

Key Highlights of the Central Bank of Nigeria's Baseline Standards for Automated Anti-Money Laundering Solution

Banking & Finance Insight



May 2026

Introduction





On March 10, 2026, the Central Bank of Nigeria ("CBN") issued The Baseline Standards for Automated Anti-Money Laundering (AML) Solution for Financial Institutions in Nigeria ("The Standards"). The Standards were issued pursuant to the powers conferred on the CBN by Section 2(d) of the CBN Act, 2007 and Section 66(2) of the Banks and Other Financial Institutions Act (BOFIA), 2020.

The issuance of the Standards comes at a critical time, as financial crimes are becoming increasingly sophisticated and regulatory authorities worldwide are intensifying efforts to combat illicit financial flows. In response, the CBN has taken a significant regulatory step to strengthen Nigeria's financial system by introducing standardised, automated AML compliance requirements to reinforce Nigeria's framework for combating money laundering, terrorist financing, and proliferation financing.

This article examines the key highlights of the Standards, focusing on their scope, core compliance requirements, and the potential impact on financial institutions operating in Nigeria.

Key Objective: To strengthen Nigeria's financial system by introducing standardised, automated AML compliance requirements to reinforce Nigeria's framework for combating money laundering, terrorist financing, and proliferation financing.

- ✓ Real-time customer identification and verification
- ✓ Comprehensive screening against watchlists
- ✓ Automated transaction monitoring

-  **Size** - Institution's scale and operations
-  **Risk profile** - ML/TF risk assessment
-  **Business model** - Type of financial services
-  **Transaction volumes** - Volume and complexity

DMB
Compliance
18 months

Sept 2027

OFI
Compliance
24 months

March 2028

Roadmap
3 months
June 2026

Scope of Application and Enforcement

The Standards apply to all banks and financial institutions within the CBN's regulatory purview. By virtue of the Standards, all financial institutions are required to operate an automated AML/CFT/CPF Solution, with the extent, configuration and sophistication calibrated to the institution's size, risk profile, business model, transaction volumes and complexity.¹

The CBN, to facilitate proportionate implementation across specific subsectors or institutional types, may issue supplementary sector-specific guidance. Furthermore, to enhance comprehensive compliance, these Standards are to be interpreted and applied in conjunction with relevant existing laws.²

The implementation of the standards shall start on the date of issuance, March 10, 2026, while full compliance shall be 18 months (for Deposit Money Banks (DMBs)) and 24 months (for Other Financial Institutions (OFIs)) from the date of issuance. Therefore, DMB have till September 10, 2027, to comply, and OFIs have till March 10, 2028. Institutions are also required to submit implementation roadmaps to the Compliance Department of the CBN within 3-months from the date of issuance of the standards.³ Therefore, institutions must submit their implementation roadmaps to the CBN's Compliance Department by June 10, 2026.

Financial institutions are required to comply with these Standards within the timelines prescribed by the CBN.⁴ The CBN will monitor and assess compliance with the standards through off-site surveillance and on-site examinations.⁵ Non-compliance will attract remedial directives, administrative sanctions, and penalties in line with extant laws and regulations, including sanctions on the institution and, where appropriate, accountable individuals, as provided for under applicable legal and regulatory frameworks.⁶



Implementation Timeline

18 months for DMBs, 24 months for OFIs



Risk Assessment

Calibrated to institution's size and risk profile



Implementation Schedule

Issuance

Mar 10, 2026

Start

Roadmap

Jun 10, 2026

3 months

DMB

Sept 10, 2027

18 months

OFI

Mar 10, 2028

24 months

Key Matters Arising

The CBN's Standards are structured around several critical components, each designed to address specific facets of AML/CFT/CPF risk management:



AML Solution

Article 8 - Automated System Definition

Article 8 of the Baseline standards defines an AML Solution as an automated system with capabilities that include customer identification and verification, risk assessment, sanctions screening, transaction and fraud monitoring, case management, reporting, audit and governance, and data protection.⁷ Where the AML Solution is also deployed for fraud monitoring, its fraud-related functionalities must be clearly segregated and appropriately governed to ensure that the effectiveness of AML/CFT/CPF detection is not compromised.⁸

● Required for all FIs

Priority: High



CDD/KYC/KYB

Customer Due Diligence, Know Your Customer, Know Your Business, and Risk Assessment

The Standards mandate that the AML solution shall enable an end-to-end support for CDD, EDD, KYC and KYB processes,⁹ and must possess robust capabilities for real-time customer identification and verification.¹⁰ This involves comprehensive screening against various watchlists, including sanctions lists, Politically Exposed Persons (PEPs) databases, and adverse media.¹¹ The objective is to ensure that financial institutions have a clear and accurate understanding of their customers and beneficial owners, thereby mitigating the risks associated with onboarding high-risk individuals or entities. Financial institutions are also required to conduct and document periodic Money Laundering/Terrorism Financing/Proliferation Financing risk assessments at enterprise and business-line level ensuring that the AML Solution configuration reflects these assessments.¹²

● Mandatory

Real-time



Transaction/Fraud Monitoring

Real-time Detection & Analysis

Continuous transaction monitoring is a cornerstone of effective AML. The Standards require automated solutions to perform real-time or near real-time monitoring of all transactions. This capability is crucial for detecting unusual patterns, anomalies, and deviations from expected behaviour that could indicate money-laundering or terrorist-financing activities.¹³ Recognising the intricate link between fraud and money laundering, the Standards provide the standard to be employed when the AML Solution is to be used for fraud monitoring.¹⁴ The solution should be able to identify and flag suspicious activities across various channels, including cards, e-channels, deposits, and lending in real time or near real time.¹⁵

● Active Monitoring

24/7



Case Management

Enterprise Case Management (ECM)

Effective case management is vital for streamlining the investigation and resolution of AML alerts. The Standards stipulate the need for an Enterprise Case Management (ECM) capability that automates the creation, assignment, prioritisation, and tracking of cases arising from AML/CFT/CPF alerts.¹⁶ This includes maintaining full audit trails of all actions taken on cases, ensuring transparency, accountability, and efficient workflow management.¹⁷

● Automated

Full Audit Trail



Reporting

Regulatory Reports & Submissions

Timely and accurate submission of regulatory reports is a critical compliance obligation. The Standards require automated AML solutions to support the generation of various regulatory reports, including Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and Foreign Currency Transaction Reports (FTRs).¹⁸ These reports must conform to the formats and channels prescribed by the CBN and other competent authorities, ensuring seamless information exchange and regulatory oversight.

● Required Reports

4 Types



Audit & Governance

System Integrity & Compliance

To ensure the integrity and reliability of automated AML solutions, the Standards impose stringent audit and governance requirements. This includes maintaining a comprehensive, tamper-proof, and immutable audit trail of all system and user activities and establishing a documented governance framework for the AML solution.¹⁹ Periodic independent internal and external reviews are required to assess the solution's effectiveness and ensure ongoing compliance.²⁰

● Mandatory

Periodic Reviews



System Integration & Scalability

Core Banking Integration

The Standards underscore the importance of seamless and secure integration between the AML solution and other critical banking systems, such as core banking, customer information/KYC systems, and other relevant applications.²¹ This ensures a unified view of customer data and transaction information, facilitating comprehensive risk assessment. Furthermore, the solutions must be scalable to accommodate increasing transaction volumes and evolving business needs without compromising performance or detection quality.

● Integrated

24/7 Available



Security & Data Protection

NDPA Compliance & Controls

Given the sensitive nature of the data processed by AML solutions, robust security and data protection measures are paramount. The Standards require the implementation of strong security controls,²² and compliance with the Nigeria Data Protection Act (NDPA) and other privacy laws.²³ This ensures the confidentiality and integrity of sensitive financial information.

● Mandatory

High Priority



Enforcement Measures

Remedial Directives

Immediate

Available

Administrative Sanctions

Applied

Active

Penalties

Financial

Up to ₦50M

Individual Sanctions

Personal

Accountable

Conclusion

The Central Bank of Nigeria's Baseline Standards for Automated Anti-Money Laundering Solution mark a significant milestone in Nigeria's fight against financial crime. By mandating the adoption of advanced technological solutions and setting clear operational and governance requirements, the CBN is not only strengthening the resilience of the financial sector but also aligning Nigeria with international best practices in AML/CFT/CPF. Financial institutions must prioritise implementing these Standards, recognising them as an essential investment in safeguarding the integrity of the financial system and fostering sustainable economic growth.



Enhanced Security

Robust automated systems for real-time detection and prevention of financial crimes



Global Standards

Alignment with international best practices in AML/CFT/CPF compliance



Economic Growth

Fostering sustainable economic growth through financial integrity

1. The Baseline Standards; Article 4, 'Scope'
2. The laws that the Baseline Standards for AML, CFT and CPF 2026 are required to be read in conjunction with include the "Money Laundering (Prevention and Prohibition) Act, 2022 (MLPPA), Terrorism (Prevention and Prohibition) Act, 2022 (TPPA), Central Bank of Nigeria (Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing of Weapons of Mass Destruction in Financial Institutions) Regulations, 2022, CBN AML, CFT and CPF (Administrative Sanctions) Regulations, 2023, CBN Risk-Based Cybersecurity Framework; Other relevant CBN regulations, circulars, and guidelines and other applicable laws or regulations
3. Central Bank of Nigeria, Circular to All Banks, Mobile Money Operators, International Money Transfer Operators, Other Financial Institutions and Payment Service Providers: Issuance of the Baseline Standards for Automated Anti-Money Laundering (AML) Solution for Financial Institutions in Nigeria BSD/DIR/PUB/LAB/019/002 (10 March 2026).
4. The Baseline Standards; Article 7(a), 'Enforcement & Implementation'
5. The Baseline Standards; Article 7(c), 'Enforcement & Implementation'
6. These applicable legal and regulatory frameworks include but are not limited to the BOFIA, the MLPPA, and the CBN AML-CFT-CPF Administrative Sanctions Regulations 2023
7. The AML Solution shall at a minimum, be required to support some functional areas such as: a. Customer Identification and Verification (including remote/onboarding channels); b. Customer Risk Assessment and Profiling; c. Sanction and Watchlist Screening; d. Politically Exposed Persons (PEPs) and High-Risk Customer Screening; e. Transaction Monitoring for ML/TF/PF risk; f. Case Management and Investigation; g. Regulatory and Internal Reporting; h. Audit and Governance (including logs and configuration trails); i. Data Protection and Security Controls relevant to AML/CFT/CPF activities
8. The Baseline Standards; Article 5.1, 'Enforcement & Implementation'
9. The Baseline Standards; Article 5.2, 'CDD, KYC and KYB'
10. Where available, institutions should integrate with national identity databases, including the Bank Verification Number (BVN) and National Identification Number (NIN) systems, as infrastructure that supports real-time identity corroboration
11. The Baseline Standards; Article 5.3, 'Sanction Lists & PEP Screening'
12. The Baseline Standards; Article 5.4, 'Risk Assessment'
13. The Baseline Standards; Article 5.6, 'Fraud Monitoring and Detection'
14. Ibid
15. Under the Baseline Standards "Real time" is used to reference the standards applicable to screening and is defined as "ability to process and evaluate a customer or transaction against relevant watchlists before the transaction is authorised or onboarding process is considered completed" while "near real time" is used to reference the standards applicable to transaction monitoring and is defined as "processing and evaluation of transactions as they occur, with the capability to generate an alert or trigger a pre-emptive action within stipulated timeframe that can prevent the completion of a suspicious activity (e.g., before funds are irreversibly settled)".
16. The Baseline Standards; Article 5.7, 'Case Management'
17. Institutions are required to investigate all cases promptly and adequately document outcomes and rationale.
18. The Baseline Standards; Article 5.8, 'Reporting'
19. The AML/CFT/CPF teams responsible for the operation, configuration, and oversight of the AML Solution are required to receive regular training on system usage, emerging ML/TF/PF typologies.
20. The Baseline Standards; Article 5.9, 'Audit and Governance'
21. The Baseline Standards; Article 5.10, 'System Integration & Scalability'
22. These security controls include the encryption of data at rest and in transit, multi-factor authentication (MFA), as well as role-based access controls, ensuring users have access only to data required for their duties
23. The Baseline Standards; Article 5.11, 'Security and Data Protection'

Contributors



Nimma Jo-Madugu
Partner, Banking & Finance



Chidera Mbaogu
Associate, Banking & Finance



CONTACT US

LAGOS

KENNA Place
8, Ogunyemi Road, Palace Way, Oniru
PO Box 73002, Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285, Abuja

ENUGU

Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner,
400211 Enugu State.

+234 811 395 1052, +234 811 395 1053
counsel@kennalp.com