



CBN Automated AML Solutions Baseline Standards

A New Era of Financial Crime
Compliance in Nigeria

home.kpmg/ng



Introduction

Source and interpretation note: This article is based on KPMG's interpretation of the Central Bank of Nigeria's Baseline Standards for Automated Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing Solutions, issued on 10 March 2026. Readers should refer to the official CBN publication for the full regulatory text and detailed compliance obligations.

The Central Bank of Nigeria's (CBN) **Baseline Standards for Automated Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) Solutions ("the Standards")**, issued on 10 March 2026, introduce a significant development in the evolution of financial crime compliance in Nigeria's financial services sector.

In KPMG's view, the Standards go beyond a narrow technology requirement and point to a broader supervisory expectation that financial institutions should manage financial crime risk through more structured, automated and evidence-based control environments.

Viewed through this lens, the Standards represent an important regulatory technology reform. They indicate a movement away from heavily manual, fragmented and reactive approaches to financial crime compliance towards operating models that are more automated, integrated, risk-based and capable of producing demonstrable compliance outcomes. For financial institutions, this raises the minimum level of capability expected to support an effective AML/CFT/CPF programme.

This shift reflects broader global trends. Across leading financial centers, regulators increasingly expect financial institutions to leverage Artificial Intelligence (AI), Machine Learning (ML), advanced analytics and real-time data processing capabilities to strengthen their ability to identify, assess and respond to evolving financial crime threats. These technologies are transforming how institutions conduct customer due diligence, perform sanctions and politically exposed person (PEP) screening, monitor transactions, identify suspicious activities and fulfil regulatory reporting obligations. The Standards align Nigeria with this international direction of travel and underscore the regulator's determination to enhance the resilience, transparency and integrity of the country's financial system.

Strategically, the Standards should not be viewed as a technology initiative or a compliance exercise alone. Rather, they represent a fundamental transformation of the AML/CFT/CPF operating model. By mandating the deployment of automated solutions supported by AI, ML and advanced analytics, the CBN is placing increased emphasis on data quality, system interoperability, risk intelligence, governance effectiveness and demonstrable compliance outcomes. At their core, financial institutions will be expected not only to implement technology solutions but also to validate their effectiveness and demonstrate that they are producing meaningful risk management and regulatory compliance outcomes.

Consequently, the implementation of the Standards will require institutions to look beyond technology procurement and undertake a broader program of transformation encompassing governance, data management, operating model redesign, workforce capabilities, third-party risk management and compliance effectiveness. For boards and senior executives, the key question is no longer whether to automate AML processes, but whether their institution possesses the technological maturity, data infrastructure and governance framework necessary to meet a new generation of regulatory expectations.



Requirements of the Standards

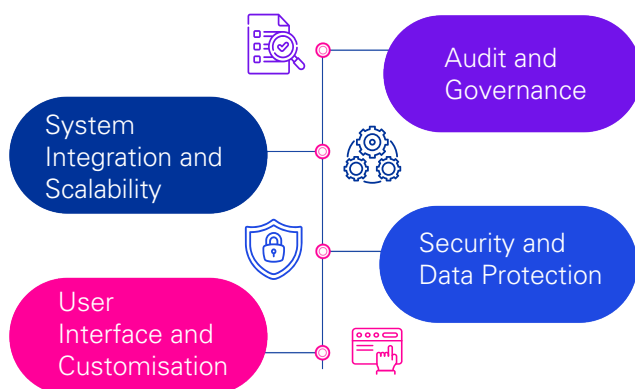
01

Based on our reading of the Standards, financial institutions will need to implement, validate and provide evidence of the effectiveness of automated AML/CFT/CPF solutions across several core areas, including:

Core Financial Crime Capabilities

- Customer Identification and Verification (Know your customer (KYC), Know your business (KYB), Customer due diligence (CDD) and Enhanced due diligence (EDD))
- Sanctions List and PEP Screening
- Risk Assessment
- Transaction Monitoring and Risk-Based Analysis
- Fraud Monitoring and Detection
- Case Management
- Regulatory Reporting

Foundational Technology and Governance Capabilities



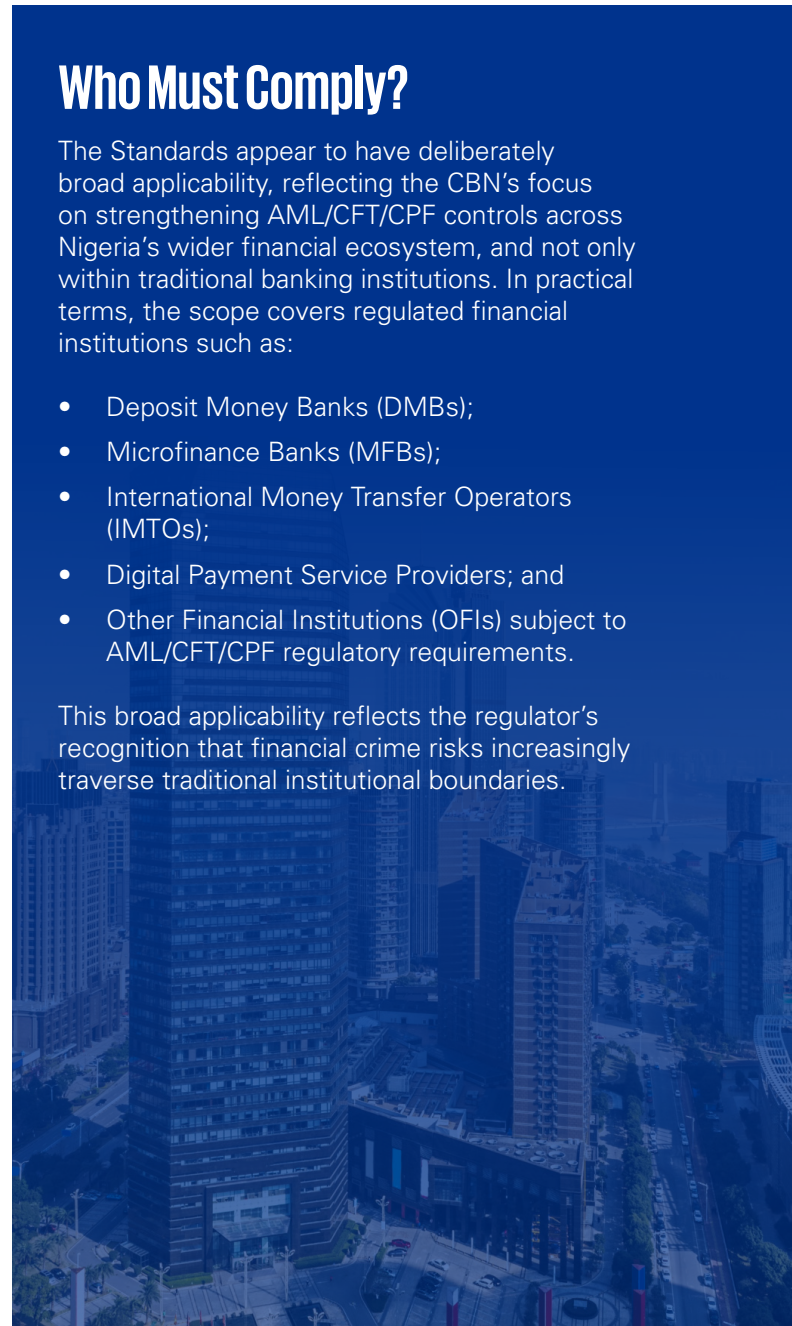
Taken together, these capability areas suggest a regulatory preference for integrated, intelligence-driven and risk-based financial crime management frameworks, rather than isolated point solutions or standalone compliance tools.

Who Must Comply?

The Standards appear to have deliberately broad applicability, reflecting the CBN's focus on strengthening AML/CFT/CPF controls across Nigeria's wider financial ecosystem, and not only within traditional banking institutions. In practical terms, the scope covers regulated financial institutions such as:

- Deposit Money Banks (DMBs);
- Microfinance Banks (MFBs);
- International Money Transfer Operators (IMTOs);
- Digital Payment Service Providers; and
- Other Financial Institutions (OFIs) subject to AML/CFT/CPF regulatory requirements.

This broad applicability reflects the regulator's recognition that financial crime risks increasingly traverse traditional institutional boundaries.



Key Regulatory Milestones: Why Time Is Already Running

02

With the roadmap submission deadline of 10 June 2026 now elapsed, the implementation phase has commenced. The focus for financial institutions should no longer be planning, but execution, integration, testing, validation and demonstrating effectiveness.

Deployment Deadline for DMBs – 10 September 2027

DMBs are required to complete the deployment, integration, and testing of AML/CFT/CPF solutions in line with the Standards within an 18-month implementation period.

Deployment Deadline for OFIs – 10 March 2028

OFIs are required to complete the deployment, integration, and testing of AML/CFT/CPF solutions within a 24-month implementation period.

At first glance, these timelines may appear generous. However, institutions that view compliance as a technology procurement exercise risk underestimating the scale of transformation required. Experience from AML maturity assessments and financial crime transformation programs across the industry suggests that the greatest implementation challenge is often not the acquisition of a solution but ensuring that the solution operates effectively within the broader enterprise ecosystem.

Previous Practice (Old) vs. The Standards (New)



From: Fragmented & Manual

Periodic • Siloed • Reactive



To: Integrated & Intelligence-LED

Continuous • Risk-based • Proactive

Capability Area

Previous Practice (Old)

The Standards (New)

1

KYC/KYB/
CDD/EDD



- Customer onboarding and due diligence largely performed manually or through systems operating in isolation.
- CDD reviews driven by calendar rather than risk events.
- KYC data rarely synchronised with transaction monitoring in real time



- Automated and integrated customer identification and verification, including linkages with relevant identity data sources where applicable.
- KYC, KYB, CDD and EDD operate as part of a continuous risk-informed process, with investigators able to consider customer profile, risk classification and transaction activity together during alert review.

Note: The comparison above reflects KPMG's interpretation of the practical shift implied by the Standards. It is intended as an explanatory guide and should be read alongside the official CBN publication.



From: Fragmented & Manual

Periodic • Siloed • Reactive



To: Integrated & Intelligence-LED

Continuous • Risk-based • Proactive

Capability Area

Previous Practice (Old)

The Standards (New)

2

Sanctions & PEP Screening



- Periodic or batch-based screening performed through standalone applications, with significant lag between list updates and screening refresh, Adverse media monitoring largely absent or conducted manually.



- Continuous or near real-time screening against relevant sanctions, PEP and adverse media sources, embedded across the customer lifecycle from onboarding through ongoing monitoring.
- Institutions must maintain sufficient screening records to demonstrate timely updates, review activity and control effectiveness review.

3

Customer Risk Assessment



- Risk ratings assigned at onboarding and updated through infrequent periodic reviews, often disconnected from the customer's actual transactional behavior or emerging risk signals.



- The Standards indicate a move towards dynamic customer risk profiling, where ratings are refreshed in response to changes in customer information, transaction behaviour and external risk indicators.
- AI or ML models support risk scoring, institutions must maintain appropriate governance, human oversight, explainability and independent validation.

4

Transaction Monitoring & Risk Analytics



- Predominantly rules-based monitoring conducted in batch cycles, with limited or no data integration across transaction channels.
- Mobile, unstructured supplementary service data (USDD), point of sale (POS), and card transactions frequently absent from or inconsistently present in monitoring environments. Alerts assessed without reference to customer KYC context.



- Integrated monitoring across relevant transaction channels, using risk-based detection logic and, where appropriate, advanced analytics or AI/ML capabilities.
- For higher-risk institutions, transaction monitoring is expected to be connected to broader customer and risk data rather than operating only from isolated transaction feeds.

5

Fraud Monitoring



- Fraud monitoring typically operated independently from AML processes and supporting systems.



- Enterprise-wide financial crime management with fraud intelligence integrated into AML monitoring, investigations and decisioning.

Note: The comparison above reflects KPMG's interpretation of the practical shift implied by the Standards. It is intended as an explanatory guide and should be read alongside the official CBN publication.



From: Fragmented & Manual

Periodic • Siloed • Reactive



To: Integrated & Intelligence-LED

Continuous • Risk-based • Proactive



Capability Area

Previous Practice (Old)

The Standards (New)

6

Case Management



- Investigations managed through manual processes, excel trackers, email correspondence, or fragmented workflow tools with no structured audit trail, inconsistent escalation, and limited management visibility of case volumes, trends, or outcomes.



- The Standards require structured case management capabilities that support streamlined case creation, assignment, review and escalation.
- Institutions should be able to evidence role-based workflows, maker-checker controls, audit trails, management reporting and clear documentation of investigative decisions.

7

Regulatory Reporting



- Significant reliance on manual data aggregation for suspicious transaction report (STR), currency transaction report (CTR), and foreign transaction report (FTR) preparation, with limited traceability between underlying data, investigation outcomes, and submitted reports.



- Automated regulatory reporting supported by integrated data sources, traceable workflows and defensible audit evidence.

8

Audit Trails & Explainability



- Audit system records maintained inconsistently across systems with varying views of traceability.
- Inability of compliance teams to explain the models generating the alerts and/or how the system works.



- Institutions should maintain comprehensive and reliable audit trails across the AML architecture including configuration changes, screening decisions, alert outcomes, case actions and regulatory report generation.
- Where AML contributes to decisions or alert outcomes, institutions should retain auditable information that explains key drivers and supports human review, regulatory inspection and independent assurance.

9

System Integration & Enterprise view



- AML capabilities distributed across multiple disconnected systems and data sources with no consolidated view of customer risk across products, channels, and entities.



- Continuous, bidirectional integration across core banking, KYC/KYB, transaction channels, screening, banking, CRM, R&D, transaction channels, sales and case management systems – providing a consolidated, real-time or near-real-time view of customer risk across all relevant data sources.

Note: The comparison above reflects KPMG's interpretation of the practical shift implied by the Standards. It is intended as an explanatory guide and should be read alongside the official CBN publication.



From: Fragmented & Manual

Periodic • Siloed • Reactive



To: Integrated & Intelligence-LED

Continuous • Risk-based • Proactive

Capability Area

Previous Practice (Old)

The Standards (New)

10

Security & Data Protection



- Security controls implemented primarily at individual application level with inconsistent encryption standards, limited multi-factor authentication for AML system access, and data protection compliance not systematically embedded in AML operations.



- Security, privacy and data protection should be embedded into the AML control environment.
- This includes appropriate encryption, access controls, multi-factor authentication, resilience planning, backup policies and clear data retention with applicable Nigerian data protection and CBN data requirements.

11

Governance and Oversight



- Governance focused primarily on regulatory compliance and policy oversight.



- Clearly defined accountability, model governance, active monitoring, and independent validation and continuous effectiveness monitoring

12

Technology Deployment



- Manual, semi-automated or fragmented solutions commonly accepted.



- Integrated, automated and scalable AML solutions expected, proportionate to the institution's size complexity and risk profile.
- In practical terms, institutions should not assume that manual or fragmented processes will be sufficient to meet the level of automation and demonstrate effectiveness contemplated by the Standards.

Note

The comparison above reflects KPMG's interpretation of the practical shift implied by the Standards. It is intended as an explanatory guide and should be read alongside the official CBN publication.

Practical Implications: The Focus Has Shifted from Planning to Execution

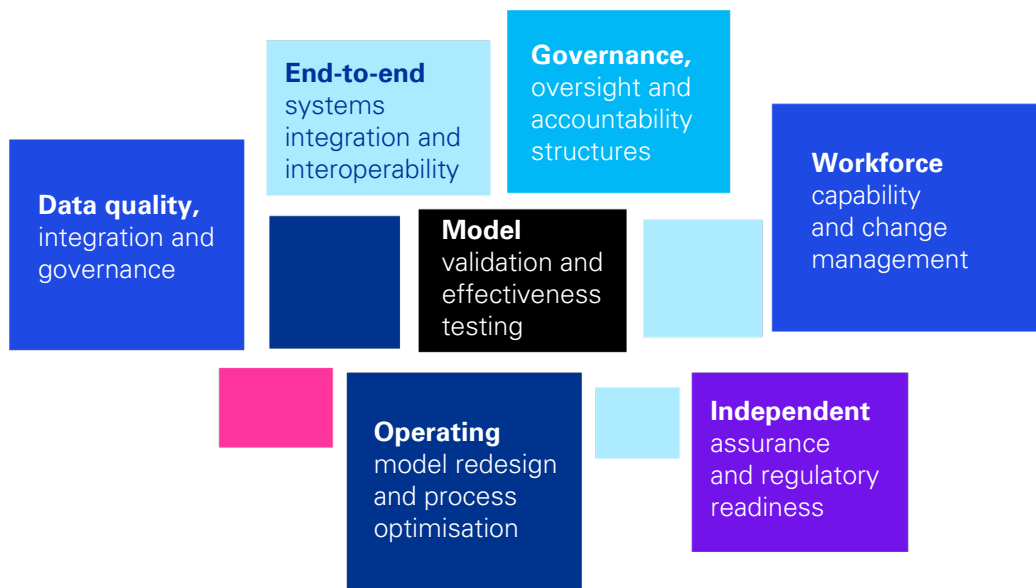
03

With the implementation roadmap submission deadline of 10 June 2026 now elapsed, financial institutions should be shifting their attention from planning and solution selection towards execution, integration, testing, validation and demonstrable effectiveness.

In practical terms, regulatory scrutiny is likely to extend beyond whether an institution has procured or deployed an AML solution. Increasingly, the focus will be on whether the institution can demonstrate that the solution operates effectively within its control environment, supports risk-based decision-making, and produces defensible compliance outcomes.

This distinction is important. The greatest implementation risk may be treating the Standards as a software acquisition exercise rather than a broader AML/CFT/CPF transformation programme.

Successful implementation will require financial institutions to address multiple interdependent components, including:



Institutions that focus solely on technology deployment may achieve implementation milestones but struggle to demonstrate the effectiveness, governance and integration required to satisfy regulatory expectations. Conversely, institutions that approach implementation as an enterprise-wide transformation initiative will be better positioned to achieve sustainable compliance and improved financial crime risk management outcomes.



Key Implementation Challenges Institutions Must Address

04

The implementation of the Standards represents a significant transformation program for financial institutions. Based on our experience supporting AML technology assessments, system implementations, model validations, and regulatory compliance reviews, achieving compliance extends well beyond technology acquisition. Institutions must address foundational challenges across data, governance, operating models, talent, and assurance to realize the full value of their AML investments and meet evolving regulatory expectations.

The following implementation challenges are likely to require strategic focus from financial institutions:

Data Quality and Accessibility

- Data remains the single most critical enabler of effective automated AML monitoring. Many institutions continue to operate with fragmented, incomplete, inconsistent, or outdated customer and transactional data, which can significantly undermine the accuracy of customer risk assessments, transaction monitoring scenarios, sanctions screening, and regulatory reporting.
- Addressing these challenges will require comprehensive KYC remediation programs, stronger data governance frameworks, and enhanced controls over customer and transactional data lifecycle management. Institutions may also benefit from industry-wide collaboration through secure shared KYC utilities and trusted data-sharing frameworks, which could reduce remediation costs, improve data consistency, and support more effective customer due diligence across the financial ecosystem.

Vendor Dependency and Solution Assurance

- Some institutions place significant reliance on vendor representations of compliance. However, institutions are often challenged with independently validating that implemented solutions operate effectively and meet regulatory requirements within their specific business and technology environments.
- The Standards will require institutions to develop stronger internal capabilities to understand, validate, challenge, and continuously monitor the effectiveness of AML models, detection scenarios, risk-scoring methodologies, and system configurations. Independent model validation, periodic effectiveness reviews, and robust governance over model changes will become increasingly important to demonstrate compliance and maintain regulatory confidence.

Limited Technical and Financial Crime Expertise

- The effective implementation and operation of modern AML solutions require a multidisciplinary workforce comprising financial crime specialists, data analysts, technology professionals, model validation experts, and compliance practitioners. However, many institutions continue to face challenges attracting, developing, and retaining these specialised skill sets.
- To address this gap, financial institutions may need to rethink their financial crime operating models, establish dedicated AML technology and analytics functions, and invest in continuous capability development program. The ability to integrate compliance expertise with advanced analytics and technology capabilities will increasingly differentiate leading institutions from those pursuing a purely compliance-driven approach.

Legacy System Fragmentation

- Many Financial Institutions operating multiple AML, fraud, KYC, payments, and customer systems that were implemented independently over time. These systems often function in silos, creating challenges in obtaining a unified view of customer activity and financial crime risks.
- Overcoming this fragmentation may require significant investment in enterprise-wide data integration, modern architecture design, API-enabled connectivity, and intelligent data platforms.

Data Privacy and Cybersecurity

- As institutions increasingly integrate data across platforms and leverage third-party technologies to meet regulatory requirements, the importance of cybersecurity, data privacy, and third-party risk management continues to grow.
- Institutions will therefore need to strengthen cybersecurity controls, enhance data governance frameworks, ensure compliance with applicable data protection regulations, and establish robust oversight of third-party service providers. Effective management of these risks will be critical to maintaining regulatory compliance, customer trust, and operational resilience.



How Institutions Will Demonstrate Effective Implementation

05



Based on the Standards, Guidance Note and Implementation Roadmap requirements, institutions will likely be expected to demonstrate:

- **Seamless integration and interoperability** across customer onboarding, transaction monitoring, sanctions screening, fraud management, case management, and regulatory reporting systems.
- **A comprehensive and consolidated customer risk view**, supported by accurate, complete, and timely customer and transactional data.
- **Robust governance frameworks**, with clearly defined ownership, accountability, escalation protocols, and Board and management oversight.
- **Effective model governance**, including independent model validation, periodic review, performance testing, and controlled change management processes.
- **Transparent and auditable decision-making**, supported by comprehensive audit trails, system logs, and explainable monitoring outcomes.
- **Effective transaction monitoring and sanctions screening capabilities**, capable of identifying suspicious activities, sanctions exposure, and emerging financial crime risks.
- **Ongoing testing, validation, and performance monitoring**, including scenario tuning, alert quality assessments, and effectiveness reviews.
- **Demonstrable improvements in financial crime risk management outcomes**, including detection rates, alert quality, investigation effectiveness, suspicious transaction reporting, and regulatory reporting accuracy.

Ultimately, compliance will extend beyond solution implementation to an institution's ability to evidence operational effectiveness, regulatory defensibility, governance maturity, and sustainable programme oversight.

Potential Consequences of Delayed or Ineffective Implementation

06

Financial institutions that do not achieve compliance within prescribed timelines, or whose implementations fail to meet regulatory expectations, may face heightened supervisory attention and regulatory intervention.

Potential consequences may include:

- ✓ Regulatory findings, sanctions, monetary penalties, or enforcement actions.
- ✓ Mandatory remediation programs and heightened reporting requirements.
- ✓ Increased exposure to money laundering, terrorist financing, proliferation financing, fraud, and related financial crime risks with the potential downstream impact:
 - Reputational damage that may affect customer confidence, investor trust, and market perception.
 - Significant financial losses arising from regulatory breaches, remediation costs, and control failures.
- ✓ Operational inefficiencies arising from ineffective monitoring, excessive false positives, and fragmented compliance processes.
- ✓ In severe cases, restrictions on business activities, licence suspension, or other regulatory measures.



Mitigating Implementation Risk

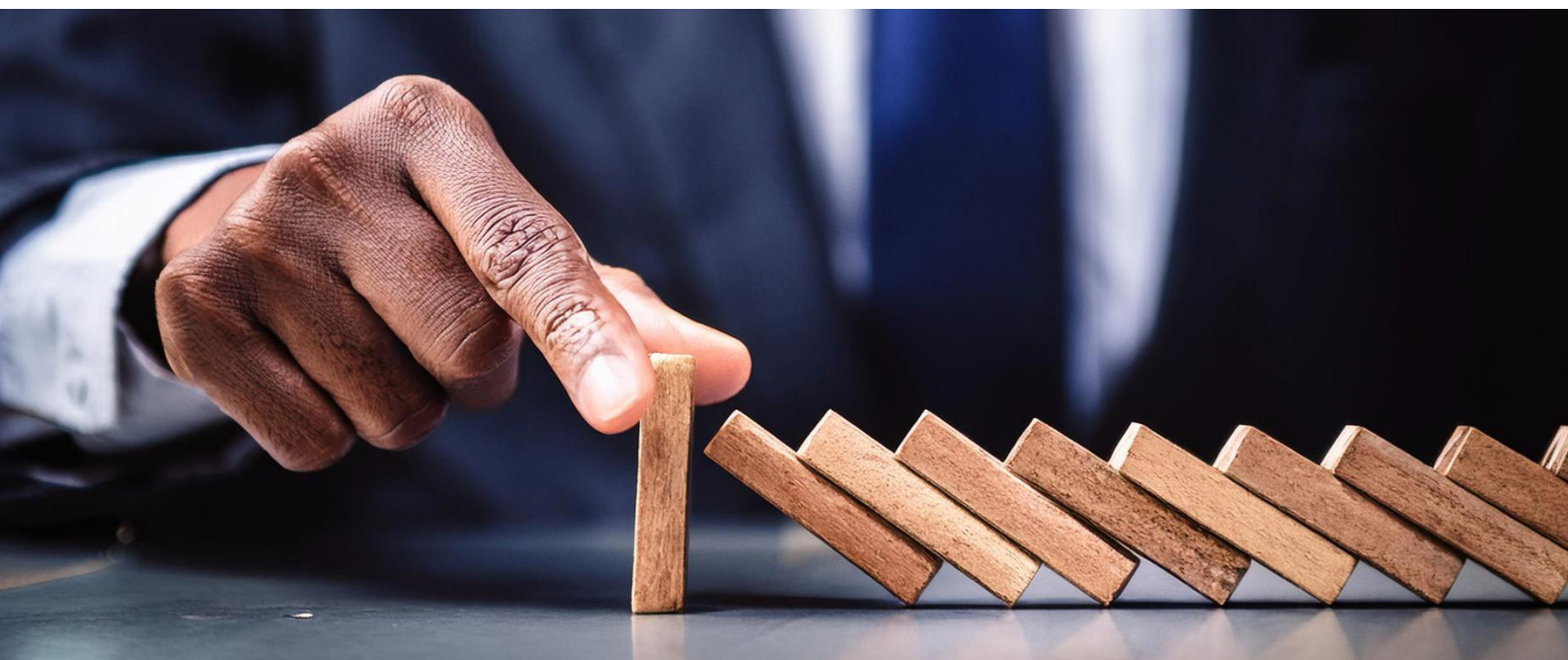
07

Given the scale and complexity of the transformation required, financial institutions should adopt a structured and enterprise-wide approach to implementation. Success will depend on strong governance, effective programs management, and a clear focus on operational effectiveness.

To improve the likelihood of successful implementation, financial institutions should consider:

- Conducting comprehensive gap assessments and developing a clear implementation roadmap aligned with regulatory milestones.
- Prioritizing data quality, KYC remediation, and enterprise-wide data integration initiatives.
- Strengthening governance structures, including clear ownership of AML models, systems, and data assets.
- Implementing independent quality assurance, testing, and validation throughout the implementation lifecycle.
- Validating transaction monitoring scenarios, risk-scoring methodologies, sanctions screening configurations, and model assumptions before deployment.
- Strengthening vendor oversight and implementing robust challenge and assurance processes over third-party solutions.
- Investing in specialist AML, technology, data analytics, and model governance capabilities.
- Conducting regulatory readiness assessments and independent effectiveness reviews prior to implementation deadlines.
- Establishing ongoing monitoring, reporting, and continuous improvement mechanisms to ensure sustained compliance.

Perhaps the greatest implementation risk is viewing the CBN Automated AML Solutions Baseline Standards as a technology procurement exercise rather than an enterprise-wide transformation program. While technology is a critical enabler, sustainable compliance will require institutions to address the broader ecosystem of **data, governance, operating models, talent, controls, assurance, and regulatory oversight**.



Conclusion



- The Standards represent far more than a technology compliance exercise. They signal the transition towards a more data-driven, intelligence-led, and technology-enabled financial crime management framework for Nigeria's financial services sector.
- Based on our experience across AML transformation programs and regulatory reviews, institutions that focus solely on procuring AML software may achieve technical deployment but are unlikely to realise the level of operational effectiveness, governance maturity, and regulatory assurance envisioned by the Standards. Sustainable compliance will require a broader transformation agenda encompassing data quality, governance, talent, operating model redesign, technology integration, and independent assurance.
- Conversely, institutions that approach compliance through an integrated transformation agenda, combining data, technology, governance, analytics and independent assurance, will be better positioned to comply with regulatory expectations while improving operational efficiency, strengthening customer intelligence and enhancing financial crime risk management capabilities.
- More importantly, institutions that approach implementation strategically will unlock value beyond compliance. The capabilities developed to support enhanced customer due diligence, risk profiling, transaction analytics, and data governance can create a robust enterprise intelligence platform that supports improved customer insight, better risk management, operational efficiency, and informed business decision-making.
- Ultimately, the institutions most likely to succeed will be those that leverage implementation as an opportunity to modernize their financial crime capabilities, strengthen customer intelligence, enhance operational resilience, and build a data-driven compliance framework that delivers value beyond regulatory compliance. In doing so, they will not only meet regulatory expectations but also position themselves for stronger risk management, improved operational performance, and long-term competitive advantage.

How KPMG Can Assist

At KPMG, we have extensive experience supporting financial institutions with AML/CFT/CPF transformation, regulatory compliance, and financial crime technology initiatives. We can assist your institution in the following areas:



Implementation Project Management / Quality Assurance

KPMG will assist you by providing project management, governance oversight, and implementation quality assurance throughout the AML solution implementation lifecycle. We will help ensure that implementation activities remain aligned with regulatory requirements, project objectives, timelines, and business expectations.



AML Data Lakehouse & Customer 360 Transformation

KPMG will assist you by designing and implementing an enterprise-wide data foundation that supports Customer 360 capabilities, financial crime monitoring, regulatory reporting, and compliance with the Standards.



Independent Validation, Testing & Regulatory Readiness

KPMG will assist you by independently validating AML solutions, models, scenarios, and control frameworks to assess their effectiveness and compliance with regulatory expectations. We will perform testing and readiness assessments to help ensure that implemented capabilities operate as intended and are audit- and regulator-ready.



Independent Assessment of AML/CFT/CPF Program

KPMG will assist you by conducting independent assessments of your AML/CFT/CPF program, including governance, policies, procedures, risk assessments, monitoring controls, and technology capabilities. We will identify gaps, benchmark current practices against regulatory expectations and leading practices, and provide actionable recommendations for improvement.



KYC remediation

KPMG can support your KYC remediation exercise through rigorous project management and an efficient risk-based approach to the exercise.



Data Privacy, Cybersecurity and Third-Party Risk Management

KPMG can help institutions:

- Assess cybersecurity risks within AML ecosystems.
- Strengthen data governance and privacy frameworks.
- Conduct third-party risk assessments of AML vendors.
- Review cloud security and data protection controls.
- Establish governance frameworks for data sharing and AI usage.
- Assess compliance with applicable data protection requirements.

Contact Us



Saheed Olawuyi

Partner and Head,
Forensic Services

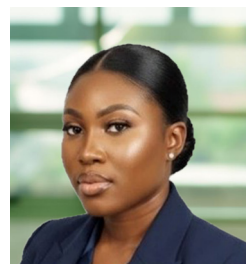
E: Saheed.Olawuyi@ng.kpmg.com



Oluwaseun Odeku

Partner,
Forensic Services

E: Oluwaseun.Odeku@ng.kpmg.com



Folasade Olanrewaju

Manager,
Forensic Services

E: Folasade.Olanrewaju@ng.kpmg.com



home.kpmg/ng
home.kpmg/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG Advisory Services, a partnership registered in Nigeria and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.