CBN 12-Standard Self-Assessment Checklist

Automated AML/CFT/CPF solution readiness guide

For Nigerian financial institutions

Based on CBN Circular BSD/DIR/PUB/LAB/019/002, issued 10 March 2026

Prepared as a Klavent lead magnet for the CBN Baseline Roadmap Sprint

How to use this

Score each standard from 0 to 3 based on evidence, not intent. Use low-scoring areas to prioritise your implementation roadmap and discovery discussion.

Source Facts, Scoring and Roadmap Signal

Grounding document

- Circular: BSD/DIR/PUB/LAB/019/002
- Issued: 10 March 2026
- Audience: Banks, MMOs, IMTOs, OFIs and PSPs
- Roadmap: submit implementation roadmap within 3 months from issuance
- Full compliance: 18 months for DMBs; 24 months for OFIs
- Scope: automated AML/CFT/CPF solutions under CBN regulatory purview

Score each standard

Score	Meaning
0	Not in place or no reliable evidence
1	Partially in place; material gaps remain
2	Mostly in place; evidence or consistency needs work
3	Fully in place, governed, and evidenced

Interpretation bands

0-12
High readiness gap

13-24
Material gaps likely

25-30
Moderate readiness; validate evidence

31-36
Stronger readiness; test governance

Scorecard

Standard	Circle score
1. AML Solution	0 1 2 3
2. CDD, KYC and KYB	0 1 2 3
3. Sanction Lists and PEP Screening	0 1 2 3
4. Risk Assessment	0 1 2 3
5. Transaction Monitoring and Risk-Based Analyses	0 1 2 3
6. Fraud Monitoring and Detection	0 1 2 3
7. Case Management	0 1 2 3
8. Reporting	0 1 2 3
9. Audit and Governance	0 1 2 3
10. System Integration and Scalability	0 1 2 3
11. Security and Data Protection	0 1 2 3
12. User Interface and Customisation	0 1 2 3

Next step

Use the lowest-scoring areas to shape a CBN-ready implementation roadmap and discovery call agenda.

Standards 1-2: Solution Coverage and Customer Data

1 AML Solution

The automated AML/CFT/CPF solution should cover core functional areas, match the institution's size and risk profile, and remain available during outages or migrations.

Self-check questions
[ ] Does the solution cover identification, risk profiling, screening, monitoring, case management, reporting, audit logs, and security controls?
[ ] Is the configuration proportionate to your customer base, products, channels, transaction volume, and documented ML/TF/PF risk profile?
[ ] Are availability, resilience, disaster recovery, and upgrade arrangements evidenced for the AML solution?

Evidence to look for

Solution inventory, architecture map, functional coverage matrix, DR test, change log, risk-profile mapping.

Red flags

Standalone tool with unclear ownership; no DR evidence; no documented coverage map; solution not reviewed when products or channels change.

Section score: 0 1 2 3

2 CDD, KYC and KYB

CDD/KYC/KYB data should connect continuously with risk profiles, transaction data, alert investigation, beneficial ownership review, and onboarding checks such as BVN/NIN where applicable.

Self-check questions
[ ] Can KYC/KYB records, customer risk profiles, and transaction data synchronise continuously into monitoring and screening workflows?
[ ] Can investigators view customer profile, source of funds, geography, transaction history, alerts, and prior cases in one workflow?
[ ] Are beneficial ownership, complex control structures, data-quality controls, and AML-solution notifications to the CBN evidenced?

Evidence to look for

CDD/KYC policy, onboarding workflow, BVN/NIN check logs, beneficial ownership records, sample alert screen, data-quality reports.

Red flags

Customer files are stale; KYC data sits outside monitoring; beneficial ownership is manual and undocumented; no evidence of CBN notification for deployed AML solutions.

Section score: 0 1 2 3

Standards 3-4: Screening and Risk Assessment

3 Sanction Lists and PEP Screening

Screening should cover customers, beneficial owners, related parties, and transactions using domestic and global sanctions/watchlists, PEP lists, adverse media, timely list updates, and interdiction controls.

Self-check questions
[ ] Are customers, beneficial owners, related parties, and transactions screened against relevant domestic and global sanctions and watchlists?
[ ] Does matching logic handle name variations and similar names, with transparent configuration and validation?
[ ] Are list updates, internal watchlists, PEP flags, adverse media checks, hit resolution, and transaction holds logged and evidenced?

Evidence to look for

List provider records, update logs, screening configuration, hit-resolution SOP, sample alerts, interdiction evidence.

Red flags

Periodic-only screening; no update logs; hits closed without rationale; PEP checks limited to onboarding; confirmed matches cannot block onboarding or transactions.

Section score: 0 1 2 3

4 Risk Assessment

The solution should reflect documented risk appetite and risk assessment, dynamically adjust customer risk, aggregate enterprise-level ML/TF/PF risk, and govern AI/ML models where used.

Self-check questions
[ ] Are rules, scenarios, thresholds, and customer risk ratings configured against the institution's documented risk appetite and risk assessment?
[ ] Can customer risk profiles change dynamically based on new data, behavioural change, and credible external risk factors?
[ ] Are enterprise and business-line risk assessments retained with evidence of resulting changes to scenarios, thresholds, or controls?

Evidence to look for

Risk assessment report, risk appetite statement, scenario-threshold register, customer risk-change reports, AI/ML governance records.

Red flags

Risk ratings never refresh; risk appetite is not linked to system rules; external risk signals are ignored; scenario changes lack approval evidence.

Section score: 0 1 2 3

Standards 5-6: Monitoring, Analytics and Fraud

5 Transaction Monitoring and Risk-Based Analyses

Monitoring should use documented scenarios, customer context, segmentation, peer grouping, explainable alerts, SLAs, tuning evidence, and independent validation for AI/ML where used.

Self-check questions
[ ] Do monitoring scenarios use CDD/KYC/KYB attributes, customer behaviour, segment, product, geography, channel, and raw transaction patterns?
[ ] Can each alert show the customer's key profile, risk score, recent behaviour, previous alerts, and case history for human review?
[ ] Are false-positive/false-negative thresholds, scenario tuning, alert-review SLAs, and automated-closure governance documented and reviewed?

Evidence to look for

Scenario register, threshold rationale, tuning log, alert queue, SLA report, validation report, model-change approvals.

Red flags

Raw transaction rules only; no threshold rationale; no ageing report; automated closures without governance or CBN notification where required.

Section score: 0 1 2 3

6 Fraud Monitoring and Detection

Where fraud monitoring is in scope, controls should detect fraud across relevant channels, update fraud rules, share risk signals with AML/CFT/CPF workflows, and preserve segregation of responsibilities.

Self-check questions
[ ] Are card, e-channel, deposit, lending, and other relevant activities monitored in real time or near real time according to fraud risk?
[ ] Can fraud rules or models be updated based on observed incidents and trends across customers, accounts, and channels?
[ ] Do AML and fraud workflows exchange risk signals while preserving clear responsibilities, traceability, and control ownership?

Evidence to look for

Fraud rule register, incident trend reports, workflow map, risk-signal integration evidence, loss-event analysis.

Red flags

Fraud signals never affect ML/TF/PF risk; AML and fraud teams work from disconnected queues; no trend analysis; no channel-specific response timing.

Section score: 0 1 2 3

Standards 7-8: Case Management and Reporting

7 Case Management

Enterprise case management should create, assign, prioritise, track, escalate, and evidence alert investigations with maker-checker controls and complete audit trails.

Self-check questions
[ ] Does the case workflow automatically create, assign, prioritise, and track alerts and investigations across AML/CFT/CPF and relevant fraud cases?
[ ] Are maker-checker review, escalation paths, timestamps, users, decisions, and supporting rationale captured in the case record?
[ ] Are case volumes, ageing, outcomes, trends, and closed-case lessons reviewed for management oversight and scenario tuning?

Evidence to look for

Case workflow screenshots, maker-checker logs, ageing report, closure rationale samples, trend-analysis report.

Red flags

Investigations live in email and spreadsheets; no ageing view; closed cases are not analysed; escalation criteria are informal.

Section score: 0 1 2 3

8 Reporting

The solution should support regulatory and internal reporting, including STR/SAR/CTR/FTR where applicable, management information, lawful external reporting, and approval governance.

Self-check questions
[ ] Can the solution generate regulatory reports such as STR, SAR, CTR, FTR, and other AML/CFT/CPF returns in required formats and schedules?
[ ] Is internal MI produced for the Chief Compliance Officer, senior management, Executive Compliance Officer, and Board oversight?
[ ] Are regulatory reports reviewed and approved against underlying data, case outcomes, and documented investigation rationale?

Evidence to look for

Report templates, filing logs, MI packs, approval records, case-to-report reconciliation, reporting calendar.

Red flags

Reports are manually rebuilt from extracts; no approval trail; board MI lacks monitoring effectiveness; filings cannot be traced to case rationale.

Section score: 0 1 2 3

Standards 9-10: Governance and Integration

9 Audit and Governance

The AML solution should maintain immutable audit trails, governance over ownership and configuration, access-right segregation, model validation, incident handling, audit review, and training records.

Self-check questions
[ ] Are system and user activities, configuration changes, access events, alert dispositions, and report generation captured in tamper-resistant audit trails?
[ ] Can audit logs, workflow histories, and transaction trails be retrieved without disrupting operations?
[ ] Are ownership, configuration, change management, model validation, access rights, incident handling, independent review, and training records documented?

Evidence to look for

Governance framework, access review, audit-log sample, configuration-change log, internal audit report, training register.

Red flags

Shared admin accounts; logs are overwritten or hard to retrieve; no access review; configuration changes bypass approval; staff training not evidenced.

Section score: 0 1 2 3

10 System Integration and Scalability

AML solutions should integrate securely and bidirectionally with core banking, customer/KYC systems, and relevant applications, while supporting growth, legacy integration, testing, and change control.

Self-check questions
[ ] Is there secure bidirectional integration with core banking, customer information, KYC/KYB repositories, and relevant applications?
[ ] Are APIs or interfaces documented, standardised, tested, and governed through change control and post-implementation review?
[ ] Can the solution handle increasing transaction volumes, new products, and new channels without degrading monitoring or screening quality?

Evidence to look for

Architecture diagram, API documentation, data-flow map, integration test results, performance report, change-control records.

Red flags

High-risk institution relies only on standalone transaction feeds; monitoring fails during batch delays; APIs undocumented; scalability not tested.

Section score: 0 1 2 3

Standards 11-12: Security, Data and Usability

11 Security and Data Protection

Sensitive AML/CFT/CPF data should be collected and protected according to regulatory need, data protection law, data sovereignty expectations, access controls, MFA, retention, and resilience planning.

Self-check questions
[ ] Are sensitive AML/CFT/CPF data protected with appropriate controls for confidentiality, integrity, availability, encryption, access, and authentication?
[ ] Do role-based access controls and MFA limit users to data and functions required for their duties?
[ ] Are NDPA, data sovereignty, retention, destruction, RTO, and RPO requirements documented and evidenced through BIA and operational controls?

Evidence to look for

Security design, access matrix, MFA evidence, BIA, RTO/RPO records, retention schedule, NDPA compliance artefacts.

Red flags

Broad user access; no MFA; retention rules unclear; sensitive data exported without control; RTO/RPO not linked to business impact.

Section score: 0 1 2 3

12 User Interface and Customisation

Dashboards and interfaces should support effective compliance work, visibility of key metrics, case workflows, configurable escalation paths, filters, and rules under governance.

Self-check questions
[ ] Do dashboards show key AML/CFT/CPF metrics, alerts, case workflow status, and near real-time visibility where relevant?
[ ] Can compliance, monitoring, and investigation teams navigate efficiently and make decisions without stitching evidence across many tools?
[ ] Are workflows, escalation paths, alert filters, rules, scenarios, thresholds, and configuration updates governed and reviewed?

Evidence to look for

Dashboard screenshots, workflow configuration, change approvals, user feedback, rules review log, escalation matrix.

Red flags

Critical metrics are not visible; investigators rely on manual extracts; workflow changes bypass governance; interface does not fit business model.

Section score: 0 1 2 3

Turn your score into a roadmap

If any section scores 0 or 1, use the Klavent CBN Baseline Roadmap Sprint to convert gaps into a board-ready implementation plan.

klavent.co