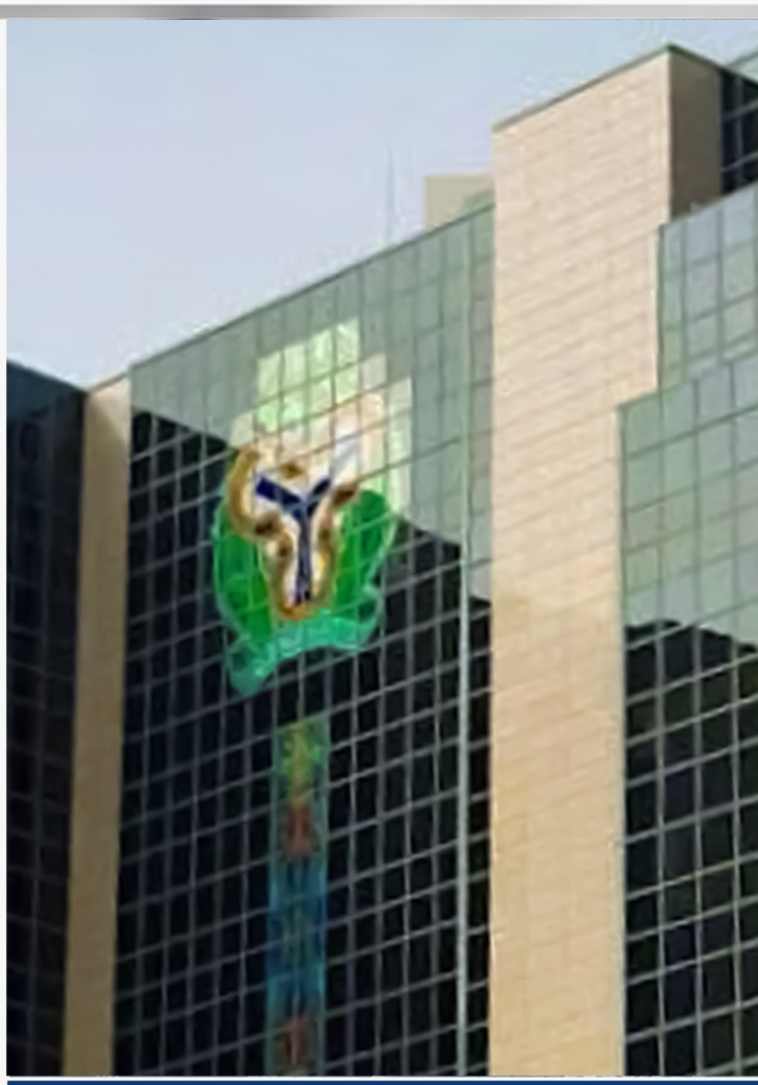
NEW ERA ATTORNEYS

Insight
Integrity
Impact

A REVIEW OF

CBN BASELINE STANDARD FOR AUTOMATED ANTI-MONEY LAUNDERING SOLUTIONS

FOR FINANCIAL INSTITUTIONS IN NIGERIA.



The growing digitization of financial services has significantly increased the volume and complexity of financial transactions within Nigeria's financial system. While this transformation has improved efficiency and financial inclusion, it has also heightened exposure to financial crimes, most notably money laundering and other illicit financial activities.

Compliance, Dispute Resolution, Data Privacy & Protection,

Debt Recovery, Intellectual Property, Real estate

White Collar Investigation/ Criminal Defence

General Corporate Advisory/ Secretarial service

AUTHORED BY:
NEW ERA ATTORNEYS

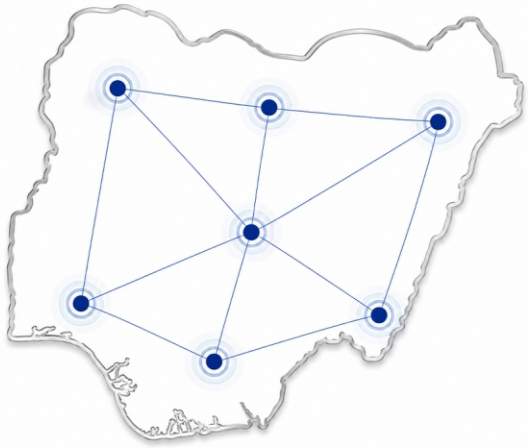
May Edition

https://neweraattorneys.com/

1. INTRODUCTION

The growing digitization of financial services has significantly increased the volume and complexity of financial transactions within Nigeria's financial system. While this transformation has improved efficiency and financial inclusion, it has also heightened exposure to financial crimes, most notably money laundering and other illicit financial activities. As a result, traditional manual AML/CFT/CPF control are becoming increasingly inadequate to effectively manage emerging financial crime risk.

In response to these, the Central Bank of Nigeria (CBN), on the 10th of March, 2026, issued the Baseline Standards for Automated Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Countering Proliferation Financing (CPF) Solutions for Financial Institutions in Nigeria (the "Baseline Standards"). The baseline standards introduce complementary regulatory requirements mandating financial institutions to deploy automated AML Solutions capable of supporting risk-based customer due diligence, facilitating the timely detection of suspicious transactions, and enabling accurate and timely reporting to the CBN, Nigerian Financial Intelligence Unit (NFIU), and other relevant authorities in line with the Financial Action Task Force (FAFT) recommendations and other applicable inter national standards.



2. OBJECTIVES OF THE BASELINE STANDARDS

The primary objective of the Baseline Standards is to establish minimum functional, governance and operational requirements for automated AML solutions deployed by financial institutions in Nigeria.

More specifically, the standards are intended to:

i. Provide a clear framework for automated AML deployment, configuration, operation, and governance; ensuring that institutions implement solutions capable of proactive and risk-based monitoring of financial transactions.

ii. Promote integration across financial institution systems. The standards encourage seamless integration between AML systems and other operational platforms such as core banking systems, payment platforms, onboarding processes, customer databases and other relevant infrastructure, enabling a more holistic assessment of finan cial crime risks.

iii. Improve the quality, accuracy and timeliness of detecting and reporting of suspicious financial activities through the use of appropriate technologies, including artificial intelligence, machine learning, and advanced ana lytics, where suitable. These tools help reduce false positives and strengthen overall compliance processes.

iv. Strengthen compliance with domestic and international AML obligations, particularly in relation to customer due diligence, sanctions, and politically exposed persons screening, record-keeping, and regulatory reporting.

v. Establish a framework for the continuous review and improvement of AML systems to ensure they remain responsive to evolving transaction patterns, changes in financial products and delivery channels, and emerging money-laundering and terrorism-financing risks.

3. SCOPE AND APPLICABILITY

These baseline standards apply to all financial institutions (Fis) operating within the CBN's supervisory purview. However, the configuration, depth and capabilities of such automated AML system solution is required to be tailored proportionately to each institution's own size, transaction volumes, type of product and services offered, operational complexity, number of customers, as well as their documented ML/TF/PF Risk assessment. Institutions with higher ML/TF/PF risk are required to apply stronger monitoring capabilities that are proportional to their risk profile.

The Baseline Standards are also intended to operate in conjunction with existing Nigerian AML/CFT regulatory frameworks. Where there is any overlap between the Baseline Standards and other regulatory requirements, fi nancial institutions are expected to apply the more stringent or risk-consistent requirement.

4. KEY REQUIREMENT OF THE BASELINE STANDARDS

a. AML SOLUTION CAPABILITIES

The Baseline Standards require financial institutions to deploy automated AML solutions with core capabilities covering customer ID and verification, risk assessment, sanction and watchlist screening, PEPs screening, transaction monitoring, case management and investigation, regulatory and internal reporting, audit and governance, as well as security control and data protection controls.

Where the AML platform is also used for fraud monitoring, its fraud detection functionality must be clearly separated and adjusted to prevent the AML/CFT/CPF detection from being watered down.[1]

Beyond that, financial institutions are required to make sure that the size and the risk profile of their operation are proportional to the AML solution, ensure AML monitoring and screening are not degraded during system migration, upgrades or technology transitions and also review and upgrade the AML solution where necessary in tandem with changes in its business model.

Importantly, CBN emphasizes that automated AML solutions must assess transactional activity in the context of the full customer profile.

Monitoring systems that rely solely on raw transactional data without effective linkage to CDD/KYC/KYB information and customer risk assessments will not be regarded as compliant with the Baseline Standards. Financial institutions are therefore expected to ensure that transaction monitoring systems are integrated with relevant customer due diligence and risk profiling data. [2]

b. CDD, KYC, KYB INTEGRATION

The Baseline Standards require the AML solutions to enable and support CDD, EDD, KYC, KYB processes. In addition, the systems must be capable of analyzing transaction behavioral patterns, based on customers' risk categories, allowing continued data linkage between KYC/KYB records and ensuring that KYB/KYC information can be accessed by investigators where need be.[3]

Financial institutions are also expected to move towards automated and semi-automated onboarding processes, which will ensure that customers' details are integrated with/linked to registered records and databases like BVN and NIN, and supported by real-time data checks in line with CBN KYC re quirements.
In addition, institutions are required to notify the CBN supervisory department of the AML solutions in use, as well as ensuring that CDD/KYC /KYB data used by the AML solution is accurate and up to date, through periodic reviews. [4]

c. SANCTIONS LISTS & PEP SCREENING EXPECTATIONS

The standards require AML solutions to be integrated with relevant domestic and international sanctions lists, watchlists and regulatory databases. The system must be capable of narration detection, support real-time or near real-time updates of sanctions and watchlists, integrate PEP and high-risk customer registers, enabling automatic flagging of PEPs and other high-risk individual or entities. further, the system must support automated interdictions or hold on transactions, including blocking of onboarding, where there are confirmed sanction match in line with legal requirements.[5]

Accordingly, Financial institutions are expected to implement risk-based sanctions and PEP screening procedures at onboarding and periodically, supported by documented procedures for investigating resolving potential matches. This procedures must include clear escalation and reporting protocols; and importantly, the institutions must be able to show upon request

CBN baseline standards for automated anti-money laundering (AML) solutions for financial institutions in Nigeria (March 2026), Para 5.1.

Ibid, Para 4.
Ibid para 5.2 (a(i-iv)).
Ibid para 5.2 (b(i-iv).
Ibid para 5.3(a(i-viii)).

4. CONTINUATION

that the sanctions & PEP screening processes are effective, including evidence of alerts generated and decisions taken.[6]

d. RISK ASSESSMENT

The Baseline Standards require AML solutions to support financial institution's documented risk appetite and risk assessment framework. The systems must be configurable to assess customer risk at the onboarding and dynamically adjusting customers' risk profile in response to new data or behavioral changes. AML solutions must also; support enterprise-level risk identification, measurement and assessment, support adaptive learning where AML-based modes are used, and generate reports on changes in customers' risk classification. [7]

Furthermore, financial institutions are required to conduct and document periodic risk assessment at the enterprise and business level, as well as generate and keep risk assessment reports along with evidence of resulting changes, thresholds, and control activities.

e. TRANSACTION MONITORING AND RISK-BASED ANALYSIS

The Baseline Standards require AML solutions to support risk-based transaction monitoring and activity analysis, using techniques such as behavioural pattern recognition, anomaly detection, predictive analytics and automated risk scoring to identify potential AML/CFT/CPF risks.

Where justified by risk, AML systems should be capable of generating pre-emptive alerts for high-risk activity, enabling institutions to take preventive or mitigating measures such as enhanced verification or temporary transaction holds pending review.

The monitoring framework must be built around configurable risk scenarios and customer segmentation, incorporating relevant CDD/KYC/KYB attributes; including customer occupation, income or turnover range, geography, delivery channels and product usage, in addition to raw transactional patterns. The standards also encourage the use of related-party mapping, peer-group analysis and network analysis to enhance the detection of unusual transaction patterns. [8]

The CBN further requires financial institutions to maintain appropriate governance over monitoring rules and thresholds, independent validation of artificial intelligence or machine-learning models where deployed, and documented service-level timelines for reviewing high-risk alerts. Institutions [4] that permit automated alert closure must restrict such automation to clearly defined low-risk scenarios, subject to governance oversight and notification to the CBN.[8]

f. FRAUD MONITORING AND DETECTION

Where an AML solution is also deployed for fraud monitoring, the system is expected to support the detection of suspicious activities across relevant channels. Institutions are required to ensure fraud detection capabilities operate in timely manner and are supported by regularly updated fraud detection rules, scenarios and models as new fraud trends emerge.

The baseline standards also require coordinated workflows [5] for managing alerts and investigations across AML, CFT, CPF, and fraud functions. In this regard, institutions are required to interface with internal blacklists, fraud registries, and relevant external databases to facilitate effective screening and verification, while ensuring that investigations and outcomes are properly documented through auditable records.[10]

Ibid para 5.3(b(i-iii)).
Ibid para 5.4(a(i-vi)).

Ibid para 5.5(a(i-iv)).
Ibid para 5.5(b).
Ibid para 5.6(a(i-vi)).

4. CONTINUATION

Financial institutions are further required, where their risk profile justifies it, to adopt a unified financial crime risk framework in which AML and fraud monitoring systems share data, analytics tools, and coordinated case management processes, provided that AML, CFT, and CPF obligations remain fully satisfied and are not subordinated to fraud priorities. Institutions with higher risk ratings or significant electronic transaction volumes are expected to demonstrate credible plan towards such integration while ensuring that material fraud indicators are incorporated into the customer's ML/TF/PF risk profile and transaction monitoring scenarios. [11]

g. CASE MANAGEMENT REQUIREMENTS

The standards further require AML solutions to provide Enterprise Case Management (ECM) capabilities that automates the creation, assignment, prioritization, and tracking of cases arising from alerts. The system should support role-based workflow and escalation paths, ensuring that cases are investigated in a timely and structured manner. It must also maintain full audit trails of each step taken on each case during the investigation process and the rationale for decisions made.[12]

Financial institution must also ensure prompt investigations of cases, make appropriate decisions with rationale and properly document the outcome. Closed cases should also be periodically analyzed and reviewed with a view to identifying patterns, weaknesses, and opportunities for improving monitoring scenarios, with findings forwarded to senior management and regulator if need be.

h. REPORTING OBLIGATIONS

AML solutions must support the automated generation of regulatory reports, including Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), Foreign Currency Transaction Reports, and other applicable AML/CFT/CPF returns, in line with the reporting requirements of the Central Bank of Nigeria. The system should also produce periodic internal management reports for the Chief Compliance Officer, senior management, and the board to support effective oversight of transaction monitoring activities. In addition, it should facilitate the submission of required reports to relevant regulators and other competent authorities.[13]

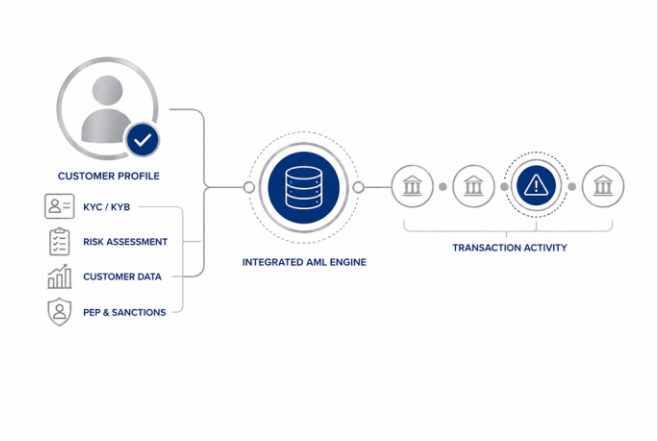
Financial institutions are equally required to ensure that reports submitted to the CBN and other relevant authorities are accurate and filed within the prescribed timelines. They are also expected to establish an internal gover nance framework for the review and approval of regulatory reports, supported by properly documented investigative procedures.

Ibid para 5.6(b(i-ii)).
Ibid para 5.7(a(i.iv)).
Ibid para 5.8 (a(i-iii)).

4. CONTINUATION

i. AUDIT AND GOVERNANCE CONTROLS

Financial institutions are required to maintain a comprehensive audit and governance controls over their AML solutions. This includes maintaining a reliable audit trail of all system and user activities, ensuring that records are readily retrievable for internal review, and regulatory inspection. In addition, financial institutions are also expected to establish a clear governance framework defining roles, access controls and oversight responsibilities for the management of AML systems, while ensuring that personnel responsible for operating and supervising the sys tems receive appropriate training and capacity development.[14]



j. SECURITY AND DATA PROTECTION

Financial institutions are required to implement appropriate data security and governance measures for AML systems. This includes limiting data collection to what is necessary for AML/CFT/CPF compliance, implementing strong security controls to protect sensitive personal data and ensure its confidentiality and integrity. In addition, they are to ensure system resilience through defined recovery objectives, and maintaining compliant data storage, retention and destruction practices in line with applicable data protection and data sovereignty requirements.[15]

5. ENFORCEMENT AND IMPLEMENTATION

The guidelines take effect immediately upon issuance. Financial institutions are required to achieve full compliance with the standards within 24 months from the date of issuance, while Deposit Money Banks (DMBs) are required to comply within 18 months. Institutions are also required to submit an implementation roadmap to the Compliance Department of the Central Bank of Nigeria within three months, outlining the steps they intend to take to achieve compliance.

During the implementation period, institutions seeking regulatory authorization must demonstrate clear plans for meeting the requirements of the standards. The CBN will monitor compliance through on-site examinations, off-site surveillance, and other supervisory mechanisms. Institutions that fail to comply may be subject to administrative sanctions, penalties, or remedial directives under applicable laws. Such sanctions may apply not only to the institution but also to accountable individuals where appropriate.[16]

Ibid, para 5.9(a & b).
Ibid para 5.11 (a & b)

6. IMPLICATIONS FOR FINANCIAL INSTITUTIONS

The introduction of the new baseline standards for automated AML solutions is expected to have significant opera tional and compliance implications for financial institutions.

First, institutions will need to undertake substantial upgrades to their technology infrastructure to ensure proper integration of AML solutions with core banking systems, payment platforms, and other operational channels. This may involve the acquisition of new compliance technologies, system enhancements, and the deployment of advanced monitoring tools capable of meeting the technical requirements prescribed by the standards. Second, the implementation of these solutions will require additional investment in operational capacity, including

specialized personnel, staff training, and enhanced compliance monitoring structures. Financial institutions will therefore need to strengthen internal expertise to effectively manage automated monitoring systems and maintain ongoing compliance with regulatory requirements.

Third, the adoption of automated transaction monitoring systems, including solutions supported by artificial intelligence and advanced data analytics, is expected to improve the early detection of suspicious transactions and reduce reliance on manual monitoring processes. This may enhance the overall effectiveness of AML/CFT/CPF controls and enable institutions to respond more efficiently to emerging financial crime risks. Finally, the standards signal heightened regulatory expectations regarding reporting, system governance, and monitoring effectiveness. Financial institutions will therefore need to ensure that their AML solutions are properly calibrated, subject to periodic review, and capable of supporting timely regulatory reporting. In addition, where AML solutions platform also supports fraud monitoring, functions, institutions must ensure clear separation of capabilities to avoid undermining the effectiveness of AML/CFT/CPF detection and monitoring processes.

[2] [5]

ibid para 7

7. CONCLUSION

The issuance of the Baseline Standards by the Central Bank of Nigeria marks a significant step in the ongoing efforts to strengthen the country's financial crime compliance framework. By formalizing minimum requirements for the deployment and governance of automated AML solutions, the CBN is clearly signaling a shift toward technology-driven, risk-based financial crime monitoring across the financial services sector.

For financial institutions, the Standards go beyond introducing new compliance obligations, they establish a clear regulatory expectation that AML systems must be robust, integrated and capable of responding to increasingly complex transaction patterns in a digital financial ecosystem. Institutions will therefore need to take a proactive approach in assessing their existing AML frameworks and implementing the necessary enhancements within the prescribed timelines.

Authors

Abubakar Ibrahim
(Partner)
i.abubakar@neweraattorneys.com

Michael Kasali
(Associate)
m.kasali@neweraattorneys.com