BSD/DIR/PUB/LAB/019/002 **March 10, 2026**

CIRCULAR TO ALL BANKS, MOBILE MONEY OPERATORS, INTERNATIONAL MONEY TRANSFER OPERATORS, OTHER FINANCIAL INSTITUTIONS AND PAYMENT SERVICE PROVIDERS

ISSUANCE OF BASELINE STANDARDS FOR AUTOMATED ANTI-MONEY LAUNDERING (AML) SOLUTION FOR FINANCIAL INSTITUTIONS IN NIGERIA

The Central Bank of Nigeria, in furtherance of its mandate to promote financial system stability and integrity hereby issues the Baseline Standards for Automated Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing Solution in Nigeria.

The Baseline Standards provide a framework for implementing automated solutions that strengthen the detection and reporting of suspicious transactions in real time and enhance compliance with applicable AML/CFT/CPF laws and regulations, while also supporting the use of emerging technologies to improve overall financial crime risk management.

The implementation of these guidelines shall start from the date of issuance, while full compliance shall be **18-months** (for Deposit Money Banks) and **24-months** (for Other Financial Institutions) from the date of issuance. Therefore, institutions shall submit implementation roadmaps to Compliance Department within 3-months from the date of issuance.

All stakeholders are required to ensure strict compliance with the guidelines and all other regulations, as the CBN continues to monitor developments and issue further guidance as may be appropriate.

Please be guided accordingly.

Akinwunmi, A. Olubukola, PhD.
Director, Banking Supervision Department

Olubunmi Ayodele-Oni
For: Director, Compliance Department

CENTRAL BANK OF NIGERIA

BASELINE STANDARDS FOR AUTOMATED ANTI-MONEY LAUNDERING (AML) SOLUTIONS FOR FINANCIAL INSTITUTIONS IN NIGERIA

MARCH 2026

Table of Contents

1. PREAMBLE

Pursuant to the powers conferred on the Central Bank of Nigeria (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 CBN hereby issues these Baseline Standards for Automated Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing Solutions ("Baseline Standards") for financial institutions in Nigeria.

These Baseline Standards set minimum functional, governance and control requirements for automated AML/CFT/CPF solutions ("AML Solutions") deployed by regulated institutions. They do not replace existing legal and regulatory obligations but complement them by specifying what the CBN expects of technology used to support those obligations.

2. INTRODUCTION

As financial services become increasingly digitised and complex, manual AML/CFT/CPF controls are no longer sufficient to manage evolving risks. Financial institutions are expected to deploy automated AML Solutions that:

- support risk-based customer due diligence;
- enable timely detection of suspicious activity, and
- facilitate accurate, complete, and timely reporting to the CBN, NFIU and other competent authorities.

These Baseline Standards align with the FATF Recommendations and other relevant international standards. They are designed to ensure that technology deployed for AML/CFT/CPF purposes deliver demonstrable effectiveness and not merely feature-based compliance or vendor-driven implementation.

Implementation of these standards is expected to enhance the Nigerian financial system's ability to prevent, detect and report Money Laundering (ML), Terrorism Financing (TF) and Proliferation Financing (PF), and to support broader financial crime risk management, without weakening core AML/CFT/CPF responsibilities.

3. OBJECTIVES

The objectives of the baseline standards include to:

a) Ensure effective implementation of automated AML Solutions: Provide a clear framework for the deployment, configuration, operation and governance of AML solutions that support proactive, preventive and risk-based monitoring in line with regulatory expectations and FATF principles.
b) Promote interoperability and integration: Facilitate seamless, secure integration of AML solutions with core banking, payment, onboarding, and other relevant systems to ensure efficient data exchange and holistic risk assessment across products, channels, and entities
c) Enhance Detection Quality and Timeliness: Leverage appropriate technologies (which may include artificial intelligence, machine learning and advanced analytics, where suitable) to improve the quality, explainability and timeliness of alerts and STR/SAR decision-making, while controlling false positives.
d) Support compliance with domestic and international obligations: Reinforce compliance with extant Nigerian laws and regulations, FATF Recommendations and other applicable standards, including obligations relating to CDD, sanctions and PEP screening, record-keeping, and reporting.
e) Provide a framework for continuous system improvement: Establish minimum expectations for ongoing tuning, validation, back-testing, and governance so that AML Solutions are updated in response to changes in products, delivery channels, customer behaviour, typologies, and emerging ML/TF/PF risks.

4. SCOPE

These Baseline Standards apply to all banks and other financial institutions operating under the regulatory purview of the CBN. All 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.

Proportionality Principle: The CBN recognises that the Nigerian financial sector comprises institutions of materially different size, operational complexity, product scope, customer base, transaction volumes, and risk exposure. These Baseline Standards apply to all CBN-regulated institutions; however, the depth, sophistication and configuration of AML Solution implementation shall be calibrated proportionately to each institution's observable characteristics, including: transaction volumes and velocity; the nature, number and complexity of products and services offered; the size and composition of the customer base; geographic footprint and delivery channels; and the institution's own documented ML/TF/PF risk assessment. Institutions operating in sectors or business lines with elevated inherent ML/TF/PF risk; as identified in National and Sectoral Risk Assessments; shall apply enhanced monitoring capabilities commensurate with that risk profile, regardless of institutional size. The CBN may issue supplementary sector-specific guidance to provide further direction on proportionate implementation for particular subsectors or institution types.

They are to be read in conjunction with, and are intended to enhance compliance with:

- 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 Frameworks
- other relevant CBN regulations, circulars, and guidelines
- and other applicable laws or regulations.

The standards cover the following key areas:

a) System Requirements: functional, technical, governance and security requirements of AML Solutions including integration, availability, resilience, and scalability.
b) Transaction monitoring and risk-based analysis: requirements for transaction and activity monitoring, dynamic risk scoring, and where applicable, the use of artificial intelligence and machine learning for anomaly detection, subject to robust governance and validation.
c) Customer Due Diligence (CDD) and Know Your Customer (KYC): requirements for supporting automating CDD and KYC processes, including risk profiling and enhanced due diligence (EDD).
d) Sanctions, Internal watchlist, and PEP screening: requirements for screening against internal, domestic and international lists or watchlists and for managing hits, matches and real-time blocking of affected customers or transactions, where required.
e) Reporting: requirements for generating and transmitting regulatory and internal AML/CFT/CPF reports, including STRs and other required returns.
f) Case management: requirements for managing alerts and investigations in a structured, auditable manner.
g) Data security and protection: requirements for protecting the confidentiality, integrity and availability of data processed by AML Solutions.
h) Third-Party and vendor management: expectations when institutions outsource or procure AML solutions from third parties including Original Equipment Manufacturers (OEMs) and service providers.
i) Risk assessment: support for enterprise-level and customer-level ML/TF/PF risk assessment including, dynamic and scenario driven approaches.
j) Fraud detection and prevention: although this Standard does not mandate a unified AML–fraud system, financial institutions are required to deploy automated fraud-monitoring capabilities appropriate to their fraud-risk profiles. These capabilities may be hosted on the same platform as the AML Solution or on a separate fraud-management system, provided that:

i. both systems can exchange relevant risk signals seamlessly;
ii. the architecture avoids blind spots, duplication, and delays in detection; and
iii. fraud-specific controls meet real-time or near-real-time expectations, which AML transaction monitoring does not require.

Where a single solution is used for both AML and fraud, the institution must ensure logical separation of rules, maintain the integrity of AML/CFT/CPF controls, and demonstrate that fraud-risk requirements are adequately addressed.

k) Audit trails and audit data retention: requirements for traceable, tamper-proof records to support investigation, supervision, and enforcement.
l) Unified customer risk view: maintain, for each customer and related parties, a consolidated view that links KYC/KYB data, risk classification, transactional behaviour, alerts, and case history, and makes this view available within monitoring, screening, and case management workflows.

In the event of overlap with other laws or regulations, institutions are expected to apply the more stringent or risk-consistent requirement. These Baseline Standards represent the minimum threshold and do not prevent the Bank from expecting higher levels of control where appropriate.

For the avoidance of doubt, the CBN expects automated AML Solutions to assess activity in the context of the full customer profile and not monitoring solely on raw transactional data. AML Solutions without effective linkage to CDD/KYC/KYB information and customer risk assessments will not be regarded as compliant with these Baseline Standards.

5. BASELINE STANDARDS

The baseline standards below establish the minimum capabilities and governance requirements. Institutions may implement more stringent controls based on their risk profile.

5.1 AML Solution

The AML Solution shall, at a minimum, support the following functional areas:

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

Where the same platform is also used to monitor fraud, its fraud-related capabilities shall be clearly segregated, governed, and tuned so as not to dilute AML/CFT/CPF detection effectiveness.

The institution shall:

i. ensure that the AML Solution is commensurate with the nature, size, complexity, customer base and risk profile of its operations.
ii. ensure appropriate availability, resilience, and disaster recovery arrangements so that AML monitoring and screening are not degraded during system outages or migrations.
iii. review and where necessary, upgrade the AML Solution in line with changes in business model, product mix, delivery channels and risk exposure.

5.2 Customer Due Diligence (CDD), Know Your Customer (KYC) and Know Business (KYB)

a) The AML Solution shall:
    i. enable end-to-end support for CDD, EDD, KYC, and KYB processes, including automated risk profiling, transaction behavioural pattern analysis, use of historical data and detection of ML/TF/PF typologies.

ii. support risk based CDD and EDD, including periodic and event driven reviews based on customers' risk categories and behaviour.

iii. allow continuous data synchronisation and linkage between KYC/KYB records, customer risk profiles and transactional data, so that monitoring scenarios and alerts are evaluated in the context of the customer's known profile, expected activity and risk classification.

iv. ensure that, for any alert or case, investigators can view relevant KYC/KYB information (e.g., occupation, source of funds, income range, business activity, geography) alongside transactional history and prior case outcomes within a single interface.

b) The institution shall:

i. implement, to the extent feasible, automated or semi-automated onboarding with customer identification processes supported by real-time data checks, in line with CBN KYC requirements. 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; i.e., confirming that presented identity credentials are linked to a registered record. Institutions should note that such database checks are one component of a broader identification and verification framework and do not, in isolation, constitute complete customer verification.

ii. Institutions shall notify the relevant CBN supervisory department of all AML Solutions in use, specifying the primary and supporting functional roles of each system. This notification shall be made at initial deployment, upon material change, and upon request by the CBN. This requirement supports the CBN's maintenance of a sector-wide inventory of AML solution infrastructure.

iii. exercise due diligence to understand and record complex ownership and control structures and beneficial ownership, including manual escalation where system capabilities are insufficient.

iv. Ensure that CDD/KYC/KYB data used by the AML Solution is accurate, complete and kept up to date through periodic reviews and data quality controls.

5.3 Sanction Lists & PEP Screening

a) The AML Solution shall:

i. Integrate with relevant domestic and global sanctions, watchlists and other prescribed lists for screening of customers, beneficial owners, related parties, and transactions.

ii. include matching logic capable of detecting name variations and similarities, which may include AI- or fuzzy-matching techniques, provided these are subject to transparent configuration and validation.

iii. support real-time or near real-time updates of sanctions and watchlists and ensure that new or updated entries are promptly reflected in screening.

iv. Possess the capability to generate comprehensive logs that provide verifiable evidence of timely updates and the effectiveness of screening processes.

v. Permit inclusion and management of institution-specific internal watch-lists.

vi. Integrate PEP and high-risk customer lists/registers and automatically flag PEPs and other high-risk individuals and entities.

vii. Support adverse media or negative news monitoring.

viii. Be capable of automated interdiction or hold on transactions, or blocking of onboarding, where there is a confirmed sanctions match, in line with CBN and legal requirements.

b) The Institution shall

i. Ensure appropriate, risk-based screening at onboarding, periodically and on a continuous basis, in line with extant regulations.

ii. maintain documented procedures for triaging, reviewing, and resolving potential matches, including escalation and reporting.

iii. be able to demonstrate, upon request, that sanctions and PEP screening processes are effective, including evidence of resolved alerts, decisions and actions taken.

5.4 Risk Assessment

a) The AML Solution shall:
   i. be configurable to reflect the financial institution's documented risk appetite and risk assessment, including rule configurations, risk scenarios, and alert thresholds.
   ii. Support automated risk assessment at onboarding, dynamically adjusting customer risk profile in response to new data, behavioural changes and external risk factors.
   iii. support enterprise-level ML/TF/PF risk identification, measurement, and assessment (for example, by aggregating data across products, segments, and channels).
   iv. Where AI/ML-based models are used, support adaptive learning and model calibration under a documented governance framework, including human oversight and explainability.
   v. generate reports on changes in customer risk classification and the drivers of such changes.
   vi. where applicable, incorporate and analyse credible external data sources to enhance risk scoring and identification of emerging threats.

b) The Institution shall
   i. conduct and document periodic ML/TF/PF risk assessments at enterprise and business-line level and ensure that the configuration of the AML Solution reflects these assessments.
   ii. generate and retain risk assessment reports, together with evidence of resulting changes to scenarios, thresholds, and control activities.

5.5 Transaction Monitoring & Risk-Based Analyses

a) The AML Solution shall:

i. support risk-based transaction and activity monitoring using appropriate techniques (including, where suitable, predictive analytics, anomaly detection, behavioural pattern recognition, and automated risk scoring) to detect potential ML/TF/PF activity.

ii. have the capability, where justified by risk, to generate pre-emptive alerts for high-risk scenarios that allow institutions to take preventive or mitigating action, such as requiring enhanced verification, or placing a temporary hold on a transaction, pending review.

iii. incorporate comprehensive transaction monitoring using multiple risk scenarios, configurable rules and customer segmentation, aligned to documented risk assessments and typologies.

iv. ensure that monitoring scenarios and models make risk-based use of relevant CDD/KYC/KYB attributes (such as occupation, declared income or turnover range, customer segment, product profile, geography, and delivery channel) in addition to raw transactional patterns.

v. Support related-party mapping, network analysis and peer-grouping to improve identification of unusual or suspicious patterns. Where AI/ML is used, provide clear, auditable information on the key factors that contributed to the alerts to support human review and explainability (like unusual transaction patterns or behaviour compared to similar customers).

vi. Present, for each alert, a consolidated view of the customer's key KYC/KYB data, risk score, recent transactional behaviour and any previous alerts or cases, to support informed human decision-making on whether to close, escalate or report.

b) The institution shall:

i. Perform independent validation of all artificial intelligence and machine learning models at least annually and upon significant change covering accuracy, performance drift, fairness audits, bias testing, and human review where relevant and appropriate to the institution's risk profile.

For the purposes of this requirement, “independent” is defined in the Glossary.

ii. Define, document, and periodically review false positive and false negative thresholds appropriate to their risk profile, product mix, customer base, and transaction volumes.

iii. Document and justify threshold settings, scenario parameters and tuning decisions at least annually, and whenever material changes are made.

iv. Develop and document procedures for pre-emptive interventions arising from high-risk patterns, ensuring such measures are proportionate and consistent with customer rights and experience.

v. Establish governance arrangements (e.g., model committee, change-control process) overseeing authorisation and periodic review of automated actions and major changes to monitoring logic.

vi. Institutions shall define and adhere to internal service level standards specifying the maximum timeframe within which high-risk alerts shall be reviewed and a disposition decision recorded. These standards shall be documented and approved by senior management.

vii. Where the institution permits automated alert closure, ensure that:

- such automation is limited to clearly low-risk scenarios defined in the AML governance framework. For the purposes of these Baseline Standards, a “clearly low-risk scenario” eligible for automated closure is one that meets **all** of the following criteria: (a) the alert is generated by a rule or threshold reviewed, approved and documented by the institution’s AML governance committee; (b) the closure decision relies explicitly on both transactional context and current KYC/KYB data; (c) the customer’s risk classification is Low and has not changed within the preceding review period; and (d) no prior unresolved alerts or open cases exist for the same customer at the time of closure;
- the decision rules explicitly rely on both transactional and KYC/KYB context;

- periodic back-testing confirms that automated closures do not mask suspicious activity;
- Institutions that permit automated alert closure shall notify the CBN of this practice, the categories of scenarios subject to automation, and the institution-defined threshold for the proportion of total alerts eligible for automated closure. This notification shall be made upon adoption and following any material change. The institution's defined threshold shall be documented, approved by the AML governance committee, and reviewed at least annually. Any quarter in which automated closures materially exceed the institution's documented threshold shall be escalated promptly to senior management and reported to the CBN; and
- Governance arrangements for automated alert closure shall be subject to independent review by internal audit at least annually, separate from the compliance.

5.6 Fraud Monitoring and Detection

Where the AML Solution is also used for fraud monitoring, the following standards apply in addition to AML/CFT/CPF expectations:

a) The AML Solution shall:
   i. Monitor activities across relevant channels (e.g. cards, e-channels, deposits, lending) in real time or near real time to detect unusual patterns indicative of fraud. For the purposes of this section, "real time" and "near real time" shall have the meanings set out in the Glossary, which distinguish between the standards applicable to screening and to transaction monitoring respectively. Fraud monitoring controls, particularly for card and electronic channels, shall be calibrated to the faster intervention timelines appropriate to those channels.
   ii. Enable updating of fraud-related risk rules and models based on observed fraud trends and incidents across customers, accounts, and channels.
   iii. Support a unified workflow or tightly integrated workflows for managing alerts and investigations across AML, CFT, CPF and fraud with clear segregation of responsibilities to applicable units.

iv. Interface with relevant fraud registries, internal blacklists and external databases for cross-verification and screening.
v. Analyse historical data to identify fraud trends and generate predictive insights, where appropriate.
vi. Maintain full traceability of fraud-related events, including decisions and outcomes.

b) The Institution shall:
   i. where the risk justifies it, having regard to the institution's transaction volumes, product complexity, customer base and documented risk assessment, implement a unified financial crime risk architecture in which AML and fraud systems share a common data lake, analytics models, and coordinated case management, while ensuring that AML/CFT/CPF requirements remain fully met and not subordinated to fraud priorities. Institutions classified as High or Above Average risk within their respective subsectors, or those with material volumes of electronic or card-based transactions, shall be expected to demonstrate a credible roadmap towards such integration.
   ii. Ensure that material fraud indicators are incorporated as risk factors into the customer's overall ML/TF/PF risk profile and relevant transaction monitoring scenarios, where appropriate.

5.7 Case Management

a) The AML Solution shall:
   i. Provide Enterprise Case Management (ECM) capability that automates the creation, assignment, prioritisation and tracking of cases arising from alerts (AML/CFT/CPF and where relevant, fraud).
   ii. Enable role-based workflows, including Maker-Checker functionality and escalation paths to ensure robust case review and resolution.
   iii. Maintain full audit trails of all actions taken on cases, including timestamps, users, decisions and supporting rationale.

iv. Support the generation of reports on case volumes, ageing, outcomes, and key trends to inform management oversight, support compliance testing, operational review, and supervisory inspections.

b) The Institution shall:
   i. Ensure that cases are investigated promptly and adequately document outcomes and rationale.
   ii. Periodically review and analyse closed cases to identify emerging patterns, control weaknesses and opportunities for scenario tuning and escalate material findings to Senior Management and, where necessary, to regulators.

5.8 Reporting

a) The AML Solution shall support:
   i. automated or semi-automated generation of regulatory reports such as Suspicious Transaction Report (STR), Suspicious Activity Reports (SARs), Currency Transaction Report (CTR), Foreign Currency Transaction Report (FTR) and other applicable AML/CFT/CPF returns, with configurable formats and schedules in line with CBN reporting instructions.
   ii. Periodic internal management information (MI) reporting to, at a minimum, the Chief Compliance Officer, senior management, the Executive Compliance Officer, and the Board, to support oversight of AML/CFT/CPF risks and the effectiveness of transaction monitoring.
   iii. External reporting only to regulators and other authorities with a lawful mandate, ensuring the confidentiality and appropriateness of all shared information.

b) The institution shall:
   i. Ensure timely, accurate and complete submission of reports to the CBN, NFIU and other competent authorities in the required formats and channels.
   ii. Establish internal governance for the review and approval of all regulatory reports, ensuring they are consistent with underlying data, case-management outcomes, and the institution's documented investigative rationale.

5.9 Audit and Governance

a) The AML Solution shall:
    i. maintain a comprehensive, tamper-proof and immutable audit trail of all system and user activities, including configuration changes, access events, alert dispositions, and report generation that can be retrieved without disrupting ongoing operations.
    ii. record and retain key information such as identity of the user, date, timestamp, and nature of activity performed within the system.
    iii. preserve a historical record of all system actions in line with extant laws and regulatory retention periods.
    iv. provide search and retrieval capabilities that enable authorised users to query, review and trace system and user activities end-to-end, to support review by Internal Audit, Compliance, Risk Management, and regulators.
    v. generate automated audit and governance reports to support compliance, substantive testing, operational review, and supervisory inspections.
    vi. support forensic investigation by maintaining verifiable linkages across all relevant data elements including, at a minimum, customer data, transaction data, alerts, user actions, and regulatory returns.
    vii. retrieve audit logs, workflow histories, and transaction trails without disrupting ongoing operations.

b) The institution shall
    i. establish a documented governance framework for the AML Solution, covering roles and responsibilities for ownership, configuration, change management, model validation, access rights and incident handling.
    ii. ensure that access rights, privileges and configuration authorities are appropriately segregated and periodically reviewed.
    iii. subject the AML Solution and its governance framework to periodic review by independent internal audit and, where appropriate, external assurance providers.

iv. ensure that AML/CFT/CPF teams responsible for the operation, configuration, and oversight of the AML Solution receive regular training on system usage, emerging ML/TF/PF typologies, and relevant regulatory developments. Training activities shall be documented and records maintained for supervisory inspection.

5.10 System Integration & Scalability

a) The AML Solution shall:
   i. support secure, bidirectional integration with core banking, customer information/KYC systems and other relevant applications to ensure real-time or near real-time exchange of customer, account and transaction data for monitoring, screening and case management.
   ii. ensure that real-time monitoring and screening processes are not unduly interrupted, impacted or degraded by other system tasks or performance constraints.
   iii. provide well-documented, standards-based Application Programming Interfaces (APIs) or interfaces for integration with internal and where applicable, external systems.
   iv. standardise the format for exchange of data through the API in line with extant regulations.
   v. support consistent, standardised data exchange formats in line with relevant CBN and national requirements.
   vi. offer flexibility to integrate with legacy systems and third-party services, if required.
   vii. be capable of handling increasing transaction volumes, new products, and channels without compromising performance or detection quality.

b) The Institution shall:
   i. deploy AML Solutions that are scalable, maintain data integrity and ensure secure data transmission.
   ii. subject major integration projects and system changes to appropriate testing, change-control, and post-implementation review, including evaluation of impacts on AML/CFT/CPF controls.

c) With prior approval of the CBN, institutions may operate AML Solutions under shared services or other centralised arrangements in line with the provisions of the Guidelines for Shared Services Arrangements for Banks and Other Financial Institutions or any other arrangement acceptable to the CBN. In such cases, responsibilities for compliance, data protection and system performance shall remain clearly allocated and documented.

d) The CBN considers it unacceptable for institutions rated High or Above Average risk within their respective subsectors to operate AML solutions that rely solely on standalone transaction feeds. Such institutions are required to ensure that their AML systems are fully integrated with KYC and KYB repositories, as well as customer risk profiles.

5.11 Security & Data Protection

a) The AML Solution shall:
    i. collect and store data necessary for AML/CFT/CPF compliance in a manner consistent with regulatory requirements.
    ii. implement security controls (including encryption of data at rest, in use and in transit, as appropriate) to protect the confidentiality, integrity, and availability of sensitive data.
    iii. enforce role-based access controls, ensuring users access only the data and functions required for their duties.
    iv. have secure authentication mechanisms, including Multi Factor Authentication (MFA), where appropriate.
    v. support compliance with the Nigeria Data Protection Act (NDPA) and other relevant data protection and data sovereignty regulations and requirements.
    vi. Have defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for AML systems, determined through a comprehensive Business Impact Analysis, and commensurate with the institution's risk profile, size, complexity, and criticality of operations.

b) The institution shall:
    i. ensure that processing and storage of data by the AML Solution comply with Nigerian data sovereignty and privacy laws.

ii. implement appropriate data retention and destruction policies for AML/CFT/CPF data.
iii. assess and manage information security risks arising from the AML Solution as part of the institution's broader cyber and information security framework.

5.12 User Interface & Customisation

a) The AML Solution shall:
   i. provide dashboards and interfaces that support real-time or near real-time visibility of key AML/CFT/CPF metrics, alerts and case management workflows.
   ii. offer a user-friendly interface that facilitates efficient navigation, analysis and decision-making by compliance, monitoring and investigation teams.
   iii. where relevant, support multi-entity, multi-currency and multi-jurisdiction configurations, in line with the institution's group structure and footprint.
   iv. support configuration of workflows, escalation paths, alert filters and other parameters under appropriate governance and change-control.
b) Financial institutions shall
   i. deploy AML Solutions that are appropriately configured to reflect their business models, product portfolios, customer segments and risk profile, and are compliant with all applicable laws and regulations.
   ii. maintain documented processes for reviewing and updating rules, scenarios, thresholds and other configuration settings in response to new risks, products, channels and typologies.

6. OTHER REQUIREMENTS

Financial Institutions shall:

a) maintain a Vendor/Third-Party Management Policy that covers procurement, implementation, support, change management, incident handling and exit strategies for AML Solutions.

b) ensure that third-party providers, including shared service centres and cloud providers, comply with all applicable provisions of these Baseline Standards and relevant CBN regulations.
c) comply with the CBN Risk-Based Cybersecurity Framework, Guidelines for Shared Services and any other applicable regulations relating to operational risks, as it pertains to IT risks, outsourcing and operational resilience.
d) Adhere to ISO 42001 and/or any other such standards in the usage/governance of Artificial Intelligence as applicable to these Baseline Standards.
e) Pending the issuance of dedicated third-party risk management regulations by the CBN, institutions shall apply heightened due diligence to vendors and third-party providers of AML Solutions, including assessment of the provider's ability to support institution-specific configuration, provide access to audit and validation data, and meet the governance requirements of these Baseline Standards. Upon issuance of CBN third-party risk management regulations, those regulations shall apply in addition to and, where more stringent, in substitution of this provision.

7. ENFORCEMENT & IMPLEMENTATION

a) Financial institutions shall comply with these baseline standards within the timelines prescribed by the CBN at the date of issuance of the accompanying circular.
b) Institutions seeking authorisation from the CBN after the date of issuance of these Baseline Standards shall be required to demonstrate compliance with, or a credible plan to achieve compliance with, these Baseline Standards as part of the licensing and authorisation process.
c) The CBN shall monitor and assess compliance through off-site surveillance, on-site examinations, thematic reviews, and any other mechanisms it considers appropriate.
d) Institutions that fail to meet these Baseline Standards, or that operate AML Solutions in a manner that results in ineffective AML/CFT/CPF control, may be subject to 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 (including, but not limited to, BOFIA, the MLPPA, and the CBN AML-CFT-CPF Administrative Sanctions Regulations 2023).

8. GLOSSARY

Term	Definition
Adverse Media Monitoring	Continuous screening of news and open-source content to identify negative information related to customers, beneficial owners, or related parties that may indicate ML/TF/PF risk.
Artificial Intelligence / Machine Learning	Advanced analytics capabilities used by the Solution to detect anomalies, recognise behavioural patterns, score risk, and enable adaptive learning for AML/CFT/CPF monitoring.
Alert	System-generated notification triggered by predefined rules, scenarios, or AI models indicating potentially suspicious or high-risk activity.
Anti-Money Laundering (AML)	Measures and controls designed to prevent, detect, and report money laundering activities within the financial system.
AML Solution	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.
Application Programming Interface (API)	Standardised interface that enables data exchange and integration between AML Solutions and other systems.

Term	Definition
Automated Scenario Calibration (ASC)	Mechanism that adjusts scenarios and thresholds using adaptive learning to optimise analysis and reduce detection errors.
Audit Trail	Tamper-proof and immutable, comprehensive log of system and user activities including user identity, timestamp, and nature of action, preserved for review and investigation.
Beneficial Owner	The natural person(s) identified by the Solution who ultimately owns or controls a customer or on whose behalf a transaction is conducted.
Case	A consolidated record created by the Enterprise Case Management system to manage investigations of alerts and potential breaches.
Clearly Low-Risk Scenario	For the purposes of automated alert closure, a scenario that meets all of the following: (a) generated by a rule approved and documented by the AML governance committee; (b) closure decision relies on both transactional context and current KYC/KYB data; (c) the customer's risk classification is Low and unchanged within the preceding review period; and (d) no prior unresolved alerts or open cases exist for the same customer at the time of closure.
Compliance Reporting	Automated internal and external reports (including regulatory returns) generated by the Solution to evidence compliance activities.
Data Encryption	Security controls ensuring sensitive data is protected at rest and in transit within the Solution.
Enterprise Case Management (ECM)	capability that automates creation, assignment, prioritisation, workflow, and audit trail of cases.
Fraud Monitoring	Real-time and historical analysis to detect patterns across

Term	Definition
	customer, accounts, and channels that has the potential to result in financial and non-financial loss due to deception.
Independent Validation	Validation conducted by a function or party that is organisationally separate from, and has no operational responsibility for, the model or system being validated. For AI/ML models, independent validation shall be performed by a team or individual with no involvement in model development or day-to-day configuration. This may be an internal model risk or internal audit function, or an external third party, provided the validator possesses the requisite technical competence to assess model accuracy, performance drift, fairness, and bias.
Maker-Checker	Role-based control that requires more than one user to complete a workflow / process.
Multi-Factor Authentication (MFA)	Secure authentication mechanism requiring two or more verification factors to access the Solution.
Nigeria Data Protection Act (NDPA)	Law governing data privacy and protection obligations in Nigeria.
Real-Time (for screening)	ability to process and evaluate a customer or transaction against relevant watchlists before the transaction is authorised or onboarding process is considered completed.
Real-Time (for monitoring)	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).
Transaction Monitoring	Surveillance of transactions using scenarios, thresholds, and peer grouping to detect patterns.
User Access	Role-based permissions ensuring users access only

Term	Definition
Controls	data/functions relevant to their roles.
Watchlist	Database of entities that are considered high-risk for predicate offences or other illegal activities.

MARCH 2026

COMPLIANCE DEPARTMENT

CENTRAL BANK OF NIGERIA