



Central Bank of Nigeria

Banking Supervision Department

P.M.B. 12194

Tinubu Square.

Lagos.

Email: bsd@cbn.gov.ng

Website: www.cbn.gov.ng

Tel:.....

BSD/DIR/CON/AML/018/033

May 20, 2025

Letter to All Financial Institutions

EXPOSURE OF DRAFT BASELINE STANDARDS FOR AUTOMATED ANTI-MONEY LAUNDERING (AML) SOLUTIONS:

REQUEST FOR COMMENTS

The Central Bank of Nigeria (CBN) is committed to ensuring the integrity and stability of the Nigerian banking system. In recognition of the high level of digitalization within the financial system and rapid emergence of innovative products, the CBN has developed a draft document titled "Baseline Standards for Automated Anti-Money Laundering (AML) Solutions". The Standard is aimed at promoting operational efficiency and regulatory compliance to AML/CFT/CPF requirements by financial institutions in Nigeria. This standard is informed by a comprehensive assessment of existing solutions within the industry. It aligns with global best practices and international regulatory frameworks, including the recommendations of the Financial Action Task Force (FATF).

The objectives of these standards include:

- Strengthening the AML/CFT/CPF capabilities of financial institutions through technology-driven approaches;
- Encouraging the adoption of emerging technologies to enhance the detection and reporting of suspicious transactions in real time;
- Reducing operational inefficiencies associated with manual AML processes;
- Supporting compliance with evolving domestic and international regulatory expectations.

The CBN hereby exposes the draft **Baseline Standards for Automated AML Solutions** to all stakeholders and invites comments and suggestions to enrich the final version.

All comments should be submitted to the Director of Banking Supervision via the following email addresses on or before June 13, 2025:

- wajakaiye@cbn.gov.ng
- ammohammed@cbn.gov.ng
- fkdaodu@cbn.gov.ng

The draft document is available for download on the CBN's official website:
www.cbn.gov.ng

We look forward to receiving your valuable feedback.

Yours faithfully,

A handwritten signature in blue ink, appearing to be 'O. Akinwunmi', written over a faint horizontal line.

Olubukola A. Akinwunmi, *Ph.D.*
Director of Banking Supervision



CENTRAL BANK OF NIGERIA

BASELINE STANDARDS FOR AUTOMATED ANTI-MONEY LAUNDERING (AML) SOLUTIONS

Table of Contents

Preamble.....	3
1. INTRODUCTION.....	3
2. OBJECTIVES.....	3
3. SCOPE	4
4. BASELINE STANDARDS	5
4.1 AML Solutions	5
4.2 User Interface & Customization.....	5
4.3 System Integration & Scalability	5
4.4 Sanction list & PEP Screening	6
4.5 Transaction Monitoring & Risk-Based Analysis.....	7
4.6 Customer Due Diligence (CDD), Know Your Customer (KYC) & Know Your Customer's Business (KYB)	7
4.8 Regulatory Reporting	8
4.9 Case Management.....	9
4.10 Security & Data Protection	9
4.11 Enforcement & Compliance Monitoring.....	9
5. OTHER REQUIREMENTS	10
6. IMPLEMENTATION AND COMPLIANCE.....	10

PREAMBLE

In pursuant of the powers conferred on the Central Bank of Nigeria (CBN) by Section 2 (d) of the Central Bank of Nigeria Act, 2007; to promote a sound financial system in Nigeria; the CBN hereby issues these Baseline Standards for Automated Anti-Money Laundering (AML) Solutions.

The standards aim to ensure uniformity, efficiency, and regulatory compliance in AML solutions across financial institutions in Nigeria.

1. INTRODUCTION

The fight against money laundering and terrorist financing is a critical priority for financial systems worldwide. In Nigeria, the Central Bank of Nigeria (CBN) plays a pivotal role in ensuring the stability and integrity of the financial system. As financial transactions become increasingly digitized, the need for robust, automated AML solutions has never been more urgent. These solutions leverage advanced technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics to detect, prevent, and report suspicious activities in real-time.

The **Baseline Standards for Automated AML Solutions** is hereby issued to ensure uniformity, efficiency, and compliance across financial institutions in Nigeria. These standards are based on findings from an assessment of AML solutions in the industry. The standards also incorporate global best practices and align with international regulatory frameworks, such as the Financial Action Task Force (FATF) recommendations.

The adoption of these standards will enable financial institutions to enhance their AML/CFT/CPF capabilities, reduce operational inefficiencies, and comply with evolving regulatory requirements. By implementing these standards, the Nigerian financial sector will be better equipped to combat money laundering and terrorist financing, thereby safeguarding the integrity of the financial system.

2. OBJECTIVES

The primary objectives of these baseline standards are to:

1. **Ensure Effective Implementation of Automated AML Solutions:** Provide a framework for the deployment and operation of automated AML solutions that meet regulatory requirements and industry best practices.
2. **Promote Interoperability and Integration:** Facilitate seamless integration of AML systems with other financial systems to ensure efficient data sharing and compliance reporting.

3. **Enhance Detection Accuracy and Reduce False Positives:** Leverage advanced technologies such as AI and ML to improve the accuracy of transaction monitoring and reduce the rate of false positives.
4. **Facilitate Compliance with Local and International Regulations:** Ensure that AML solutions comply with local regulations, such as the CBN AML/CFT/CPF Guidelines, and international standards, such as the FATF recommendations.
5. **Provide a Framework for Continuous Improvement:** Establish mechanisms for regular updates, performance validation, and adaptation to emerging risks.

3. SCOPE

These baseline standards apply to all financial institutions operating in Nigeria, including:

- Deposit Money Banks.
- Microfinance Banks.
- Primary Mortgage Banks.
- Digital Payment Service Providers.
- Other financial institutions subject to AML/CFT/CPF regulations.

The standards cover the following key areas:

1. **System Functionality and Integration:** Requirements for the functionality and integration of AML solutions with other financial systems.
2. **Transaction Monitoring and Risk-Based Analysis:** Guidelines for transaction monitoring, risk scoring, and the use of AI/ML for anomaly detection.
3. **Customer Due Diligence (CDD) and Know Your Customer (KYC):** Standards for automating CDD and KYC processes, including risk profiling and enhanced due diligence (EDD).
4. **Sanctions Screening and Watchlist Compliance:** Requirements for integrating global and local watchlists and ensuring real-time updates.
5. **Regulatory Reporting and Case Management:** Guidelines for automating compliance reporting and managing suspicious activity cases.
6. **Data Security and Protection:** Standards for ensuring the security and protection of sensitive customer data.
7. **Vendor Management and System Scalability:** Requirements for managing vendors and ensuring the scalability of AML solutions.
8. **Risk assessment:** Guidelines for dynamic risk profiling, AI/ML-driven scoring system to classify customers and transactions.

4. BASELINE STANDARDS

4.1 AML Solutions

The AML solutions shall include

- i. Risk Profiling,
- ii. Politically Exposed Person (PEP) and other high-risk profiling
- iii. Risk Assessment
- iv. Identification and Verification
- v. Sanction screening
- vi. Transaction Monitoring
- vii. Regulatory Reporting

4.2 User Interface & Customization

Financial institutions shall:

- i. Deploy robust automated AML solutions that is user-friendly, customized to its peculiarities, and compliant with all applicable AML/CFT/CPF laws and regulations. The solution may be developed in-house or procured off-the-shelf.
- ii. Configure the AML system to allow for rule updates and scenario modifications with minimal vendor dependency.
- iii. The system should include a centralized dashboard that offers real-time reporting, trend analysis, tracking, and case management to facilitate decision-making and response.
- iv. The AML solution shall provide an intuitive, user-friendly interface that allows users to efficiently navigate and operate the system.
- v. Multi-language and multi-currency support is essential to ensure the system's usability across different geographical regions and subsidiaries (for banks with international authorization).

4.3 System Integration & Scalability

- i. The solution shall support real-time data exchange between systems involved in the AML/CFT lifecycle, ensuring real-time processing of transactions and alerts.
- ii. Batch processing shall be supported for periodic tasks such as report generation and historical analysis without interrupting real-time monitoring.
- iii. The solution shall provide well-documented, standard-based APIs (e.g. RESTful APIs) for integration with internal and external systems.

- iv. The solution shall offer flexibility to integrate with legacy systems and external third-party services if required via configurable connectors.
 - v. With approval of the CBN, the solution may be operated under a shared services arrangement in line with the provisions of the Guidelines for Shared Services Arrangements for Banks and Other Financial Institutions (2021).
 - vi. Where integration between certain systems is not feasible, user-friendly interfaces and automated data import/export capabilities should be provided to facilitate ease of data entry and validation.
 - vii. All Institutions shall deploy scalable AML solutions capable of handling increasing transaction volumes and ensuring secure data transmission.
 - viii. The AML solution shall support seamless integration with other key financial systems, including core banking applications, customer onboarding systems, transaction processing systems and regulatory reporting platforms.
 - ix. The solution shall leverage Application Programming Interfaces (APIs) to enable seamless integration between systems and ensure smooth data flow.
 - x. Format for exchange of data through the API shall be standardized in line with extant regulations.
- 4.4 Sanction list & PEP Screening
- i. The solution shall integrate with domestic and global watchlists for sanctions screening.
 - ii. The solution shall include AI-driven fuzzy matching algorithms to detect name variations and similarities.
 - iii. The screening solution shall have Real-time update of sanction lists for screening of new and continuous screening of existing customers.
 - iv. The system shall allow the addition of internal watch-list.
 - v. The solution shall integrate a Politically Exposed Persons (PEPs) database and automatically flag PEPs and high-risk individuals.
 - vi. The system shall have capability for adverse media monitoring.

- 4.5 Transaction Monitoring & Risk-Based Analysis
- i. Institutions shall conduct periodic system Stress Testing & validation to ensure reduction of False Positive.
 - ii. The institution should define a predetermined threshold for false positives and ensure that the false positive rate remains below this threshold.
 - iii. The AML solution shall have AI/ML capabilities for anomaly detection, behavioural pattern recognition, automated risk scoring, and adaptive learning to recommend improvements based on insights from flagged alerts and resolution outcomes.
 - iv. The solution shall have real-time alerts for cross-border transactions (where applicable), excessive cash deposits, crypto-related transactions, or other high-risk activities as defined in line with extant AML regulations. Time taken to screen and make decision on such alerts shall not exceed the predetermined timeline.
 - v. The AML solution must incorporate comprehensive transaction monitoring capabilities, using multiple risk scenarios based on configurable filtration rules and customer segmentation to detect suspicious activities.
 - vi. The system shall include related-party mapping and peer grouping analysis to enhance effective monitoring.
- 4.6 Customer Due Diligence (CDD), Know Your Customer (KYC) & Know Your Customer's Business (KYB)
- i. The AML solution shall have real-time access to the customer due diligence information for risk profiling, screening and transaction monitoring.
 - ii. Financial Institutions shall automate its onboarding process with real-time customer identification and verification in line with AML/CFT/CPF Regulations. The system must have the capability for integration with BVN and/or NIN databases to ensure real-time identification and verification.
 - iii. The solution shall have a comprehensive KYC/KYB capability, including automated customer risk profiling, transactional behaviour, historical data, other risk factors derived from ML/TF/PF risk assessments and typologies.
 - iv. The solution shall enable continuous customers classification into appropriate risk categories to facilitate targeted risk management and

due diligence processes. It shall also provide reports on reclassification of customers for review by control functions.

- v. The system shall support automated Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) procedures, with continuous reviews based on the risk category of the customer.
- vi. The solution shall allow continuous data synchronization, ensuring KYC records remain updated vis-a-vis customer profiles and transactional data.

4.7 Risk Assessment

- i. The solution should be customizable to meet the specific needs of the financial institution, including the ability to tailor rule configurations, risk scenarios, and alert thresholds.
- ii. The AML solution must automatically conduct risk assessments of customers at onboarding, continuously assess customers' risk levels and adjust risk profiles based on new data or changes in behaviour.
- iii. The system should support enterprise AML/CFT/CPF risk identification, measurement, and assessment.
- iv. The AML solution shall apply dynamic risk profiling, based on customer behaviour, transaction history, location, business type, KYC/KYB data, etc.
- v. Adaptive learning and automated scenario calibration (ASC) must be employed to optimize risk-based analysis and reduce detection errors.

4.8 Regulatory Reporting

- i. The Transaction Monitoring System shall support automated detection, case escalation and electronic reporting of suspicious transaction/activity (STR/SAR) to NFIU within stipulated timeframes.
- ii. The AML solution shall include comprehensive compliance reporting features, including real-time insights and reporting capabilities for transaction monitoring, and regulatory obligations (e.g. Suspicious Transaction Report (STR) Currency Transaction Reports (CTRs) Foreign Currency Transaction Report (FTRs).
- iii. Automated reporting tools shall generate detailed compliance reports for internal and external stakeholders, ensuring all relevant information is captured.

4.9 Case Management

- i. The solution shall integrate an Enterprise Case Management (ECM) system that automates the creation, assignment, and management of cases.
- ii. The ECM shall include a risk-based transaction scoring mechanism to prioritize cases based on customer risk level and alert severity.
- iii. Role-based workflows (Maker-Checker functionality) should be implemented to ensure thorough review and approval of cases before resolution.
- iv. The solution shall have aging and resolution analysis for cases and keep audit trail of all system generated cases.

4.10 Security & Data Protection

- i. The solution shall collect and store essential data required for AML/CFT/CPF compliance.
- ii. The AML solution shall include built-in data security mechanisms, including encryption at rest and in transit, to protect sensitive customer information and transaction data.
- iii. The system shall implement measures to ensure that users have access only to the data and functionality relevant to their role.
- iv. Multiple Factor Authentication (MFA) shall be required for accessing the system, especially for administrators and users with access to sensitive data or system settings.
- v. The solution shall implement secure authentication protocols.
- vi. The solution shall comply with the Nigerian data protection laws and regulations.
- vi. The system shall include comprehensive audit trails and logging features to track user actions and system changes for accountability and compliance monitoring.

4.11 Enforcement & Compliance Monitoring

- i. Financial institutions shall maintain this baseline standard.
- ii. The CBN shall conduct periodic compliance inspections and system validation exercises.

- iv. Institutions failing to meet these baseline standards will be subject to regulatory sanctions and penalties.

6. OTHER REQUIREMENTS

FIs shall also:

- i. Document and report to the relevant CBN Department, all AML solutions in use specifying primary and supporting roles.
- ii. Maintain a Vendor Management Policy outlining roles, responsibilities, rights, and support agreements for all AML solutions that require vendor support.
- iii. Ensure that where a third-party service provider is used, the entity complies with all applicable provisions in this document.

7. IMPLEMENTATION AND COMPLIANCE

Financial institutions shall align their AML solutions with these baseline standards within 12 months of the issuance of these standards.

The CBN will conduct follow-up reviews and periodic industry assessments to ensure compliance.

Institutions shall provide regular training to AML teams on system usage and emerging risks.

CENTRAL BANK OF NIGERIA
MAY 2025