of account officer and manager positions and the compensation, recruitment and training program for these positions.

viii. Make available the code of ethics policy for private banking officers.

ix. Provide a risk assessment covering private banking customers and transactions.

x. Provide a list of suspense, concentration or omnibus accounts used for private banking transactions. Describe the purpose for each account and the controls governing it.

xi. Provide management reports covering 25 to 50 of the largest most active or most profitable private banking customers.

xii. Provide a list of the financial institution's private banking account-holders who meet the following criteria:

a. Politically exposed persons (PEP), export or import business owners, money transmitters, Private Investment Companies (PIC), financial advisers, offshore entities or money managers (when an intermediary is acting on behalf of customers).

b. Customers who were introduced to the financial institution by individuals previously employed by other financial institutions.

c. Customers who were introduced to the financial institution by a third-party investment adviser.

d. Customers who use nominee names.

e. Customers who are from or do business with a higher-risk geographic location.

f. Customers who are involved in cash-intensive businesses.

g. Customers who were granted exceptions to policies, procedures and controls.

h. Customers who frequently appear on unusual activity monitoring reports.

xiii. Provide STRs and subpoenas related to private banking customers.

xiv. Make available a copy of account-opening documentation or agreements for private banking customers.

38. Trust and Asset Management Services

i. Make available copies of AML/CFT policies, procedures and processes for trust and asset management services.

ii. Make available trust and asset management procedures and guidelines used to determine when EDD is appropriate for higher-risk accounts and parties to the relationship. These should include methods for identifying account-interested parties (i.e., individual grantors, co-trustees or outside investment managers).

iii. Provide a list of politically exposed persons (PEP), export or import business owners, money transmitters, Private Investment Companies (PIC), financial advisers, offshore entities or money managers (when an intermediary is acting on behalf of customers).

iv. Provide a list of financial institution's trust and asset management account-householders who meet the following criteria:

a. Customers who were introduced to the financial institution by individuals previously employed by other financial institutions.

b. Customers who were introduced to the financial institution by a third-party investment adviser.

c. Customers who use nominee names.

d. Customers who are from or do business with a higher-risk geographic location.

e. Customers who are involved in cash-intensive businesses.

f. Customers who were granted exceptions to policies, procedures and controls.

g. Customers who frequently appear on unusual activity monitoring reports.

V. Make available reports and minutes submitted to the board of directors or its designated committee relating to AML/CFT matters pertaining to trust and asset management business lines and activities.

vi. Provide an organizational chart for the AML/CFT compliance function as it relates to the trust and asset management services.

vii. Provide a risk assessment of trust and asset management services that identifies those customers, prospective customers or products the financial institution has determined to be higher risk.

viii. Provide management reports covering 25 to 50 of the largest most active or most profitable trust and asset management customers.

ix. Provide a AML/CFT independent review or audit of trust and asset management services. Make work-papers available upon request.

x. Make available a copy of the AML/CFT training materials for management and employees involved in trust and asset management activities.

xi. Identify the trust accounting systems used. Briefly explain how they accommodate and assist compliance with AML/CFT regulations and guidelines.

xii. Provide a list of newly opened trust and asset management accounts since _____. Examiner is to insert a period of time appropriate for the size and complexity of the financial institution.

xiii. Provide procedures for checking requests relating to trust and asset management services.

xiv. Provide a list of all trust and asset management accounts designated as higher risk and a list of all accounts whose assets consist of PICs and asset protection trusts.

xv. Provide copies of STRs associated with trust and asset management services.

xvi. Provide a list of subpoenas, particularly AML/CFT-related relating to trust and asset management activities.

39. **Non-resident Aliens and Foreign Individuals**

i. Make available copies of policies, procedures and processes specific to non-resident alien (NRA) accounts, including guidelines and systems for establishing and updating any exempt status.

ii. Provide a list of NRA and foreign individual accounts held by the financial institution, particularly those accounts the financial institution has designated as higher risk.

iii. Provide a list of NRA and foreign individual accounts without a TIN, passport number or other appropriate identification number.

iv. Provide a list of STRs and subpoenas related to NRA and foreign individual accounts.

40. **Politically Exposed Persons**

i. Make available copies of policies, procedures and processes specific to politically exposed persons (PEP). Policies should include the financial institution's definition of a PEP as well as procedures for opening PEP accounts and senior management's role in the approval process for opening PEP accounts.

ii. Provide a list of accounts in the name of or for the benefit of a PEP. List should include the country of residence of the PEP, the account balances and the average number and Naira volume of transactions per month.

iii. Provide a list of the information systems or other methods used to identify PEP accounts.

iv. Make available management reports used to monitor PEP accounts including reports for identifying unusual and suspicious activity.

41. Embassy and Foreign Consulate Accounts

i. Make available copies of policies, procedures and processes specific to embassy and foreign consulate account relationships.

ii. Provide a list of embassy and foreign consulate accounts held by the financial institution, including the average account balances and the average number and dollar volume of transactions per month.

iii. Provide a list of accounts that are in the name of individuals who work for the embassy or foreign consulate.

42. Designated non-financial Institutions (DNFIs)

i. Make available copies of policies, procedures and processes related to DNFI
ii. Provide a list of designated non-financial institution accounts including all related accounts.
iii. Provide a risk assessment of DNFI accounts, identifying those accounts the financial institution has designated as higher risk. This list should include products and services offered by the DNFI; the average account balance; and the average number, type, and Naira volume of transactions per month.
iv. Provide a list of foreign DNFI accounts, including the products and services offered; the average account balance; and the average, number, type, and dollar and Naira volume of transactions per month.
v. Provide a sample of account opening documentation for higher-risk DNFIs.
vi. Provide a list of STRs and subpoenas related to DNFIs.

43. Professional Service Providers

i. Make available copies of policies, procedures and processes related to professional service provider accounts.
ii. Provide a list of professional service provider accounts, including all related accounts (such as interest on lawyers' trust accounts (IOLTA) which should include the name of the attorney on each account).
iii. Provide a list of any professional service provider accounts that the financial institution has designated as higher risk.

44. Non-governmental Organizations and Charities

i. Make available copies of policies, procedures and processes related to non-governmental organizations and charities.
ii. List of non-governmental organizations and charities, particularly those that the financial institution has designated as higher risk. This list should include average account balances and the average number and Naira volume of transactions.
iii. List of non-governmental organizations involved in higher-risk geographic locations.

45. Business Entities (Domestic and Foreign)

i. Make available copies of policies, procedures and processes specifically related to domestic and international business entities.

ii. Provide a list of accounts opened by business entities. If this list is unreasonably long, amend the request to look at those entities incorporated in higher-risk jurisdictions or those accounts the financial institution has designated as higher risk.

iii. Provide a list of loans to business entities collateralized by bearer shares.

46. Cash-Intensive Businesses

i. Make available copies of policies, procedures and processes related to other businesses and entities.

ii. Provide risk assessment of other businesses and entities, list those other businesses and entities that the financial institution has designated as higher risk. The listing should include average account balances and the average number and Naira volume of transactions.

APPENDIX I

Quantity of Risk Matrix

Financial institutions and Examiners may use the following matrix to formulate summary conclusions. Prior to using this matrix, they should familiar themselves with the identification and quantification.

Low	Moderate	High
Stable, known customer base.	Customer base increasing due to branching, merger or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the Web site is informational or non-transactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
On the basis of information received from the AML/CFT-reporting database, there are few or no large currency or structured transactions.	On the basis of information received from the AML/CFT-reporting database, there is a moderate volume of large currency or structured transactions.	On the basis of information received from the AML/CFT-reporting database, there is a significant volume of large currency or structured transactions.
Identified a few higher-risk customers and businesses.	Identified a moderate number of higher-risk customers and businesses.	Identified a large number of higher-risk customers and businesses.

No foreign correspondent financial institution accounts. The financial institution does not engage in pouch activities, offer special-use accounts or offer payable through accounts.	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML/CFT policies and procedures from lower-risk countries, and minimal pouch activities, special-use accounts, offer payable through accounts (PTAs).	The bank maintains a large number of foreign correspondent financial institution accounts with financial institutions with inadequate AML/CFT policies and procedures, particularly those located in higher-risk jurisdictions, or offers substantial pouch activities, special-use accounts (PTAs).
Low	Moderate	High
The bank or other financial institution offers limited or no private banking/other financial institution services or trust and asset management products or services.	The bank or other financial institution offers limited domestic private banking services or trust and asset management products or services over which the bank/ other financial institution has investment discretion. Strategic plan may be to increase trust business.	The bank or other financial institution offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly nondiscretionary versus where the bank/ other financial institution has full investment discretion.
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers, noncustomers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically lower-risk countries.	A large number of noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions. Frequent funds from personal or business accounts to or from higher-risk jurisdictions, and financial secrecy havens or jurisdictions.
The bank or other financial institution is not located in a High Intensity Financial Crime Area (HIFCA). No fund transfers or account relationships involve HIFCAs.	The bank or other financial institution is located in an HIFCA. Bank/ other financial institution has some fund transfers or account relationships that involve HIFCAs.	Bank/ other financial institution is located in an HIFCA. A large number of fund transfers or account relationships involve HIFCAs.
No transactions with higher-risk geographic locations.	Minimal transactions with higher-risk geographic locations.	Significant volume of transactions with higher-risk geographic locations.
Low turnover of key personnel or frontline personnel (e.g., customer service representatives, tellers or other branch personnel).	Low turnover of key personnel but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

APPENDIX J

STR quality guidance

The following information is provided as guidance:

Often STRs have been instrumental in enabling law enforcement agencies (LEAs) to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in STR forms also allows AML/CFT regulators to identify emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

Financial institutions must file STR forms that are complete, sufficient and timely. Unfortunately, some financial institutions file STR forms that contain incomplete, incorrect or disorganized narratives, making further analysis difficult, if not impossible. Some STR forms are submitted with blank narratives. Because the STR narrative serves as the only free text area for summarizing suspicious activity, the narrative section is critical. The care with which the narrative is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood by AML/CFT regulators and LEAs and thus a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the STR.

The STR form should include any information readily available to the filing financial institution obtained through the account opening process and due diligence efforts. **In general, a STR narrative should identify the five essential elements of information (who? what? when? where? and why?) for the suspicious activity being reported. The method of operation (or how?) is also important and should be included in the narrative.**

WHO is conducting the suspicious activity?

While one section of the STR form calls for specific suspect information, the narrative should be used to further describe the suspect or suspects, **including occupation, position or title within the business, the nature of the suspect's business (or businesses) and any other information and identification numbers associated with the suspects.**

WHAT instruments or mechanisms are being used to facilitate the suspect transactions?

A list of instruments or mechanisms that may be used in suspicious activity includes, but is not limited to, funds transfers, letters of credit and other trade instruments, **correspondent accounts, casinos, structuring, shell companies, bonds or notes, stocks, mutual funds, insurance policies, traveller's cheques, bank drafts, money orders, credit or debit cards, prepaid cards, and digital currency business services.** The STR narrative

should list the instruments or mechanisms used in the reported suspicious activity. If a STR narrative summarizes the flow of funds, **the narrative should always include the source of the funds (origination) and the use, destination or beneficiary of the funds.**

WHEN did the suspicious activity take place?

If the activity takes place over a period of time, indicate the date when the suspicious activity was first noticed and describe the duration of the activity. When possible, in order to better track the flow of funds, individual dates and amounts of transactions should be included in the narrative rather than only the aggregated amount.

WHERE did the suspicious activity take place?

The narrative should indicate if multiple offices of a single financial institution were involved in the suspicious activity and provide the addresses of those locations. The narrative should also specify if the suspected activity or transactions involves a foreign jurisdiction.

WHY does the filer think the activity is suspicious?

The STR reporter should describe, as fully as possible, why the activity or transaction is unusual for the customer, considering the types of products and services offered by the filing financial institution's industry and drawing any applicable contrasts with the nature and normally expected activities of similar customers.

HOW did the suspicious activity occur?

The narrative should describe the "modus operandi" or the method of operation of the subject conducting the suspicious activity. In a concise, accurate and logical manner, the narrative should describe how the suspect transaction or pattern of transactions was committed. For example, if what appears to be structuring of currency deposits is matched with outgoing funds transfers from the accounts, the STR narrative should include information about both the structuring and outbound transfers including dates, destinations, amounts, accounts, frequency and beneficiaries of the funds transfers.

A financial institution should not include any supporting documentation with a filed STR nor use the terms "see attached" in the STR narrative.

Financial institutions should keep any supporting documentation in their records for five years so that this information is available to LEAs & regulatory agencies upon request.

APPENDIX K

Quantity of Risk Matrix — OFAC Procedures

Examiners should use the following matrix, as appropriate, when assessing a financial institution's risk of encountering an OFAC issue:

Low	Moderate	High
Stable, well-known customer base in a localized environment.	Customer base changing due to branching, merger, or acquisition in the domestic market.	A large, fluctuating client base in an international environment.
Few higher-risk customers; these may include non-resident aliens, foreign individuals (including accounts with U.S. powers of attorney), and foreign commercial customers.	A moderate number of higher-risk customers.	A large number of higher-risk customers.
No overseas branches and no correspondent accounts with foreign banks.	Overseas branches or correspondent accounts with foreign banks.	Overseas branches or multiple correspondent accounts with foreign banks.
No electronic banking (e-banking) services offered, or products available are purely informational or non-transactional.	The bank offers limited e-banking products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
Limited number of funds transfers for customers and noncustomers, limited third-party transactions, and no international funds transfers.	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts.	A high number of customer and noncustomer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH, and management of sovereign debt.	Limited other types of international transactions.	A high number of other types of international transactions.
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	A small number of recent actions (e.g., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the bank addressed the issues and is not at risk of similar violations in the future	Multiple recent actions by OFAC, where the bank has not addressed the issues, thus leading to an increased risk of the bank undertaking similar violations in the future.

APPENDIX L

Examiners' Tools for Transaction Testing

1. Currency Transaction Reporting and Suspicious Transaction Reporting

If the financial institution does not have preset filtering reports for currency transaction reporting and the identification of suspicious currency transactions, the Examiner should consider requesting a custom report. For example, a report could be generated with the following criteria: currency transactions of N 1 million or higher (in and out) for the preceding period (to be determined by the Examiner) before the date of examination. The time period covered and the transaction amounts may be adjusted as determined by the Examiner. The report should also capture:

i. The customer information file (CIF) number, if available or taxpayer identification number (TIN).

ii. The date, amount and account number of each transaction.

iii. The teller and branch or other applicable identifying information.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The data can be sorted in a number of different criteria (e.g., by branch, by teller, by TIN or CIF number, if available). Analysis of this information should enable the Examiner to determine whether CTRs and STRs have been appropriately filed.

2. Funds Transfer Monitoring

If the financial institution does not have preset filtering reports for funds transfer record-keeping and the identification of suspicious transactions, the Examiner should consider requesting a custom report. The Examiner may consider requesting that the financial institution provide a report from its funds transfer systems that identifies all funds transfers (in and out) for a time period determined by the Examiner. **The report should also capture:**

i. The customer's full name, country of residence, TIN and AML/CFT risk rating, if applicable.

ii. The date, amount, transaction type and account number of each transaction.

iii. The originator's name, country, financial institution and account number.

iv. The beneficiary's name, country, financial institution and account number.

The financial institution should provide a list of financial institution internal codes necessary to fully identify the account type, AML/CFT risk rating, country, transaction type, financial institution number, account number, and any other codes on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient originator or beneficiary information. Missing information may indicate funds transfer monitoring deficiencies. A large number of transfers or those

of high currency amounts to and from higher-risk jurisdictions or involving parties that do not appear likely to be involved in such transactions may indicate the need for additional scrutiny.

3. **Adequacy of Deposit Account Information and Trust and Asset Management Account Information**

This test is designed to ensure that the financial institution is in compliance with the CIP regulatory requirements and to test the adequacy of the financial institution's CDD policies, procedures and processes.

The Examiner should request an electronic list (spreadsheet or database) of all deposit accounts and trust/asset management accounts as of the date of examination. The balances should be reconciled to the general ledger. **The report should also capture:**

i. The customer's full name, date of birth, address, country of residence, TIN and AML/CFT risk rating, if applicable.

ii. The date the account was opened.

iii. The average daily balance (during the review period) and balance of the account as of the examination date.

The financial institution should provide a list of its internal codes necessary to fully identify the account type, AML/CFT risk rating, country, transaction type, branch number, teller number and any other codes found on the electronic reports. The list should be sorted to identify those accounts that do not contain sufficient information.

4. Testing of Currency-Shipment Logs for Unusual Activity

Review all or a sample of the institution's currency-shipment logs for significant aberrations or unusual patterns of currency-shipment activity. Examiners may also consider reviewing the **Summary of Deposits (SOD) data** for unusual trends in branch deposit growth.

Assess whether shipment levels and the frequency of shipments appear commensurate with the expected institution and its branch activity levels. This assessment should include transactions to and from the central currency vault and the branches. Unusual activity warranting further research may include significant exchanges of small-denomination bills for large-denomination bills and significant requests for large bills.

5. Non-resident Aliens and Foreign Individuals

An effective method to identify and review the level of the financial institution's non-resident aliens (NRA), foreign individuals and offshore corporations is by obtaining MIS reports that provide no TINs or account-holders with individual taxpayer identification numbers (ITIN). **The report should capture:**

i. Customer's full name, date of birth, address, country of residence and TIN.

ii. Date the account was opened.

iii. Average daily balance and balance of the account as of the examination date.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. The financial institution should provide a list of its internal codes necessary to fully identify the information on the spreadsheet. This information can be used to assess whether the amount of NRAs and foreign individuals provide heightened risk to the financial institution by determining the aggregate average daily balance, the account types and countries in which the financial institution is exposed.

6. Funds Flow Reports

Examiners can review this information to identify customers with a high velocity of funds flow and those with unusual activity. A velocity of funds report reflects the total debits and credits flowing through a particular account over a specific period (e.g., 30 days). **The electronic reports should capture:**

i. Name of customer.

ii. Account number.

iii. Date of transaction.

iv. Dollar amount of payments (debits).

v. Dollar amount of receipts (credits).

vi. Average balance of the account.

vii. Type of account.

This data should be prepared in an electronic spreadsheet or database format to facilitate the sorting of the data. This report can be used to identify customer accounts with substantial funds flow relative to other accounts.

APPENDIX M

AML/CFT Record Retention Requirements

This appendix is provided as a summary listing. For comprehensive and current AML/CFT record retention requirements, refer to MLPA 2004 and CBN AML/CFT Regulation. These record retention requirements are independent of and in addition to record retention requirements under any other law.

Five-Year Retention for Records as Specified Below

The AML/CFT regime establishes record-keeping requirements related to all types of records including customer accounts (e.g., loan, deposit or trust), AML/CFT filing requirements and records that document a financial institution's compliance with the AML/CFT regulations. In general, the AML/CFT requires that a financial institution maintains most records for at least five years. These records can be maintained in many forms including original, microfilm, electronic, copy or a reproduction. A financial institution is not required to keep a separate system of records for each of the AML/CFT requirements. However, a financial institution must maintain all records in a way that makes them accessible in a reasonable period of time.

The records related to the transactions discussed below must be retained by a financial institution for five years. However, as noted below, **the records related to the identity of a financial institution customer must be maintained for five years after the account (e.g., loan, deposit or trust) is closed. Additionally, on a case-by-case basis, a financial institution may be ordered or requested to maintain some of these records for longer periods.**

1. International Transactions in Excess of N5 million

Financial institutions are required to maintain records of requests made or instructions received or given regarding transfers of currency or other monetary instruments, cheques, funds, investment securities or credit greater than N5 million to or from any person, account or place outside Nigeria.

2. Signature Cards

Financial institutions are required to keep records of each grant of signature authority over each deposit account.

3. Account Statements

Financial institutions are also required to keep statements, ledger cards or other records on each deposit account showing each transaction in or with respect to that account.

4. **Cheques**

Each cheque, draft or money order drawn on the financial institution or issued and payable by it must be kept.

5. Deposits

Each deposit slip or credit ticket reflecting a transaction, record for direct deposit or other funds transfer deposit transactions are required to be kept. The slip or ticket must record the amount of any currency involved.

6. Records to Reconstruct Demand Deposit Accounts

To be kept are the records prepared or received by the financial institution in the ordinary course of business which would be needed to reconstruct a transaction

account and to trace a cheque deposited in a demand deposit account through its domestic processing system or to supply a description of a deposited cheuque.

7. Certificates of Deposit Purchased or Presented

This record which contained the following will be kept:

i. Name of customer (purchaser or presenter).

ii. Address of customer.

iii. Taxpayer identification number (TIN) of customer.

iv. Description of the certificate of deposit.

v. Notation of the method of payment if purchased.

vi. Date of transaction.

8. Purchase of Monetary Instruments

A financial institution must maintain records of each of its cheques/draft, cashier's cheque, money order or traveller's cheque.

If the purchaser has a deposit account with the financial institution, this record shall contain:

i. Name of purchaser.
ii. Date of purchase
iii. Type(s) of instrument purchased.
iv. Amount of each of the instrument(s) purchased.
v. Serial number(s) of the instrument(s) purchased.

If the purchaser does not have a deposit account with the bank, this record shall contain:
i. Name of purchaser.
ii. Address of purchasers.
iii. Social security number of purchaser or alien identification number.
iv. Date of birth of purchaser.
v. Date of purchase
vi. Type(s) of instrument purchased.
vii. Amount of each of the instrument(s) purchased.
viii. Serial number(s) of the instrument(s) purchased.
ix. Description of document or method used to verify the name and address of the purchaser (e.g., state of issuance and number driver's licence).

Funds Transfers

A financial institution's AML/CFT record-keeping requirements with respect to funds transfer vary based upon its role with respect to the funds transfer.

Financial institution acting as an originator

For each payment order that the financial institution accepts as the originator, it must obtain and retain records of the following information:

i. Name and address of originator.

ii. Amount of the payment order.

iii. Execution date of the payment order.

iv. Any payment instruction received from the originator with the payment order.

v. Identity of the beneficiary's financial institution.

vi. As many of the following items as are received with the payment order:

a. Name and address of the beneficiary

b. Account number of the beneficiary.

c. Any other specific identifier of the beneficiary.

d. For each payment order that a financial institution accepts for an **originator that is not its established customer,** it (in addition to the information listed above) must obtain appropriate extra information as may be required.

Bank acting as an intermediary or a beneficiary's bank

For each payment order that a bank accepts as an intermediary bank or a beneficiary's financial institution, it must retain a record of the payment order.

For each payment order that a financial institution accepts for a beneficiary that is **not its established customer,** the financial institution must also obtain additional information as required.

9. Taxpayer Identification Number (TIN)

The institution is required to keep the record of the TIN of any customer opening an account.

In cases of joint accounts, information on a person with a financial interest must be maintained.

If the person is a non-resident alien (NRA), the record of the passport number or description of some other government documents used to verify identity must be obtained and kept. This information must be recorded within 30 days of the date the transaction occurs.

In the event a financial institution is unable to secure the information, it must maintain a list containing the names, addresses and account numbers of those customers for whom it has not been able to secure the information.

10. Exceptions in respect of TIN

A financial institution does not need to maintain TIN for accounts or transactions with the following:

i. Agencies and instrumentalities of federal, state, local or foreign governments.

ii. Judges, public officials or clerks of courts of record as custodians of funds in controversy or under the control of the court.

iii. Certain aliens.

iv. Certain tax exempt organizations and units of tax-exempt organizations.

v. A person under 18 years of age with respect to an account opened as a part of a school thrift savings program.

11. Suspicious Transaction Report and Supporting Documentation

A financial institution must maintain a record of any STR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing.

12. Currency Transaction Report

A financial institution must maintain a record of all Currency Transaction Reports (CTR) for a period of five years from the date of filing.

Customer Identification Program

A financial institution must maintain a record of all information it obtains under its procedures for implementing its CIP. **At a minimum, these records must include the following:**

i. All identifying information about a customer (e.g., name, date of birth, address and TIN).

ii. A description of the document that the bank/other financial institution relied upon to identity of the customer.

iii. A description of the non-documentary methods and results of any measures the financial institution took to verify the identity of the customer.

iv. A description of the financial institution's resolution of any substantive discrepancy discovered when verifying the identifying information obtained.

A financial institution must retain the identifying information about a customer for a period of five years after the date the account is closed or in the case of credit card accounts, five years after the account becomes closed or dormant.

A financial institution must retain the information relied on, methods used to verify identity and resolution of discrepancies for a period of five years after the record is made.

These AML/CFT record-keeping requirements are independent of and in addition to requirements to file and retain reports imposed by other laws.

APPENDIX N

Acronyms

Acronym	Full name
ACH	Automated Clearing House
AML	Anti-money Laundering
ATM	Automated Teller Machine
APT	Asset Protection Trust
BCBS	Basel Committee on Banking Supervision
BHC	Bank Holding Company
BIS	Bank for International Settlements
CDD	Customer Due Diligence
CHIPS	Clearing House Interbank Payments System
CIF	Customer Information File
CIP	Customer Identification Program
CTR	Currency Transaction Report
DCN	Document Control Number
E-banking	Electronic Banking
E-cash	Electronic Cash
EDD	Enhanced Due Diligence
EFT	Electronic Funds Transfer
EIN	Employer Identification Number
EPN	Electronic Payments Network
FAQ	Frequently Asked Question
FATF	Financial Action Task Force
FIL	Financial Institution Letter

FinCEN	Financial Crimes Enforcement Network
FIRS	Federal Internal Revenue Service
HIFCA	High Intensity Financial Crime Area
IAIS	International Association of Insurance Supervisors
IAT	International Automated Clearing House Transaction
IBC	International Business Corporation
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
IOLTA	Interest on Lawyers' Trust Account
IP	Internet protocol
IRA	Individual Retirement Account
ISO	Independent Sales Organization
ITIN	Individual Taxpayer Identification Number
IVTS	Informal Value Transfer System
KYC	Know Your Customer
MIS	Management Information Systems
MLPA	Money Laundering (Prohibition) Act of 2004
NACHA	Nigerian Electronic Payments Association
NBFI	Non-bank Financial Institutions
NCCT	Non-Cooperative Countries and Territories
NGO	Non-Governmental Organization
NRA	Non-Resident Alien
NSF	Non-sufficient Funds
PEP	Politically Exposed Person

PIC	Private Investment Company
POS	Point-of-Sale
PTA	Payable Through Account
PUPID	Payable Upon Proper Identification
RA	Regulatory Alerts
RCC	Remotely Created Cheque
RDC	Remote Deposit Capture
RDFI	Receiving Depository Financial Institution
STR	Suspicious Transaction Report
SEC	Securities and Exchange Commission
SOD	Summary of Deposits
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIN	Taxpayer Identification Number
TPSP	Third-Party Service Provider
UBPR	Uniform Bank Performance Report
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Act Tools Required to Intercept and Obstruct Terrorism Act of 2001
Web CBRS	Web Currency and Banking Retrieval System

APPENDIX O

Enforcement Guidance

Inter-Agency Statement on Enforcement of Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Requirements

This interagency statement sets forth the policy on the circumstances in which a Regulatory Agency will issue a cease and desist order to address non-compliance with certain Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)

requirements, particularly in light of the specific AML/CFT compliance provisions in the MLPA 2004 and CBN AML/CFT Regulation 2009.

1. AML/CFT Compliance Program Requirement

Under the provisions of the MLPA 2004 and CBN AML/CFT Regulation 2009, it is expected that each of the regulatory agencies should prescribe regulations requiring each regulated institution under its regulatory purview to establish and maintain procedures reasonably designed to assure and monitor the institution's compliance with the requirements of its **AML/CFT Compliance Program.** It also requires that each agency's examinations of the regulated financial institution review the AML/CFT Compliance Program and identify and observe in its examination reports any problem with the AML/CFT Compliance Program. Finally, if the regulated financial institution has failed to establish and maintain a AML/CFT Compliance Program or has failed to correct any problem with the AML/CFT Compliance Program previously reported to the institution by the appropriate agency, the latter shall issue sanctions including a cease and desist order against the institution accordingly.

Specifically, each regulated financial institution's AML/CFT Compliance Program must have, at a minimum, the following five (5) elements:

i. A system of internal controls which ensure on-going compliance with the MLPA 2004 and CBN AML/CFT Regulation 2009;

ii. Independent testing for compliance with MLPA 2004 and CBN AML/CFT Regulation 2009;

iii. A designated individual or individuals responsible for coordinating and monitoring AML/CFT compliance; and

iv. Training for appropriate personnel.

v. Customer Identification Program (CIP) with risk-based procedures that enable the institution to form a reasonable belief that it knows the true identity of its customers.

2. Communication of Supervisory Concerns about AML/CFT Compliance Programs

When CBN identifies supervisory concerns relating to a financial institution's AML/CFT Compliance Program in the course of an examination or otherwise, it is required to communicate those concerns by various means. The particular method of communication used typically depends on the seriousness of the concerns. **These methods include:**

i. Informal discussions by Examiners with an institution's management during the examination process;

ii. Formal discussions by Examiners with staff & management as part of or following the examination process and at the end of the examination;

iii. Supervisory letters and written communications from Examiners to the institution's management;
iv. A finding contained in the AML/CFT examination reports or in other formal communications from the CBN to the institution's board of directors indicating deficiencies or weaknesses in the AML/CFT Compliance Program; or

v. A finding contained in the AML/CFT examination reports or in other formal communications from the CBN to an institution's board of directors of a violation of the regulatory requirement to implement and maintain a reasonably designed AML/CFT Compliance Program.

For a finding/observation to be a "problem" with the AML/CFT Compliance Program that results in issuance of cease and desist order (if not corrected by the institution), the **deficiencies in the AML/CFT Compliance Program must be identified in an AML/CFT examination report** or other written document to an institution's board of directors or senior management as matters that must be corrected. However, other issues or suggestions for improvement may be communicated through other means.

3. Enforcement Actions for AML/CFT Compliance Program Failures

In accordance with the provisions of MLPA 2004 and CBN AML/CFT Regulation 2009 the CBN will issue a cease and desist order against a financial institution for non-compliance with AML/CFT Compliance Program requirements in the following circumstances, based on a careful review of all the relevant facts and circumstances:

i. **Failure to establish and maintain a reasonably designed AML/CFT Compliance Program**

The CBN will issue a cease and desist order based on a violation of the MLPA 2004 and CBN AML/CFT Regulation 2009 requirements to establish and maintain a reasonably designed AML/CFT Program where the institution:

a. Fails to have a written AML/CFT Compliance Program, including a CIP that adequately covers the required program elements (i. e., internal controls, independent testing, designated compliance personnel and training); or

b. Fails to implement a AML/CFT Compliance Program that adequately covers the required Program elements (institution-issued policy statements alone are not sufficient; the program as implemented must be consistent with the financial institution's written policies, procedures and processes); or

c. Has defects in its AML/CFT Compliance Program in one or more program elements that indicate that either the written Compliance Program or its implementation is not effective. **For example, where the deficiencies are coupled with other aggravating factors such as** (i) highly suspicious

activity creating a significant potential for unreported money laundering or terrorist financing, (ii) patterns of structuring to evade reporting requirements, (iii) significant insider complicity or (iv) systemic failures to file CTRs, STRs or other required AML/CFT reports.

d. For example, an institution that has procedures to provide AML/CFT training to appropriate personnel, independent testing and a designated AML/CFT compliance officer, would nonetheless be subject to a cease and desist order if its system of internal controls (such as customer due diligence, procedures for monitoring suspicious activity or an appropriate risk assessment) fails with respect to a higher risk area or to multiple lines of business that significantly impact the institution's overall AML/CFT compliance.

Similarly, a cease and desist order would be warranted if, for example, an institution has deficiencies in the required independent testing element of the Program and those deficiencies are coupled with evidence of highly suspicious activity creating a significant potential for unreported money laundering or terrorist financing in the institution.

Other types of deficiencies in an institution's AML/CFT Compliance Program or in implementation of one or more of the required Program elements will not necessarily result in the issuance of a cease and desist order, unless the deficiencies are so severe as to render the Program ineffective when viewed as a whole. For example, an institution that has deficiencies in its procedures for providing AML/CFT training to appropriate personnel but has effective controls, independent testing and a designated AML/CFT compliance officer, may ordinarily be subject to Examiner criticism and supervisory action other than the issuance of a cease and desist order (unless the training program deficiencies viewed in the light of all relevant circumstances) are so severe as to result in a finding that the financial institution's Program, taken as a whole, is not effective.

In determining whether a financial institution has failed to implement an AML/CFT Compliance Program, the CBN is required to also consider the application of the institution's Program across its business lines and activities. In the case of institutions with multiple lines of business, deficiencies affecting only some lines of business or activities would need to be evaluated to determine if the deficiencies are so severe or significant in scope as to result in a conclusion that the institution has not implemented an effective overall program.

ii. Failure to correct a previously reported problem with the AML/CFT Compliance Program

A history of deficiencies in an institution's AML/CFT Compliance Program in a variety of different areas or in the same general areas can result in a cease and desist order on that basis. The CBN is required (in accordance with the provisions of the MLPA 2004 and CBN AML/CFT Regulation 2009 and based on a careful review of the relevant facts and circumstances) to issue a cease and desist order whenever an institution fails to correct a problem with AML/CFT compliance identified during the supervisory process.

In order to be considered a deficiency as a "problem", it would ordinarily involve a serious defect in one or more of the required components of the institution's AML/CFT Compliance Program or its implementation thereof that a examination report or other written supervisory communication identifies as requiring communication to the institution's board of directors or senior management as a matter that must be corrected. For example, failure to take any action in response to an express criticism in an examination report regarding a failure to appoint a qualified CCO could be viewed as an un-corrected problem that would result in a cease and desist order.

The CBN will ordinarily not issue a cease and desist order for failure to correct an AML/CFT Compliance Program problem unless the deficiencies subsequently observed by the Bank Examiners are substantially the same as those previously reported to the institution. For example, if the CBN notes in one examination report that an institution's training program was inadequate because it was out of date (for instance, if it did not reflect changes in the law) and at the next examination, the training program is adequately updated but flaws are discovered in the internal controls contained in the AML/CFT Program, the CBN will determine not to issue a cease and desist order for failure to correct previously reported problems and will consider the full range of potential supervisory responses.

Similarly, if an institution is cited in an examination report described above for failure to designate a qualified AML/CFT CCO and the institution by the next examination has appointed an otherwise qualified person to assume that responsibility, but the Examiners recommend additional training for the person, the CBN shall determine not to issue a cease and desist order based solely on that deficiency. Statements in a written examination report or other supervisory communication identifying less serious issues or suggesting ways for improvement which the examination report does not identify as requiring communication to the board of directors or senior management as matters that must be corrected, would not be considered problems.

The CBN recognizes that certain types of problems with an institution's AML/CFT Compliance Program may not be fully correctable before the next examination, for example, remedial action involving adoption or conversion of computer systems. In these types of situations, a cease and desist order is not required provided the CBN determines that the institution has made acceptable & substantial progress toward correcting the problem at the time of the examination immediately following the examination where the problem was first identified and reported to the institution.

iii. Other enforcement actions for AML/CFT Compliance Program deficiencies

In addition to the situations where the CBN will issue a cease and desist order for a violation of the AML/CFT Compliance Program regulation or for failure to correct a previously reported Program problem, the CBN shall also issue a cease and desist order or enter into a formal written agreement or take informal enforcement action against an institution for other types of AML/CFT Program concerns. In these situations, depending upon the particular facts involved, the CBN may pursue enforcement actions based on unsafe and unsound practices or violations of law, including the MLPA 2004 and CBN AML/CFT Regulation 2009. The form of the enforcement action in a particular case shall

depend on the severity of the non-compliance, weaknesses or deficiencies, the capability and cooperation of the institution's management and the CBN's confidence that the institution will take appropriate and timely corrective action.

4. AML/CFT Reporting and Record-keeping Requirements

i. Suspicious Transaction reporting requirements

Under provisions of the MLPA 2004 and CBN AML/CFT Regulation 2009 financial institutions are required to file a STR when they detect certain known or suspected criminal violations or suspicious transactions. Suspicious transaction reporting forms the cornerstone of the AML/CFT reporting system and is critical to Nigeria's ability to utilize financial information to combat money laundering, terrorist financing and other financial crimes. **The regulations require financial institutions to file STRs with respect to the following general types of activity:**

a. Known or suspected criminal violations involving insider activity in any amount;

b. Known or suspected criminal violations aggregating to any amount when a suspect can be identified;

c. Known or suspected criminal violations aggregating to any amount regardless of potential suspects; or

d. Suspicious transactions of any amount that involve potential anti-money laundering or terrorism financing violations.

The STR must be filed within 7 days of detecting facts that may constitute a basis for filing a STR (or within 30 days if there is no subject).

The CBN shall cite a violation of the STR regulations and will take appropriate supervisory action, if the institution's failure to file a STR (or STRs) evidences a systemic breakdown in its policies, procedures or processes to identify and research suspicious activity, involves a pattern or practice of non-compliance with the filing requirement or represents a significant or egregious situation.

ii. Other AML/CFT reporting and record-keeping requirements

Financial institutions are also subject to other AML/CFT reporting and record-keeping requirements set forth in the MLPA 2004 and CBN AML/CFT Regulation 2009. These requirements reviewed in detail in the AML/CFT Examination Manual include requirements applicable to cash and monetary instrument transactions and funds transfers, CTR filing, exemption rules, due diligence, certification and other requirements for foreign correspondent and private banking accounts.

iii. Enforcement actions for non-AML/CFT Program requirements

In appropriate circumstances, the CBN shall take formal or informal enforcement actions to address violations of AML/CFT requirements other than the AML/CFT

Compliance Program requirements. These other requirements include the STR, CTR and PEP returns regulatory obligations described above.

APPENDIX P

Key Suspicious Transaction Monitoring Components

Identification of Unusual Activity (Employee identification, law enforcement inquiries, other referrals, transaction, and surveillance monitoring system	Alert Management	STR Decision Making	STR Completion and Filing