

BANK EXAMINERS' MANUAL FOR AML/CFT RBS EXAMINATION

Contents

1. EXAMINATION PROCEDURES ON SCOPING AND PLANNING.....	1
Objective.....	1
2. EXAMINATION PROCEDURES OF AML/CFT COMPLIANCE PROGRAM.....	3
Objective.....	3
3. OVERVIEW OF AML/CFT COMPLIANCE PROGRAM.....	6
Objective.....	6
Risk assessment in AML/CFT compliance program.....	7
Internal controls.....	7
Independent testing.....	8
Chief compliance officer.....	9
Training.....	10
Transaction testing.....	10
Independent testing.....	11
Preliminary evaluation.....	11
4. EXAMINATION PROCEDURES OF HOW TO DEVELOP CONCLUSIONS AND FINALIZE AML/CFT EXAMINATION.....	11
Objective.....	11
All relevant determinations should be documented and explained.....	12
Discuss findings with examiner in charge and identify necessary action.....	13
Preparing the AML/CFT comments for examination report.....	13

Items for examiners to discuss.....	14
5. EXAMINATION PROCEDURES IN RESPECT OF CUSTOMER DUE DILIGENCE....	15
Objective.....	15
Transaction testing.....	15
6. EXAMINATION PROCEDURES OF SUSPICIOUS TRANSACTION REPORTING...16	
Objective.....	16
Identification of unusual activity.....	16
Transaction (manual transaction) monitoring.....	17
Surveillance (automated account) monitoring.....	17
Managing alerts.....	17
STR decision making.....	18
STR completion and filing.....	18
Transaction testing.....	18
7. EXAMINATION PROCEDURES ON INFORMATION SHARING.....20	
Objective.....	20
Information sharing between lea and financial institutions.....	20
Voluntary information sharing.....	20
Transaction testing.....	22
9. EXAMINATION PROCEDURES OF PURCHASE AND SALE OF MONETARY INSTRUMENTS & RECORD-KEEPING.....23	
Objective.....	23
Transaction testing.....	23
10. OBJECTIVE OF EXAMINATION PROCEDURES OF FUNDS TRANSFERS RECORD- KEEPING.....23	
Transaction testing.....	24
11. EXAMINATION PROCEDURES OF FOREIGN CORRESPONDENT ACCOUNT RECORD- KEEPING AND DUE DILIGENCE.....24	

Objective.....	24
Foreign shell bank prohibition and foreign correspondent account record keeping.....	24
Special due diligence program for foreign correspondent accounts.....	25
Transaction testing.....	27
Foreign shell bank prohibition and foreign correspondent account record Keeping.....	27
12. EXAMINATION PROCEDURES OF PRIVATE BANKING DUE DILIGENCE PROGRAM (NIGERIAN/NON-NIGERIA PERSONS).....	29
Objective.....	29
Transaction testing.....	30
13. EXAMINATION PROCEDURES OF SPECIAL MEASURES.....	31
Objective.....	31
Transaction testing.....	31
14. EXAMINATION PROCEDURES FOREIGN FINANCIAL INSTITUTION AND FINANCIAL ACCOUNTS REPORTING.....	32
Objective.....	32
Transaction testing.....	32
15. EXAMINATION PROCEDURES OF INTERNATIONAL TRANSPORTATION OF CURRENCY OR MONETARY INSTRUMENTS REPORTING.....	32
Objective.....	32
Transaction testing.....	33
16. EXAMINATION PROCEDURES FOR AML/CFT COMPLIANCE PROGRAM STRUCTURES.....	33
Objective.....	33
17. EXAMINATION PROCEDURES OF PARALLEL BANKING.....	35
Objective.....	35

Transaction testing.....36

18. EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PRODUCTS AND SERVICES.....36

19. EXAMINATION PROCEDURES OF CORRESPONDENT ACCOUNTS (DOMESTIC).....	36
Objective.....	36
Transaction testing.....	37
20. EXAMINATION PROCEDURES OF CORRESPONDENT ACCOUNTS (FOREIGN).....	37
Objective.....	37
Transaction testing.....	38
21. EXAMINATION PROCEDURES OF BULK SHIPMENTS OF CURRENCY.....	39
Objective.....	39
Transaction testing.....	40
22. EXAMINATION PROCEDURES OF FOREIGN CURRENCY DENOMINATED DRAFTS.....	41
Objective.....	41
Transaction testing.....	41
23. EXAMINATION PROCEDURES OF PAYABLE THROUGH ACCOUNTS.....	42
Objective.....	42
Transaction testing.....	44
24. EXAMINATION PROCEDURES OF POUCH ACTIVITIES.....	45
Objective.....	45
Transaction testing.....	45
25. EXAMINATION PROCEDURES OF ELECTRONIC BANKING.....	46
Objective.....	46
Transaction testing.....	46
26. EXAMINATION PROCEDURES OF FUNDS TRANSFERS.....	47
Objective.....	47
Review of financial institution’s procedures for cross border funds transfer.....	48
Transaction testing.....	48

27. EXAMINATION PROCEDURES OF AUTOMATED CLEARING HOUSE TRANSACTIONS.....	49
Objective.....	49
Transaction testing.....	50
28. EXAMINATION PROCEDURES OF ELECTRONIC CASH.....	50
Objective.....	50
Transaction testing.....	50
29. EXAMINATION PROCEDURES OF THIRD-PARTY PAYMENT PROCESSORS.....	51
Objective.....	51
Transaction testing.....	52
30. EXAMINATION PROCEDURES OF PURCHASE AND SALE OF MONETARY INSTRUMENTS..	52
Objective.....	52
Transaction testing.....	53
31. EXAMINATION PROCEDURES OF BROKERED DEPOSITS.....	53
Objective.....	53
Transaction testing.....	54
32. EXAMINATION PROCEDURES OF NON-DEPOSIT INVESTMENT PRODUCTS.....	54
Objective.....	54
Transaction testing.....	55
33. EXAMINATION PROCEDURES OF INSURANCE PRODUCTS.....	56
Objective.....	56
Transaction testing.....	56
34. EXAMINATION PROCEDURES OF CONCENTRATION ACCOUNTS.....	57
Objective.....	57
Transaction testing.....	57

35. EXAMINATION PROCEDURES OF LENDING ACTIVITIES.....	58
Objective.....	58
Transaction testing.....	58
36. EXAMINATION PROCEDURES OF TRADE FINANCE ACTIVITIES.....	58
Objective.....	58
Transaction testing.....	59
37. EXAMINATION PROCEDURES OF PRIVATE BANKING ACTIVITIES.....	59
Objective.....	59
Transaction testing.....	60
38. EXAMINATION PROCEDURES OF TRUST AND ASSET MANAGEMENT SERVICES.....	61
Objective.....	61
Transaction testing.....	61
39. EXAMINATION PROCEDURES OF NON-RESIDENT ALIENS AND FOREIGN INDIVIDUALS.....	62
Objective.....	62
Transaction testing.....	63
40. EXAMINATION PROCEDURES OF POLITICALLY EXPOSED PERSONS.....	63
Objective.....	63
Transaction testing.....	64
41. EXAMINATION PROCEDURES OF EMBASSY AND FOREIGN CONSULATE ACCOUNTS..	64
Objective.....	64
Transaction testing.....	65

42. EXAMINATION PROCEDURES OF DESIGNATED NON-FINANCIAL INSTITUTIONS....	65
Objective.....	65
Money services businesses.....	66
Transaction testing.....	66
43. EXAMINATION PROCEDURES OF PROFESSIONAL SERVICE PROVIDERS.....	66
Objective.....	66
Transaction testing.....	67
44. EXAMINATION PROCEDURES OF NONGOVERNMENTAL ORGANIZATIONS AND CHARITIES.....	67
Objective.....	67
Transaction testing.....	68
45. EXAMINATION PROCEDURES OF BUSINESS ENTITIES (DOMESTIC AND FOREIGN)..	68
Objective.....	68
Transaction testing.....	69
46. EXAMINATION PROCEDURES OF CASH-INTENSIVE BUSINESSES.....	70
Objective.....	70
Transaction testing.....	70

AML/CFT RBS MANUAL FOR BANK EXAMINERS – EXAM PROCEDURES

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:

1. **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:**

- i. AML/CFT Compliance Program;
- ii. ML/FT Risk Assessment;
- iii. Suspicious transaction monitoring and reporting systems; and
- iv. 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.

2. **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.
3. **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.

4. **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:
 - i. Volume of activity and whether it is commensurate with the customer's occupation or type of business;
 - ii. Number and Naira volume of transactions involving higher-risk customers;
 - iii. 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
 - iv. 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.
5. **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.
6. **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:

- i. **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.
- ii. **Review the institution's independent testing of its AML/CFT Compliance Program.**
 - iii. **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.
 - iv. **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)).
7. **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.

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.

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.

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 Regulatory requirements.

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

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 unusual 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 unusual 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). 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 unusual transaction.
- iv. Has reviewed whether suspicious transaction reporting systems include the research and referral of unusual 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".

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.

All relevant determinations should be documented and explained.

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.

As applicable, the Examiner should prepare to discuss on the following items:

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.

EXAMINATION PROCEDURES IN RESPECT OF CUSTOMER DUE DILIGENCE

Objective

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.

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:
 - i. STRs contain accurate information.
 - ii. STR narratives are complete and thorough, and clearly explain why the activity is suspicious.
 - iii. 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.

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.

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.

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.

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 institution has taken reasonable steps to ensure that any correspondent accounts maintained 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:**
 - a. 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.
 - b. Monitor transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity.
 - c. 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.

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 **that satisfies all three of the following criteria:**
 - i. Requires a minimum aggregate deposit of funds or other assets of not less than USA **\$50,000 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 \$50,000 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.

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.

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.

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.

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.

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.

The Examiner also should assess how effectively the financial institution or entire organization monitors AML/CFT compliance throughout the organization, including how well the consolidated and non-consolidated AML/CFT Compliance Program capture relevant data from subsidiaries.

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.

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.

EXPANDED EXAMINATION OVERVIEW AND PROCEDURES FOR PRODUCTS AND SERVICES

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.

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.

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.

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.

EXAMINATION PROCEDURES 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.

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. Required 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.

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.

EXAMINATION PROCEDURES ON 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.

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.

6. 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

7. 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.

8. 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.

9. 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).

10 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.

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.

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.

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.

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.

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.

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 **Examiners 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. 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.

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.

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.

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.

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.

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.

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.
9. Update the section Notes, Risk Assessment Summary and Knowledge of Business of the financial institution.

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.

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.

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.

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 DNFI's and for financial institutions with significant relationships with DNFI's, 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.

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.

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.

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.

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.