VOVE ID

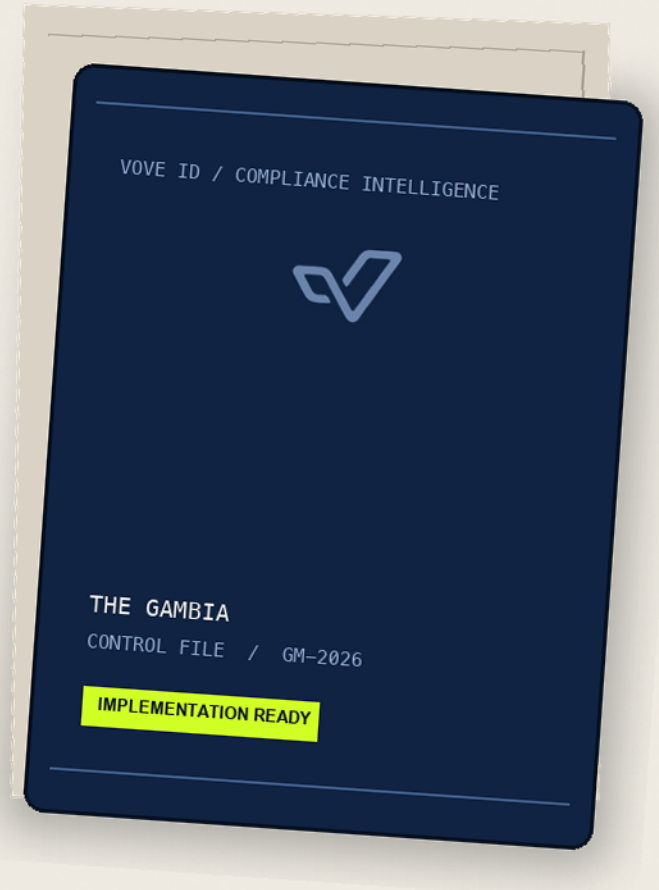
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

THE GAMBIA

THE GAMBIA / GM



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

The Gambia KYC, KYB, AML, CFT, CPF and Data Governance Compliance Checklist 2026

An implementation checklist for customer and business verification in The Gambia under the Anti-Money Laundering and Combating of Terrorist Financing Act 2012, FIU guidance, financial-sector supervision and company-registration requirements.

Primary AML/CFT law	**Anti-Money Laundering and Combating of Terrorist Financing Act 2012**
Financial intelligence unit	**Financial Intelligence Unit of The Gambia**
STR timing	**As soon as practicable and no later than three working days**
Casual-customer CDD	**More than GMD 200,000; suspicion and identity doubt apply regardless of amount**
Large-cash purpose inquiry	**More than USD 10,000 or Gambian-dalasi equivalent**
Core AML retention	**Minimum five years under record-class-specific clocks**
Beneficial ownership	**Natural person with ultimate ownership/control or ultimate effective control; no universal AML percentage**
Company registry	**Companies Department, Ministry of Justice**
Payments and fintech	**Obtain activity-specific CBG classification and authority before launch**
FATF public lists	**Not named in June 2026 statements; GIABA enhanced follow-up is separate**

Scope and legal framework

The Anti-Money Laundering and Combating of Terrorist Financing Act 2012 is the principal preventive AML/CFT statute and establishes the FIU. It applies to financial institutions and listed non-financial businesses and professions. CBG supervises licensed financial institutions; the Ministry of Justice Companies Department administers the Companies Act 2013 and Single Window Business Registry Act 2013. CPF, sanctions, payments, virtual assets and privacy require activity-specific confirmation because the reviewed public framework does not support a universal procedure or deadline.

FATF context

As at 21 July 2026, The Gambia was not named in FATF's June 2026 public statements on jurisdictions under increased monitoring or jurisdictions subject to a call for action. GIABA's 2024 second enhanced follow-up report is a technical-compliance assessment and is not FATF public-list status.

IMPORTANT	This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 21 July 2026. Confirm FIU registration, current reporting forms and channels, threshold-report treatment, sanctions and CPF procedures; CBG licensing for each payment, remittance, e-money, fintech or virtual-asset model; registry beneficial-ownership filings; and privacy, biometric, breach and transfer requirements with Gambian counsel and the competent authority before launch. VOVE ID supports evidence collection and audit trails; the reporting entity remains responsible for acceptance, reporting, restraint and compliance decisions.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and regulated activities

Resolve entity, activity and supervisor scope before launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial institutions and listed DNFBPs are reporting entities under the 2012 Act.	Map each entity, product, profession, branch, agent and outsourced service to the Act's schedules and competent supervisor.	Perimeter memorandum, entity-product map, licences and supervisor register.	2012 Act, ss.2 and 59; First and Second Schedules
The FIU receives and analyses reports, issues instructions and supervises compliance within its mandate.	Register compliance contacts and obtain the FIU's current reporting access, forms and instructions.	FIU correspondence, access records, contacts and regulatory calendar.	2012 Act, ss.3-7, 18 and 33
Banking, money services, payments, fintech and virtual-asset activity require activity-specific authority.	Obtain a written CBG or relevant-authority perimeter decision and every required licence before pilot or launch.	Classification, application, licence, conditions and approved product map.	CBG Banking Supervision and official licensing materials; controlled perimeter dependency

Governance, risk assessment and control ownership

Build documented, risk-based and accountable controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting entities maintain customer-identification, records, reporting, employee-screening and technology controls.	Approve a risk-based AML/CFT programme covering every entity, product, channel and customer class.	Programme, risk assessments, procedures, approvals and issue log.	2012 Act, s.39
A compliance officer, staff training and independent audit are required.	Appoint an empowered officer, train relevant staff and independently test the control lifecycle.	Appointment, charter, training records, audit reports and remediation.	2012 Act, s.39

Natural-person identification and CDD

Apply statutory triggers without treating thresholds as safe harbours.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD applies before or within a reasonable time of a relationship or transaction, to electronic transfers, suspicion and identity doubt.	Configure relationship, transaction, transfer, suspicion and identity-quality triggers and record the applicable basis.	Trigger matrix, cases, verification timestamps and exceptions.	2012 Act, s.25(1)
Natural persons are identified and verified using official documents and reliable independent sources.	Capture name, address, occupation and valid photo identification and authenticate the evidence proportionately.	Identity file, authenticity result, address evidence and decision.	2012 Act, s.25(1)-(2)(b)
Casual-customer identification applies above GMD 200,000, including connected transactions once the aggregate crosses the threshold.	Aggregate apparently connected activity and apply CDD earlier where suspicion or doubt exists.	Aggregation logic, alerts, identity file and decision.	2012 Act, s.25(2)(e)
For cash above USD 10,000 or its dalasi equivalent, purpose, origin and ultimate destination require reasonable measures.	Obtain and corroborate source, purpose and destination evidence before release.	Customer explanation, source documents, destination evidence and approval.	2012 Act, s.25(4)

KYB, authority and beneficial ownership

Verify existence, authority and ultimate natural-person ownership or control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Legal-entity CDD verifies incorporation, address, directors, principal owners, beneficiaries, control structure and binding powers.	Obtain current registry and constitutive evidence and reconcile directors, mandates, ownership and control.	Registry extract, certificate, constitution, annual return, directors and discrepancy log.	2012 Act, s.25(2)(c); definition of identification record
Representatives and third-party principals require verified identity and authority.	Verify each representative and the person for whose ultimate benefit the transaction is conducted.	Identity files, mandate, board authority and verification result.	2012 Act, s.25(2)(c)(iv) and s.25(3)
A beneficial owner is the natural person who ultimately owns or controls, or exercises ultimate effective control.	Trace every ownership layer and test non-ownership control without inventing a universal percentage.	Ownership chart, source records, control analysis and BO identity files.	2012 Act, s.2 definition of beneficial owner
Company registration evidence must be obtained from the Companies Department and kept current.	Confirm the live forms, annual-return position and any beneficial-ownership filing directly with the registry.	Registry receipt, certified records, annual return and registry correspondence.	Companies Act 2013; Ministry of Justice Companies Department guidance

PEPs, enhanced due diligence and reliance

Apply stronger controls to higher-risk relationships.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
PEPs require identity verification, senior-management approval, reasonable source-of-wealth measures and enhanced monitoring.	Screen customers and beneficial owners, corroborate source evidence and document approval before activation.	Screening, match decision, source file, approval and monitoring plan.	2012 Act, s.25(2)(d)
Third-party reliance does not remove the reporting entity's duty to obtain information immediately and documents without delay.	Assess the intermediary's regulation and controls, contract for access and test retrieval.	Due diligence, agreement, retrieval tests and monitoring.	2012 Act, s.25(7)
Remote onboarding must achieve reliable independent verification and manage technology misuse risk.	Use document-integrity, liveness or presence, device and fraud controls proportionate to risk.	Remote standard, test results, fraud logs and exceptions.	2012 Act, ss.25(1) and 39(e); recommended implementation control

Failed CDD, monitoring and suspicious reporting

Block unsafe activity and report suspicion promptly and confidentially.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
If satisfactory identity evidence cannot be obtained, the entity must not establish or maintain the relationship and may report the attempt.	Block activation or terminate under controlled procedures and refer the case for confidential STR review.	Failure reason, block, closure, STR decision and receipt.	2012 Act, s.26
Complex, unusual and large transactions, higher-risk jurisdictions and incomplete wire information receive special monitoring.	Examine and record background and purpose and make findings available to FIU or competent authority.	Alerts, cases, written findings, escalation and refreshed CDD.	2012 Act, s.30
Transactions, attempted transactions and relevant information linked to crime, ML or TF are reportable to the FIU.	Escalate immediately, preserve the suspicion timestamp and submit the prescribed STR.	Internal report, analysis, STR, receipt and timeline.	2012 Act, s.33(1)-(3)
An STR is due as soon as practicable and no later than three working days after suspicion or information.	Use a shorter internal SLA measured from the recorded formation or receipt time.	Trigger timestamp, approval, submission time and SLA monitoring.	2012 Act, s.33(1)
Tipping off is prohibited and good-faith reporting is protected.	Restrict access and govern customer communications and lawful disclosures.	Access logs, communication plan, training and disclosure register.	2012 Act, ss.34-37

Wires, thresholds, payments and agents

Keep CDD, transaction records and reportable thresholds distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Wire transfers carry accurate originator information, subject to stated card and inter-institution exceptions.	Validate required information through the payment chain and govern incomplete messages.	Field matrix, validation, repair or reject queue and samples.	2012 Act, ss.29-30
Sector thresholds in the Act are not a universal transaction-reporting threshold.	Map each threshold to its exact sector and control and confirm any current FIU threshold-report direction before implementation.	Threshold matrix, FIU direction, configuration and receipts.	2012 Act, ss.40-43; controlled live-direction dependency
Payment, remittance, e-money, fintech, agent and virtual-asset models require current perimeter confirmation.	Do not launch until CBG or the relevant authority confirms licensing, agent and AML/CFT conditions in writing.	Legal classification, application, authority, agent register and monitoring.	CBG official supervision and licensing materials; controlled uncertainty

8. TARGETED FINANCIAL SANCTIONS AND CPF

Targeted financial sanctions and CPF

Apply current lists and authority instructions without inventing procedures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Terrorist property and court-directed restraint provisions require controlled escalation and preservation.	Screen customers, BOs, representatives and transactions against current UN and domestic designations and escalate potential matches immediately.	List provenance, screening logs, match decisions, holds and authority correspondence.	2012 Act, Parts III, VII and VIII; current procedure must be confirmed
The live freezing, reporting, false-positive and CPF procedure must be confirmed with the competent authority.	Maintain a 24/7 escalation route and obtain written instructions before releasing or dealing with potentially affected property.	Procedure, escalation log, instruction, decision and audit trail.	Controlled uncertainty; FIU and competent-authority confirmation required

9. RECORDS, ACCESS AND ASSURANCE

Records, access and assurance

Retain reconstructable evidence under the correct clock.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identity, transaction, correspondence, FIU report and enquiry records are kept for at least five years under record-class-specific clocks.	Map each class to identity collection, transaction/correspondence, and later of closure or relationship cessation and apply legal holds.	Retention schedule, configuration, samples and deletion tests.	2012 Act, s.27(1)-(2)
Records must reconstruct transactions and be immediately available to FIU or competent authorities.	Index linked identity, transaction, investigation and reporting evidence and test retrieval.	Request register, retrieval tests, access controls and response package.	2012 Act, s.27(3)-(5)
Electronic records require backup, recovery and authentication controls.	Test integrity, backup, recovery and authorised access throughout retention.	Architecture, backup tests, audit logs and recovery evidence.	2012 Act, s.27(4)

10. PRIVACY, BIOMETRICS AND TRANSFERS

Privacy, biometrics and transfers

Use cautious data governance while the public legal framework is confirmed.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identity and transaction data must be protected while remaining available for lawful AML/CFT access.	Document purpose and necessity, minimise collection, restrict access and preserve AML evidence.	Data inventory, access matrix, notices, logs and retention mapping.	2012 Act, ss.27 and 35; recommended privacy control
Biometrics, breach notification, data-subject rights and international transfers require a verified current legal basis.	Confirm applicable law and regulator expectations before processing; do not invent a deadline or transfer mechanism.	Legal memo, impact assessment, transfer map, incident playbook and contracts.	Controlled uncertainty; 2019 national policy is contextual, not enacted-law authority

11. PRACTICAL EVIDENCE PACKS AND CHANGE CONTROL

Practical evidence packs and change control

Make decisions reconstructable and keep time-sensitive rules current.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A complete customer file links identity, KYB, ownership, screening, risk, approval, monitoring and reporting decisions.	Block activation when mandatory evidence or approval is missing and preserve the release decision.	Control checklist, linked file, approvals and release log.	2012 Act, Parts V-VII
FIU instructions, thresholds, sanctions lists, FATF status, registry and licensing requirements require ongoing monitoring.	Assign owners and review FIU, CBG, Ministry of Justice, Gazette, FATF and GIABA sources on a governed schedule.	Legal inventory, source log, change assessments and implementation tickets.	Official sources listed below

SOURCES AND FURTHER READING

Verify against current official material

Primary law and regulator guidance control. Contextual VOVE ID reading is included to help teams operationalize the requirements and is not legal authority.

Anti-Money Laundering and Combating of Terrorist Financing Act 2012
Financial Intelligence Unit of The Gambia · Primary legislation - official FIU copy
Open official source

AML/CFT Guidelines for Financial Institutions
FIU and Central Bank of The Gambia · Official sector guidance
Open official source

AML/CFT Guidelines for DNFBPs
Financial Intelligence Unit of The Gambia · Official sector guidance
Open official source

FIU downloads and reporting resources
Financial Intelligence Unit of The Gambia · Official FIU guidance
Open official source

Banking supervision and licensing materials
Central Bank of The Gambia · Official regulator
Open official source

Companies Department registration guidance
Ministry of Justice · Official company registry guidance
Open official source

The Gambia second enhanced follow-up report, 2024
GIABA · Authoritative regional assessment
Open official source

Jurisdictions under Increased Monitoring - June 2026
FATF · Authoritative public statement
Open official source

High-Risk Jurisdictions subject to a Call for Action - June 2026
FATF · Authoritative public statement
Open official source

Document control

Version 1.0 / Published 2026 / Last reviewed 21 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 21 July 2026. Confirm FIU registration, current reporting forms and channels, threshold-report treatment, sanctions and CPF procedures; CBG licensing for each payment, remittance, e-money, fintech or virtual-asset model; registry beneficial-ownership filings; and privacy, biometric, breach and transfer requirements with Gambian counsel and the competent authority before launch. VOVE ID supports evidence collection and audit trails; the reporting entity remains responsible for acceptance, reporting, restraint and compliance decisions.