VOVE ID

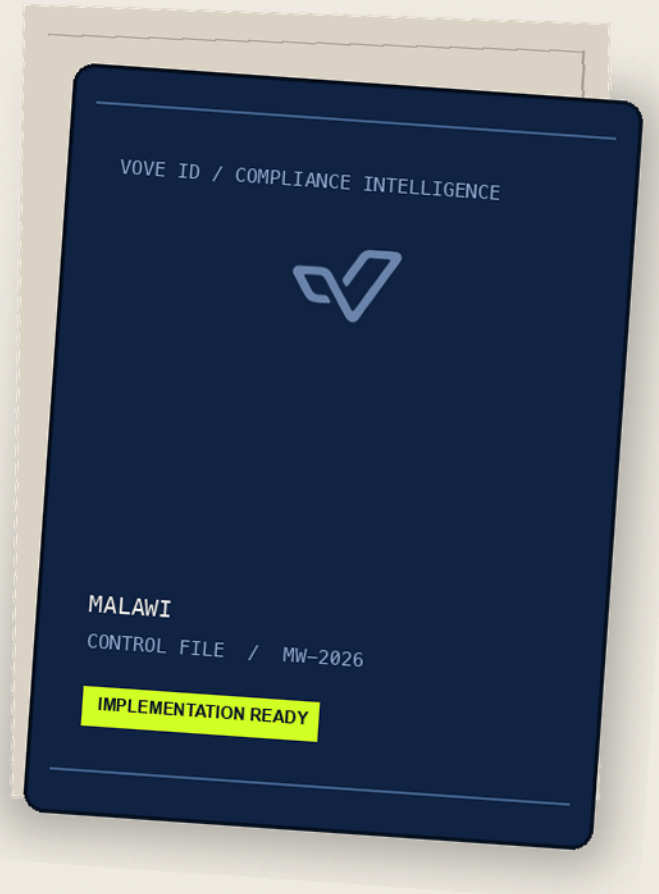
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

MALAWI

MALAWI / MW



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Malawi KYC, KYB, AML, CFT, CPF and Data Protection Compliance Checklist 2026

An implementation checklist for customer and business verification in Malawi, covering the Financial Crimes Act, 2020 Money Laundering Regulations, targeted financial sanctions, company verification, payments and the Data Protection Act 2024.

Primary AML/CFT law	**Financial Crimes Act (Chapter 7:07), commenced 17 February 2017**
Financial intelligence unit	**Financial Intelligence Authority (FIA)**
STR timing	**As soon as possible and no later than three days after suspicion; attempts and any amount are covered**
Large transaction reporting	**MWK 5,000,000 transaction or aggregate under the 2020 Regulations; current FIA direction controls submission timing**
Local mobile-money transfer reporting	**Each transfer above MWK 300,000 under regulation 21**
Casino CDD trigger	**MWK 2,000,000 within 24 hours for specified gaming transactions, plus entry/access identification duties**
Core AML retention	**Seven years, with the start event determined by record class**
Beneficial ownership	**Natural-person ownership/control, other control, then senior-management fallback; no universal percentage stated in the Act**
Data protection	**Data Protection Act 2024, commenced 31 May 2024; confirm live registration and incident procedures with MACRA**
FATF public lists	**Not named in FATF statements dated 19 June 2026; ESAAMLG follow-up continues**

Scope and legal framework

The Financial Crimes Act (Chapter 7:07) is the principal AML/CFT statute and establishes the Financial Intelligence Authority. The Financial Crimes (Money Laundering) Regulations 2020 add operational CDD, reporting, record, wire and governance rules. Government Notice 11 of 2017 governs suppression of terrorist financing and proliferation. Financial services and payment activities remain subject to Reserve Bank of Malawi licensing and supervision. Company information is administered by CRIPC. The Data Protection Act 2024, commenced on 31 May 2024, governs personal-data processing under MACRA oversight.

FATF context

As at 17 July 2026, Malawi was not named in FATF's 19 June 2026 public statements on jurisdictions under increased monitoring or jurisdictions subject to a call for action. Malawi remains within ESAAMLG's follow-up process; the April 2024 enhanced follow-up report assessed technical-compliance progress. Public-list status is dated and does not replace customer-specific risk assessment.

IMPORTANT

This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 17 July 2026. Confirm current Gazette amendments, FIA directives and report channels, RBM licensing conditions, CRIPC filing mechanics and MACRA data-protection procedures with Malawian counsel and the competent authority before launch. Monetary reporting thresholds, AML beneficial-ownership analysis and company-registry disclosures are distinct. VOVE ID supports evidence collection and audit trails; the reporting institution remains responsible for acceptance, reporting, freezing 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, product, profession and supervisor scope before configuring controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial institutions and designated non-financial businesses and professions within the statutory definition are reporting institutions.	Map each entity, product, branch, profession, agent and outsourced activity to the Act and its supervisor.	Perimeter memorandum, entity-product matrix, licences and authority map.	Financial Crimes Act (FCA), s.2 and Second Schedule
The FIA receives and analyses reports, issues guidance and supervises compliance within its mandate.	Register required contacts and reporting access, appoint alternates and maintain a regulatory calendar.	FIA registration, channel access, contact register and calendar.	FCA, ss.3-6 and 23, 33
Deposit-taking, payments, remittance, e-money and other financial services require the applicable RBM authority before launch.	Obtain a written perimeter and every required RBM licence or approval before pilot or production operation.	RBM classification, licence, conditions, approved product map and renewal register.	Financial Services Act 2010; National Payment Systems Act; RBM licensing framework

Governance, risk assessment and control ownership

Build accountable controls from documented customer, product, delivery, geography and transaction risk.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting institutions identify, assess, document and keep current their ML/TF risks and apply proportionate mitigation.	Approve enterprise and customer-risk methodologies, document inputs and overrides and review material change.	Risk assessments, methodology, ratings, approvals and remediation plan.	FCA, s.21(1)-(4); 2020 Regulations, reg.3
A written customer-acceptance policy is updated annually or on new developments and approved by the board.	Define acceptance, escalation, prohibition and exception rules and obtain annual board approval.	Policy, board minutes, change record and staff guidance.	2020 Regulations, reg.18
The AML programme includes internal rules, training, compliance oversight and independent testing.	Appoint an authorised compliance officer, provide information access and test the complete lifecycle independently.	Appointment, charter, training, audit reports and issue tracker.	FCA, ss.27-28; 2020 Regulations, regs.30-35

Natural-person identification and CDD

Identify and verify customers at relationship, prescribed transaction, wire, suspicion and identity-doubt triggers.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD is required for a relationship, prescribed occasional or wire transaction, suspicion, and doubt about earlier evidence.	Configure all five triggers and linked-transaction detection; never let a monetary threshold suppress suspicion-driven CDD.	Trigger matrix, aggregation logic, test cases and exceptions.	FCA, s.16(1); 2020 Regulations, reg.4
A natural person is identified through official documentation and verified using reliable, independent sources.	Capture name, address, occupation and official identity evidence; validate authenticity and screen the person.	Identity record, authenticity result, independent verification and screening decision.	FCA, s.16(1)-(2)(b); 2020 Regulations, regs.5-6, 10-12
Purpose, intended nature and risk-relevant source information must be understood.	Record intended products, expected activity, counterparties, geography and corroborated source information proportionate to risk.	Customer profile, purpose statement, expected-activity baseline and source evidence.	FCA, s.16(2)(a)-(b); 2020 Regulations, reg.11
Deferred verification is exceptional and allowed only where prompt completion and effective risk management are assured.	Apply restrictions, a short completion deadline and escalation; do not treat deferral as routine onboarding.	Exception approval, rationale, restrictions and completion timestamp.	FCA, s.16(7); 2020 Regulations, reg.10(2)-(3)

KYB, authority and beneficial ownership

Verify legal existence, representatives and the natural persons who ultimately own or control the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Legal-person CDD covers name, legal form, existence, binding powers, senior management, registered office, ownership and control.	Obtain current CRIPC evidence and constitutive documents and reconcile directors, addresses, mandates and ownership.	Registry extract, constitution, directors, address, licence and discrepancy log.	FCA, s.16(2)(c); 2020 Regulations, regs.8-9, 13-15
A person acting for another customer must have verified authority and identity.	Verify each representative separately and validate the mandate before permitting activity.	Identity file, mandate, board authority and verification result.	FCA, s.16(9)(b); 2020 Regulations, reg.16
Beneficial-owner analysis follows natural-person controlling ownership, control through other means and senior-management fallback.	Trace every ownership layer, test non-ownership control and document why any senior-manager fallback was necessary.	Ownership chart, registry evidence, control analysis, BO KYC and fallback rationale.	FCA, ss.2 and 16(3)-(4)
Trust CDD identifies the settlor, trustee, protector if any, beneficiaries or class and every other natural person exercising ultimate effective control.	Verify the trust instrument, roles, powers, control chain and relevant natural persons.	Trust deed, role register, powers analysis and verified identity files.	FCA, s.16(5)-(6); 2020 Regulations, regs.8, 13

PEPs, enhanced due diligence and remote onboarding

Higher-risk and politically exposed relationships require accountable approval and stronger evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Systems determine whether a customer or beneficial owner is a PEP and extend reasonable measures to family and close associates.	Screen before activation and continuously, resolve matches and preserve reliable role and relationship evidence.	Screening, match decision, role evidence and relationship analysis.	FCA, ss.2 and 16(2)(d); 2020 Regulations, reg.7
PEP relationships require senior-management approval, source-of-wealth and source-of-funds measures and enhanced ongoing monitoring.	Corroborate source evidence, record approval before starting or continuing and configure enhanced monitoring.	Source file, approval, monitoring plan and reviews.	FCA, s.16(2)(d)
High risk receives enhanced CDD; simplified measures require substantiated lower risk.	Define standard, enhanced and simplified control sets with eligibility rules and prohibited overrides.	Risk-control matrix, rationale, approvals and override log.	FCA, s.21(5)-(6); 2020 Regulations, regs.3-4
Non-face-to-face relationships receive the same identification, verification and monitoring standards as face-to-face relationships; the Act's non-resident limitation must be assessed.	Confirm legal eligibility, then use document-integrity, presence, independent-data, device and fraud checks proportionate to risk.	Eligibility memo, remote standard, test results, fraud logs and exceptions.	FCA, s.16(8)

Failed CDD, monitoring and suspicious reporting

Block unsafe activity, monitor continuously and report suspicion promptly and confidentially.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
If satisfactory identity evidence is unavailable, do not open, start or transact; submit an STR within three days and do not proceed unless FIA directs.	Route failed CDD to block and confidential reporting review without alerting the customer.	Failure reason, block, STR, submission receipt and FIA direction if any.	FCA, s.19; 2020 Regulations, reg.4(3)-(4)
Ongoing monitoring tests activity against customer knowledge, business, risk and source information and keeps records current.	Configure risk-based refresh, event triggers and transaction monitoring; investigate deviations.	Refresh schedule, triggers, scenarios, alerts, cases and updated CDD.	FCA, s.29; 2020 Regulations, regs.19(5), 24
Suspected or confirmed transactions and attempted transactions connected to an offence are reportable regardless of amount.	Escalate immediately, preserve the suspicion timestamp and submit a complete STR to FIA.	Internal report, analysis, STR, receipt and case timeline.	FCA, s.23(1)-(2); 2020 Regulations, reg.29
An STR is due as soon as possible and no later than three days after suspicion, wherever possible before execution.	Use a shorter internal SLA measured from the documented formation of suspicion.	Suspicion timestamp, approval, submission timestamp and SLA monitoring.	FCA, s.23(1)
Tipping off and unauthorised disclosure of reports or suspicion are prohibited; reporting overrides inconsistent secrecy duties subject to legal privilege.	Restrict case access, control customer communications and train staff on permitted disclosures.	Access logs, communication plan, training and disclosure register.	FCA, ss.24-26 and 32

Threshold reports, wires and sector triggers

Keep CDD, STR and prescribed threshold-reporting duties separate.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Transactions or aggregate transactions of at least MWK 5,000,000 require the prescribed large-currency or electronic-transfer report, with timing guided by FIA.	Aggregate accurately, apply current FIA formats and timing and submit an STR separately where suspicion exists.	Threshold configuration, aggregation tests, report, FIA receipt and linked STR decision.	FCA, s.33; 2020 Regulations, reg.28
Local mobile-money or similar local transfer reporting applies to each transfer above MWK 300,000; domestic and international electronic transfers also fall within regulation 21.	Confirm current FIA file specifications and configure the correct transfer populations without treating the threshold as a CDD safe harbour.	Scope memo, transfer rules, test cases, submissions and receipts.	2020 Regulations, reg.21
Electronic transfers carry complete originator and beneficiary information; deficient transfers require risk-based execution, rejection or suspension and reporting controls.	Validate required fields through the chain, hold deficient messages and monitor persistent counterpart failures.	Field matrix, validation, repair/reject queue, monitoring and samples.	FCA, s.28; 2020 Regulations, reg.20
Casinos identify customers at entry or remote access and apply the MWK 2,000,000 24-hour transaction triggers specified in regulation 17.	Aggregate chips, gaming-machine and remote-gaming activity per customer over 24 hours and retain identification records.	Access record, aggregation, identity file and test results.	2020 Regulations, reg.17

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Implement current UN and domestic designations without delay and without prior notice.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting institutions screen against current domestic and United Nations designation lists and must not make funds or services available to designated persons.	Screen customers, beneficial owners, representatives, counterparties and transactions at onboarding and on list change.	List provenance, screening logs, population reconciliation and match decisions.	Financial Crimes (Suppression of Terrorist Financing and Proliferation) Regulations 2017, regs.8-12
Property of a designated person is frozen without delay and the competent authority is notified using the current procedure.	Maintain a 24/7 escalation path, validate matches, block access without notice and contact FIA for the live reporting route.	Match analysis, freeze timestamp, asset inventory, report and receipt.	2017 TFS Regulations, regs.11-12

9. RECORDS, ACCESS AND ASSURANCE

Records, access and assurance

Retain reconstructable evidence for the correct seven-year clock and make it promptly available.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identity, transaction, correspondence, FIA reports, unreported investigations and FIA enquiries are retained for at least seven years under class-specific clocks.	Map each record class to its statutory start event, legal hold and deletion control.	Retention schedule, system configuration, samples, legal holds and deletion tests.	FCA, s.22; 2020 Regulations, reg.19
Records must reconstruct transactions and be immediately available to FIA and competent authorities.	Index linked CDD, transaction, investigation and report evidence and test retrieval.	Request register, retrieval tests, access control and response package.	FCA, s.22(3)-(5)
Reliance on a third party does not transfer ultimate CDD responsibility.	Assess supervision and country risk, obtain core information immediately and contract for documents without delay.	Due diligence, agreement, document tests, monitoring and exit plan.	FCA, s.17

10. PRIVACY, BIOMETRICS AND TRANSFERS

Privacy, biometrics and transfers

Apply the Data Protection Act 2024 alongside AML retention and disclosure duties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Personal data needs a documented lawful basis, specified purpose, proportionate collection, accuracy, security and governed retention.	Maintain a data inventory and notices, minimise onboarding fields and reconcile AML retention with privacy deletion rules.	Inventory, lawful-basis record, notices, retention map, access and deletion logs.	Data Protection Act 2024
Biometric and other sensitive verification data require heightened necessity, access, security and vendor controls.	Complete a documented privacy and security assessment before biometric processing and preserve consent or another applicable legal condition.	Assessment, legal condition, template controls, access logs and vendor assurance.	Data Protection Act 2024
Security incidents and international transfers must follow the Act and current MACRA procedures.	Confirm live notification, registration and transfer mechanics with MACRA; maintain incident and transfer playbooks without inventing deadlines not verified in the official text.	MACRA confirmation, incident register, transfer map, contracts and assessments.	Data Protection Act 2024; Government Notice 40 of 2024

11. PRACTICAL EVIDENCE PACKS AND CHANGE CONTROL

Practical evidence packs and change control

Make every decision 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 case file, approvals and release log.	FCA, ss.16-23; 2020 Regulations
Thresholds, report channels, sanctions lists, FATF status, licensing conditions and privacy procedures require ongoing legal monitoring.	Assign owners and review FIA, RBM, CRIPC, MACRA, Gazette, FATF and ESAAMLG 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.

Financial Crimes Act (Chapter 7:07)
Malawi Gazette text via MalawiLII · Primary legislation reproduction
Open convenience reproduction

Financial Crimes (Money Laundering) Regulations, 2020
Malawi Gazette text via MalawiLII · Primary regulations reproduction
Open convenience reproduction

Financial Crimes (Money Laundering) (Amendment) Regulations, 2020
Malawi Gazette text via MalawiLII · Primary regulations reproduction
Open convenience reproduction

Financial Crimes (Suppression of Terrorist Financing and Proliferation) Regulations, 2017
Malawi Gazette text via MalawiLII · Primary regulations reproduction
Open convenience reproduction

Financial Services Act
Malawi Gazette text via MalawiLII · Primary legislation reproduction
Open convenience reproduction

Reserve Bank of Malawi
Reserve Bank of Malawi · Official regulator
Open official source

Companies Registrations and Intellectual Property Centre
CRIPC · Official company registry
Open official source

CRIPC services and beneficial-ownership updates
CRIPC · Official registry guidance
Open official source

MACRA confirmation of the Data Protection Act, 2024
MACRA · Official regulator confirmation
Open official source

Data Protection Act, 2024: Commencement
Malawi Gazette text via MalawiLII · Primary commencement notice reproduction
Open convenience reproduction

Malawi fourth enhanced follow-up report, April 2024
ESAAMLG · Authoritative regional assessment
Open official source

Jurisdictions under Increased Monitoring - 19 June 2026
FATF · Authoritative public statement
Open official source

High-Risk Jurisdictions subject to a Call for Action - 19 June 2026
FATF · Authoritative public statement
Open official source

Document control

Version 1.0 / Published 2026 / Last reviewed 17 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 17 July 2026. Confirm current Gazette amendments, FIA directives and report channels, RBM licensing conditions, CRIPC filing mechanics and MACRA data-protection procedures with Malawian counsel and the competent authority before launch. Monetary reporting thresholds, AML beneficial-ownership analysis and company-registry disclosures are distinct. VOVE ID supports evidence collection and audit trails; the reporting institution remains responsible for acceptance, reporting, freezing and compliance decisions.