



Central Bank of Nigeria

Compliance Department
Plot 33, Abubakar Tafawa Balewa Way,
Central Business District, P.M.B. 0187, Garki Abuja
Telephone:
Email: cmd@cbn.gov.ng
Website: www.cbn.gov.ng

CMD/DIR/PUB/CIR/001006

March 31, 2026

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

IMPLEMENTATION OF THE BASELINE STANDARDS FOR AUTOMATED AML/CFT/CPF SOLUTIONS

The Central Bank of Nigeria (CBN) recently issued the Baseline Standards for Automated AML/CFT/CPF Solutions (the “Baseline Standards”) to strengthen the effectiveness, governance, and integration of AML/CFT/CPF control frameworks across financial institutions.

Following this issuance, the CBN has observed increased industry engagement, including commentary and representations from technology service providers regarding alignment with the Baseline Standards.

While this reflects positive responsiveness, there is a growing risk of misinterpretation of regulatory expectations, particularly where compliance is framed primarily in terms of system features, vendor capabilities, or technology solutions.

1. Issuance of Guidance Note

To ensure clarity and consistency in implementation, the CBN has issued a Guidance Note on the Implementation of the Baseline Standards (the “Guidance Note”), which is attached to this letter.

The Guidance Note:

- clarifies the CBN’s expectations



- reinforces that compliance is assessed at the level of the financial institution
- addresses key areas of potential misinterpretation

The Guidance Note should be read together with the Baseline Standards and does not replace or supersede the requirements set out therein.

2. Implementation Requirement

Financial institutions are required to implement the Baseline Standards in full, taking into account their size, complexity, and risk profile.

In line with this requirement, all financial institutions are required to submit an implementation plan outlining how they will achieve compliance with the Baseline Standards.

Implementation plans must comprehensively address all requirements set out in the Baseline Standards.

3. Submission of Implementation Plan

The implementation plan must:

- cover all requirements set out in the Baseline Standards
- clearly identify current state, target state, and actions required
- include defined timelines, ownership, and governance arrangements
- demonstrate how effectiveness, integration, and defensibility will be achieved

The implementation plan must be submitted in accordance with the CBN Implementation Plan Template attached. An editable version of the template (in Microsoft Word format) will be provided to facilitate completion.

The template sets out the minimum information required. Financial institutions may provide additional relevant information where necessary, provided that such information is clearly structured and does not replace the required format.

4. Submission Timeline

All financial institutions are required to submit their implementation plans within three (3) months of the issuance of the Baseline Standards i.e., **June 10, 2026**. Submissions should be made electronically in both editable (Word) and final (PDF) formats.



5. Supervisory Assessment

Submissions will form the basis for supervisory review and engagement.

The CBN will assess:

- the adequacy of implementation approaches
- the robustness of governance arrangements
- the effectiveness and integration of proposed solutions

Incomplete, inconsistent, or unsupported submissions may attract supervisory action.

6. Further Engagement

The CBN will continue to engage with financial institutions as necessary to support effective implementation and ensure alignment with regulatory expectations.

Please ensure that this directive is brought to the attention of relevant officers within your institution for immediate action.

Yours faithfully,

A handwritten signature in black ink, appearing to be 'Olubunmi Ayodele-Oni', is written over a horizontal line.

Olubunmi Ayodele-Oni

For: Director, Compliance Department



CENTRAL BANK OF NIGERIA

**GUIDANCE NOTE ON THE IMPLEMENTATION OF
THE BASELINE STANDARDS FOR AUTOMATED
AML/CFT/CPF SOLUTIONS**

Providing Clarifications on Regulatory Expectations



Purpose

Following the issuance of the Baseline Standards for Automated AML/CFT/CPF Solutions, the Central Bank of Nigeria (CBN) has observed increased engagement from financial institutions and technology service providers, including public commentary on the interpretation of the Standards.

While this reflects positive industry responsiveness, there is a growing risk of misinterpretation of regulatory expectations, particularly where compliance is framed primarily in terms of system features, vendor capabilities, or technology choices.

This Guidance Note provides clarification on the Central Bank's expectations and should be read alongside the Baseline Standards.

1. Core Regulatory Position

For avoidance of doubt:

- a. Compliance with the Baseline Standards is assessed at the level of the financial institution, based on its ability to demonstrate effective, governed, and defensible AML/CFT/CPF controls.
- b. Technology solutions are enablers of effective AML/CFT/CPF control environments, including governance, oversight, risk-based decision-making, and operational effectiveness, but do not substitute for these elements.

Accordingly, for the purposes of implementing the Baseline Standards for Automated AML/CFT/CPF Solutions, the Central Bank does not approve, certify, or endorse AML solutions or technology providers.

2. Clarification on Technology and AI

The Baseline Standards are technology neutral.

The Standards do not mandate the use of artificial intelligence or any specific technology.

Financial institutions may deploy:

- rules-based systems
- machine learning models
- hybrid approaches

provided that the deployed solution demonstrably meets regulatory expectations. The presence of advanced technology (including AI) does not, in itself, constitute compliance.

3. Clarification on Vendor Claims

The Central Bank has observed claims by third-party providers that their solutions are “fully



compliant” with CBN requirements.

For avoidance of doubt, claims by vendors or service providers regarding “full compliance” or “alignment with CBN standards” are not recognised by the Central Bank of Nigeria.

Compliance is assessed only:

- within the context of a financial institution’s implementation;
- including governance, configuration, and effectiveness.

4. What Constitutes Compliance

Meeting the Baseline Standards requires more than system deployment.

Financial institutions are expected to demonstrate, at a minimum:

a. Defensibility:

- clear audit trails
- explainable decisions
- traceability of actions

b. Governance

- defined ownership and oversight
- model validation and change control
- structured investigation workflows

c. Effectiveness

- credible detection capability
- timely investigation and resolution
- measurable outcomes (including false positive management)

The elements outlined above are not exhaustive and the Central Bank may require additional controls or enhancements where necessary to ensure effective AML/CFT/CPF compliance.

Solutions that are technically advanced but lack governance or demonstrable effectiveness will not be regarded as compliant.

5. Scope of AML Solution Requirements

AML solutions are expected to operate as an integrated control environment covering all relevant components of the AML/CFT/CPF framework.

At a minimum, solutions must support the functional requirements set out in the Baseline Standards (see Section 5.1: AML Solution Requirements).

These include, among others:

- customer identification and verification
- customer risk assessment and profiling



- sanctions, watchlist, and PEP screening
- transaction monitoring for ML/TF/PF risks
- case management and investigation
- regulatory and internal reporting
- audit, governance, and control logging
- relevant data protection and security controls

Financial institutions must ensure full alignment with the detailed requirements specified in the Baseline Standards.

AML solutions must provide a consolidated, real-time or near real-time view of customer risk across all relevant data sources.

Implementations that rely on fragmented or partially integrated systems without robust, automated integration will not meet regulatory expectations.

6. Accountability of Financial Institutions

Financial institutions remain fully responsible for compliance, regardless of reliance on third-party solutions.

Outsourcing or use of vendor platforms does not transfer:

- regulatory responsibility
- accountability for effectiveness
- accountability for demonstrating compliance with the Baseline Standards.

The deployment of any technology solution, including the transition from manual or partially automated processes to automated systems, without demonstrable governance, effective integration and evidence of detection and control effectiveness, will not be regarded as compliance with the Baseline Standards.

This applies irrespective of how such solutions are marketed, including claims that they are “compliant” or “aligned with CBN requirements.”

7. Supervisory Approach

The Central Bank will assess compliance based, at a minimum, on the following:

- the adequacy of system implementation, including the extent of integration across relevant data sources and channels;
- the robustness of governance arrangements, including ownership, oversight, model validation, and change management;
- the demonstrated effectiveness of the solution in supporting detection, investigation, and regulatory reporting.



Additional factors may be considered where necessary to ensure effective supervision. Solutions that do not demonstrate these elements in a coherent and integrated manner will not be regarded as compliant with the Baseline Standards.

8. Proportionality and Minimum Control Expectations

The Central Bank does not expect uniform system sophistication across all institutions. However, reliance on purely manual processes that do not ensure consistency, auditability, and timely detection will not meet regulatory expectations.

Accordingly, institutions are expected to implement control environments capable of meeting these requirements, with the level of sophistication proportionate to their risk profile, size, and complexity.

9. Implementation Submissions and Assessment

Financial institutions are reminded of the requirement to submit implementation roadmaps within three (3) months of the date of issuance of the Baseline Standards i.e., **June 10, 2026**.

The Central Bank will assess these submissions based on:

- alignment with the Baseline Standards;
- evidence of integration, governance, and effectiveness;
- the institution's ability to demonstrate that its AML solution is appropriately configured to its risk profile.

Submissions that rely on partial implementation, manual workarounds, or unsupported claims of capability will not be regarded as meeting regulatory expectations.

COMPLIANCE DEPARTMENT



CENTRAL BANK OF NIGERIA

**CBN AML BASELINE STANDARDS
IMPLEMENTATION ROADMAP
TEMPLATE**



General Instruction

1. Financial institutions are expected to provide complete, accurate, and evidence-based responses.
2. Where tables are provided, all fields must be completed unless otherwise specified.
3. Narrative responses without supporting detail or evidence may be treated as incomplete.
4. Submissions will form the basis for supervisory assessment. Incomplete, inconsistent, or unsupported responses may result in supervisory action.
5. Responses must be internally consistent across all sections of this template. Inconsistencies may result in supervisory challenge or rejection of the submission.



Table of Contents

SECTION 1: EXECUTIVE SUMMARY (MANDATORY)	3
SECTION 2: IMPLEMENTATION STRATEGY	5
SECTION 3: BASELINE STANDARDS IMPLEMENTATION PLAN (CORE SECTION)	7
SECTION 4: SYSTEM ARCHITECTURE TRANSITION	11
SECTION 5: DATA INTEGRATION PLAN	14
SECTION 6: GOVERNANCE IMPLEMENTATION PLAN	16
SECTION 7: EFFECTIVENESS BUILD PLAN	18
SECTION 8: DEPENDENCIES & RISKS	20
SECTION 9: IMPLEMENTATION TIMELINE	22
SECTION 10: RESOURCE PLAN	24
SECTION 11: BOARD / SENIOR MANAGEMENT OVERSIGHT	26
SECTION 12: DECLARATION	27



SECTION 1: EXECUTIVE SUMMARY (MANDATORY)

1.1 Current AML Setup

Indicate current state:

- Manual
- Semi-automated
- Automated

Provide brief description (max 3–4 lines)

1.2 Target State

Provide a concise description of the intended AML solution, including:

- core system approach (upgrade / replacement / hybrid)
- key capabilities to be implemented

1.3 Implementation Approach

Select one:

- Upgrade existing system
- Replace existing system
- Hybrid (overlay + enhancement)

Provide brief justification (max 3–4 lines)

1.4 Key Gaps Identified

List the top 5 gaps preventing full compliance:

Gap Impact Priority (High/Medium/Low)

,

1.5 Target Completion Timeline

- Planned completion date: _____
- Key milestone date (if applicable): _____

1.6 Overall Implementation Owner

- Name: _____



- Role: _____

Guidance for Completion

- Current AML Setup: Indicate the dominant operating model. Where hybrid, select the closest category and explain briefly.
- Target State: Focus on the *end-state capability*, not vendor description.
- Key Gaps: Identify gaps that materially affect compliance (not generic statements).
- Timeline: Must reflect realistic delivery timelines aligned with regulatory expectations.



SECTION 2: IMPLEMENTATION STRATEGY

Q1. What is your implementation approach?

Select one:

- Upgrade existing system
- Replace system
- Hybrid (overlay + upgrade)

Q2. Justification for chosen approach

Guidance for Response (Mandatory Considerations)

The justification for the chosen implementation approach should, at a minimum, address the following:

- alignment with the institution's ML/TF/PF risk profile
- extent to which the approach resolves identified control gaps
- impact on system integration and ability to achieve a consolidated view of customer risk
- implications for governance, including model validation, oversight, and change management
- expected impact on detection effectiveness and reduction of false positives
- limitations or constraints associated with the chosen approach

Responses should be specific to the institution's environment and not rely solely on vendor representations.

Q3. Implementation Feasibility and Delivery Commitment (Mandatory)

Provide:

- expected implementation timeline for the chosen approach
- key dependencies (e.g. vendor, internal systems, data availability)
- critical risks to delivery and how they will be mitigated

Q4. Additional Requirement for Hybrid Approaches (if selected)

Where a hybrid (overlay + upgrade) approach is selected, institutions must:

- explain how underlying system limitations will be addressed
- demonstrate how integration gaps will be resolved



- confirm how reliance on overlay solutions will not compromise governance, integration, or effectiveness

Hybrid approaches that do not adequately address underlying control weaknesses or integration gaps may not be accepted.

Guidance for Completion

- Responses should demonstrate clear linkage between risk, control gaps, and chosen approach.
- Generic statements (e.g. “industry best practice”, “vendor recommendation”) are not sufficient.
- Institutions selecting hybrid approaches should clearly demonstrate how underlying system limitations will be addressed.



SECTION 3: BASELINE STANDARDS IMPLEMENTATION PLAN (CORE SECTION)

The implementation plan presented in this section must be consistent with the strategies, timelines, and outcomes described in other sections of this document.

Financial institutions must ensure that all sub-requirements and expectations under each heading in Section 5.1 of the Baseline Standards are fully considered. Responses should not be limited to the headings listed below.

All fields in the table below must be completed. Blank or incomplete responses will be treated as non-compliance.

Status (select one only):

- Not Started
- In Progress
- Implemented (Not Yet Tested)
- Implemented and Tested
- Partially Implemented
- Not Applicable (Justification Required)

Where “Partially Implemented” or “Not Applicable” is selected, a detailed justification must be provided.

Instructions

- Key Sub-Requirements Considered (Y/N): Indicate whether all sub-requirements under the relevant Section 5.1 heading have been considered. Where “Yes” is selected, provide a brief description.
- Current State: Clearly describe the institution’s existing capability, including whether the requirement is manual, semi-automated, or automated.
- Target State: Describe the intended end-state aligned with the Baseline Standards.
- Action Required: Specify the actions required to transition from the current state to the target state.

Where Current State differs from Target State, this must be clearly reflected in the Action Required column.

- Evidence Available (Y/N):
Where “Yes” is selected, supporting evidence must be available for supervisory



review.

Where “No” is selected, the requirement will be treated as not evidenced.

Baseline Requirement (Section 5.1)	Key Sub-Requirements Considered (Y/N)	Current State	Target State	Action Required	Owner	Start Date	End Date	Status	Evidence Available (Y/N)
Customer Due Diligence (CDD), Know Your Customer (KYC) and Know Business (KYB)									
Sanction Lists									
PEP Screening									
Risk Assessment									
Transaction Monitoring									
Risk-Based Analyses									



Case Management									
Regulatory Reporting									
Management Information Reporting									
Audit and Governance									
System Integration & Scalability									
Security & Data Protection									
User Interface & Customisation									
Vendor/Third-Party Risk Management									
Fraud Monitoring and Detection									



Mandatory Confirmation

Confirm that all requirements under Section 5.1 of the Baseline Standards have been fully addressed in this table (Y/N).

If No, provide details of any omissions.

Guidance for Completion

Key Sub-Requirements Considered: Indicate whether all detailed expectations under Section 5.1 have been reviewed and incorporated.

Current State: Must reflect actual capability (manual, semi-automated, automated).

Target State: Should align fully with Baseline Standards requirements.

Action Required: Must clearly describe how identified gaps will be closed.

Status: Select the option that most accurately reflects current progress.

Evidence Available: Where “Yes”, evidence must be available for supervisory review.



SECTION 4: SYSTEM ARCHITECTURE TRANSITION

4.1 Current Architecture (Mandatory)

Provide a concise but specific summary of the current AML system architecture, including:

- core systems supporting AML/CFT/CPF activities
- level of automation (manual / semi-automated / automated)
- key integration gaps or limitations

Attach architecture diagram (mandatory).

4.2 Target Architecture (Mandatory)

Provide a clear description of the target AML system architecture, including:

- key system components and capabilities
- integration across customer, transaction, and screening data
- how the architecture supports a consolidated view of customer risk

Attach target architecture diagram (mandatory).

4.3 Integration Plan (Mandatory)

Provide a structured plan for system integration:

System / Data Source	Current State	Action Required	Target State	Timeline
----------------------	---------------	-----------------	--------------	----------

Include, at a minimum:

- core banking system
- customer/KYC systems
- transaction channels (mobile, USSD, cards, etc.)
- screening engines
- case management systems

Supporting evidence of integration (e.g. system interfaces, data flows, or sample outputs) must be available for supervisory review.

4.4 Data Lineage and Flow (Mandatory)

Describe how data flows through the AML system from:

- customer onboarding → risk profiling
- transaction processing → alert generation



- alert → case → regulatory reporting

Provide at least one example demonstrating end-to-end data flow (evidence to be made available for supervisory review).

4.5 Implementation Sequencing

Provide clear sequencing of implementation phases, including:

- key milestones
- dependencies between systems
- critical path items

Generic descriptions (e.g. “phased implementation”) are not sufficient.

4.6 Expected Outcome

Explain how the target architecture will:

- eliminate fragmentation
- enable integration across relevant data sources
- support a consolidated, real-time or near real-time view of customer risk

4.7 Overlay / Hybrid Architecture (if applicable)

Indicate whether the target architecture relies on overlay solutions.

Where applicable, institutions must:

- explain how underlying system limitations will be addressed
- demonstrate how integration gaps will be resolved
- confirm how reliance on overlay solutions will not compromise governance, integration, or effectiveness

Overlay approaches that do not adequately address underlying control weaknesses or integration gaps may not be accepted.

Guidance for Completion

- Architecture descriptions should be specific and system-based, not conceptual.
- Diagrams must clearly show:
 - data sources



- system interactions
- processing flows
- Integration should demonstrate ability to support a consolidated view of customer risk.
- Where overlay solutions are used, institutions must demonstrate how fragmentation risks are addressed.



SECTION 5: DATA INTEGRATION PLAN

5.1 Overview (Mandatory)

Provide a summary of all data sources required to support AML/CFT/CPF activities. Financial institutions must ensure that all relevant data sources are identified and included. Partial or selective integration will not meet regulatory expectations.

Data Source	Current State	Action Required	Target State	Integration Method	Frequency	Timeline	Evidence Available (Y/N)

5.2 Minimum Data Sources (must be included)

At a minimum, the following must be addressed:

- core banking system
- customer/KYC/BVN/NIN data
- transaction channels (mobile, USSD, cards, POS, etc.)
- sanctions/watchlist data
- PEP databases
- case management systems
- external data sources (where applicable)

5.3 Integration Requirements

For each data source, institutions must:

- describe how data is integrated into the AML system
- indicate whether integration is automated or manual
- specify frequency (real-time / near real-time / batch)



Manual or delayed integration must be clearly justified.

5.4 Data Quality and Completeness

Explain how the institution ensures:

- completeness of data
- accuracy of data
- consistency across systems

5.5 Evidence Requirement

Where “Evidence Available (Y/N)” is marked as Yes, supporting evidence (e.g. system interfaces, data extracts, or sample outputs) must be available for supervisory review. Where No, the data integration will be treated as not evidenced.

Guidance for Completion

- All relevant data sources must be included.
- Partial or selective integration is not sufficient.
- Integration method should specify whether data is:
 - real-time
 - near real-time
 - batch
- Data quality controls should address:
 - completeness
 - accuracy
 - consistency



SECTION 6: GOVERNANCE IMPLEMENTATION PLAN

6.1 This section should describe how governance will be established or enhanced to support the AML solution.

Governance Element	Current State	Action Required	Target State	Owner	Timeline	Evidence Available (Y/N)

6.2 Minimum Governance Elements (must be addressed)

At a minimum, the following must be included:

- system ownership and accountability
- model validation and periodic review
- change management and approval processes
- oversight and reporting structures
- escalation and issue management processes
- documentation and audit trail requirements

6.3 Governance Effectiveness

Explain how governance will ensure:

- ongoing monitoring of system performance
- timely identification and remediation of issues
- accountability for AML/CFT/CPF outcomes

Supporting evidence must be available for supervisory review. Where evidence is not available, governance will be treated as not established.

Guidance for Completion

- Governance should focus on how oversight will operate in practice, not just structure.
- Ownership must be clearly assigned and accountable.



- Model validation and change management processes must be defined and operational.
- Governance should enable:
 - monitoring
 - escalation
 - accountability



SECTION 7: EFFECTIVENESS BUILD PLAN

This section should demonstrate how the institution will achieve measurable improvements in AML/CFT/CPF effectiveness.

Where target values are not achieved within stated timelines, institutions may be required to provide justification and remediation plans.

7.1 Effectiveness Improvement Table (Mandatory)

Metric	Current Value	Target Value	Action Required	Timeline	Evidence Available (Y/N)

Current Value:

Provide the institution's current, measured performance for each metric based on available data.

Target Value:

Provide the expected performance following implementation of the AML solution. Targets must be realistic, measurable, and aligned with the institution's risk profile.

Where current values are not available, this must be explicitly stated and addressed as part of the implementation plan.

7.2 Minimum Metrics (must be included)

- alert volumes
- false positive rate
- STR conversion rate
- investigation turnaround time

Additional Metrics (if applicable)

- Financial institutions may include additional metrics relevant to their business model and risk profile.

Metrics should be clearly defined and consistently measured. Institutions should specify how each metric is calculated.



7.3 Detection Capability

- Explain how the proposed solution will:
- improve detection of ML/TF/PF risks
- enhance risk-based monitoring
- reduce noise without weakening detection

7.4 Validation of Effectiveness

- Explain how effectiveness will be assessed, including:
- testing approaches
- performance monitoring
- periodic review

Statements of expected improvement must be supported by measurable targets. Unquantified claims will not be considered sufficient.

Guidance for Completion

- Current Value: Provide actual measured performance based on available data.
- Target Value: Provide realistic, measurable improvements expected post-implementation.
- Where current values are unavailable, this must be explicitly stated and addressed.
- Metrics should be clearly defined, including how they are calculated.
- Improvements must be quantifiable and linked to system enhancements.



SECTION 8: DEPENDENCIES & RISKS

8.1 Dependencies (Mandatory)

Identify key dependencies required for implementation:

Dependency	Description	Impact if Not Met	Mitigation

Examples may include:

- vendor delivery
- system integration readiness
- data availability
- internal resource capacity

8.2 Implementation Risks (Mandatory)

Risk	Impact	Likelihood (High/Medium/Low)	Mitigation	Owner

8.3 Critical Risks

Identify any risks that could significantly delay or prevent implementation within the required timeline.

Failure to adequately identify and manage dependencies and risks may result in delays that will not be considered acceptable from a supervisory perspective.

Guidance for Completion



- Dependencies: Include all internal and external factors required for successful implementation (e.g. vendors, systems, data).
- Risk: Risks should relate specifically to implementation delivery and AML control effectiveness, not generic operational risks.
- Impact: Describe effect on timeline, delivery, or effectiveness.
- Mitigation: Must be practical and actionable.



SECTION 9: IMPLEMENTATION TIMELINE

This section must present a clear, structured timeline for implementation of all activities outlined in this plan.

9.1 Implementation Timeline (Mandatory)

Phase / Milestone	Description	Start Date	End Date	Dependencies	Owner

9.2 Requirements

The timeline must include:

- all key implementation phases
- major system deployment milestones
- integration activities
- governance implementation milestones
- testing and validation activities

Narrative descriptions are not sufficient. A structured timeline must be provided.

9.3 Critical Deadlines

Identify:

- final implementation completion date
- any interim milestones critical to delivery

Timelines must be realistic and aligned with the regulatory submission deadline.



Guidance for Completion

- Phase / Milestone: A distinct stage or deliverable in implementation (e.g. system selection, integration, testing, deployment).
- Dependencies: Factors required for completion (e.g. vendor delivery, system readiness).
- Owner: Individual or function accountable for delivery.
- Timeline must be:
 - structured
 - realistic
 - aligned with implementation plan



SECTION 10: RESOURCE PLAN

10.1 Internal Resources (Mandatory)

Role / Function	Responsibility	Assigned (Y/N)	Name (if assigned)

10.2 Vendor Involvement (Mandatory, if applicable)

Vendor	Scope of Work	Dependency Level (High/Medium/Low)	Risk if Delayed

10.3 Resource Adequacy

Explain whether the institution has sufficient:

- technical capability
- operational capacity
- governance oversight

to deliver the implementation plan.

10.4 Budget (Optional)



Provide high-level indication of budget allocation (if available).

Insufficient resourcing may impact the feasibility of the implementation plan and will be considered during supervisory review.

Guidance for Completion

- Internal resources should reflect actual assigned roles, not planned or assumed capacity.
- Vendor involvement should clearly indicate:
 - scope
 - dependency level
 - delivery risk
- Institutions should assess whether resources are sufficient to deliver within timelines.



SECTION 11: BOARD / SENIOR MANAGEMENT OVERSIGHT

11.1 Accountability (Mandatory)

- Overall accountable executive: _____
- Role: _____

11.2 Oversight Structure

Describe:

- governance structure overseeing implementation
- committees or forums responsible
- escalation mechanisms

11.3 Reporting

Specify:

- reporting frequency (e.g. weekly, monthly)
- recipients (Board, Board Committee, Senior Management)
- type of reporting (progress, risk, issues)

Implementation plans must be subject to active oversight by senior management and/or the Board.

Guidance for Completion

- Accountability should be assigned to a named senior individual.
- Oversight structures should reflect actual governance forums, not theoretical constructs.
- Reporting should include:
 - frequency
 - recipients
 - content (progress, risks, issues)



SECTION 12: DECLARATION

We confirm that this implementation plan:

- covers all requirements of the Baseline Standards
- is achievable within the stated timelines
- reflects the institution's actual implementation strategy
- has been reviewed and approved by senior management

Authorisation

- Name: _____
- Role: _____
- Signature: _____
- Date: _____

The Central Bank may take supervisory action where information provided is found to be inaccurate, incomplete, or misleading.

Guidance for Completion

- Declaration must be signed by an appropriate senior officer.
- Submission implies that:
 - the plan has been reviewed
 - the plan is deliverable
 - the institution accepts accountability

This template should be read together with the Baseline Standards and the Guidance Note on the Implementation of the Baseline Standards. The Guidance Note provides clarification and does not replace or supersede the requirements set out in the Baseline Standards.