VOVE ID

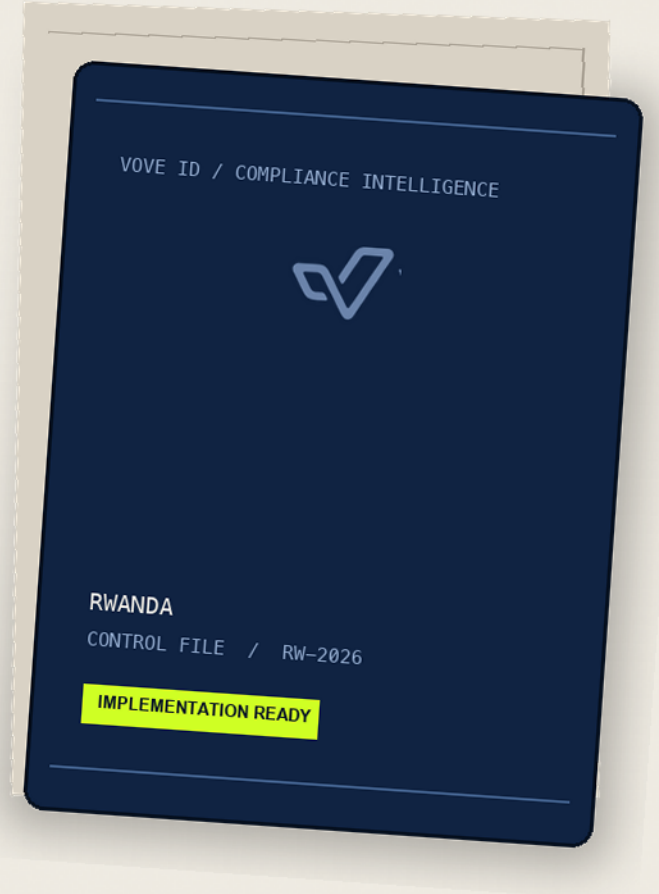
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

RWANDA

RWANDA / RW



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Rwanda KYC, KYB & AML Compliance Checklist

A practical implementation checklist for reporting persons operating in Rwanda, with a focused payment and financial-services overlay. It translates the January 2025 AML/CFT/CPF law, current FIC rules, National Bank of Rwanda requirements, RDB beneficial-ownership filings and Rwanda's personal-data law into operational controls and reviewable evidence.

Financial intelligence unit	**Financial Intelligence Centre (FIC Rwanda)**
Current AML law	**Law No. 001/2025 of 22 January 2025**
Suspicion reporting	**Within 24 hours**
Threshold-report filing	**Within 2 working days**
Record retention	**At least 10 years**
FATF public list	**Not listed as of 19 June 2026**

Scope and legal framework

Law No. 001/2025 of 22 January 2025 on the prevention and punishment of money laundering, terrorist financing and proliferation financing; Law No. 045/2021 governing the Financial Intelligence Centre as amended by Law No. 002/2025; FIC Regulation No. 002/FIC/2023, to the extent it remains in force and compatible with Law No. 001/2025; FIC Guidelines No. 001/2025 and No. 002/2025; FIC Regulation No. 001/FIC/2025 and January 2026 guidance on targeted financial sanctions; Law No. 061/2021 governing payment systems and the 2023 regulation governing payment service providers; company, partnership, trust and other legal-person laws and RDB beneficial-ownership guidance; Law No. 058/2021 relating to protection of personal data and privacy.

FATF context

Rwanda was not named in FATF's jurisdictions under increased monitoring or jurisdictions subject to a call for action statements published on 19 June 2026. This is not a low-risk designation and does not replace the reporting person's documented customer, ownership, product, channel and geographic risk assessment.

IMPORTANT

This checklist is general compliance information, not legal advice. Law No. 001/2025 is the current national AML/CFT/CPF baseline and repealed Law No. 028/2023. FIC Regulation No. 002/FIC/2023 is cited because FIC continues to publish it for operational reporting, CDD, wire and threshold rules; confirm its current application and any replacement or amendment directly with FIC. Add the current sector rules of the National Bank of Rwanda, Capital Market Authority, insurance, gaming, professional or other competent supervisor before implementation.

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.

1. SCOPE, REGISTRATION AND GOVERNANCE

Scope, registration and governance

Confirm reporting-person status, register with FIC and establish accountable, independently tested AML/CFT/CPF governance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map every reporting person and supervisor	Document which entities and activities are reporting persons under Law No. 001/2025. Map FIC obligations and the competent sector supervisor, including the National Bank of Rwanda for licensed financial institutions and payment services, CMA for capital markets and the relevant authority for DNFBPs or other regulated activities.	Entity-perimeter memo, licence inventory, supervisor matrix and named obligations owner	Law 001/2025; FIC mandate; applicable sector law
Register the reporting person with FIC	Use the FIC system to register each reporting person. Under the operational rule, register a new reporting person within 30 days after receiving its incorporation certificate and notify FIC in writing of changes to registered particulars within seven working days.	FIC registration, incorporation date, filing receipt, particulars register and change notifications	FIC Regulation 002/FIC/2023, arts. 3-4
Appoint and notify a managerial compliance officer	Designate an AML/CFT/CPF compliance officer at managerial level with sufficient authority, independence, access and resources. Notify FIC of the appointment within three working days and maintain effective cover for absence or vacancy.	Appointment, role profile, reporting line, FIC notification, access rights, deputy and resource assessment	FIC Regulation 002/FIC/2023, art. 5
Make the board and senior management accountable	Require governing and senior-management bodies to approve the programme, enterprise risk assessment, customer-acceptance standard and material remediation; receive meaningful compliance and risk reporting; and ensure the compliance function can escalate without interference.	Approved framework, committee terms, minutes, dashboards, decisions and remediation tracking	Law 001/2025; FIC Regulation 002/FIC/2023
Maintain complete internal controls	Document risk assessment, customer acceptance, CDD, beneficial ownership, PEP, sanctions, transaction monitoring, wires, reporting, records, training, privacy, agents and outsourcing. Payment service providers must maintain comprehensive and effective AML/CFT policies, procedures and controls and may not invoke banking, professional or contractual secrecy to avoid reporting.	Policy suite, regulatory mapping, approvals, version history, PSP control mapping and staff attestations	Law 001/2025; Payment Service Provider Regulation 2023, art. 46
Independently audit at least annually	Maintain an independent audit function that evaluates compliance with AML/CFT/CPF policies, procedures, controls, CDD, monitoring, reporting and records. Conduct the audit at institution level at least annually and track findings to verified closure.	Audit independence, annual plan, report, sampled controls, issue register, owners and closure proof	FIC Regulation 002/FIC/2023, art. 25

2. CUSTOMER DUE DILIGENCE AND REMOTE ONBOARDING

Customer due diligence and remote onboarding

Identify customers, representatives and beneficial owners from reliable sources before service, with equivalent controls for remote channels.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify every customer	Identify permanent and occasional customers, whether natural persons, legal persons or legal arrangements, using reliable and independent documents, data or information. Verify any representative's authority and identity and prohibit anonymous or fictitious accounts.	Identity record, verification response, representative authority, source provenance and quality review	AML Law 001/2025, arts. 12-13
Understand purpose and expected activity	Record the purpose and intended nature of the relationship, occupation or business, products, expected volumes, counterparties, countries, channels and source of funds where required by risk. Use the profile as the monitoring baseline.	Customer profile, expected-activity fields, source evidence, risk rationale and review triggers	Law 001/2025, art. 13; FIC Regulation 002/FIC/2023, arts. 6 and 9
Apply every CDD trigger and threshold	Apply CDD when establishing a relationship; for an occasional cash transaction at or above FRW 10 million; an occasional wire transfer at or above FRW 1 million; a casino transaction at or above FRW 3 million; a real-estate purchase or sale regardless of amount; and a precious-metals or precious-stones cash transaction at or above FRW 15 million. Aggregate linked transactions, and also apply CDD whenever suspicion exists or prior identification data may be unreliable.	CDD trigger and equality matrix, linked-transaction logic, completed CDD cases, suspicion escalation and refreshed verification	AML Law 001/2025, art. 12; FIC Regulation 002/FIC/2023, art. 13
Verify before or during establishment	Verify the customer and beneficial owner before or during establishment or an occasional transaction. Use deferred completion only within the narrow statutory conditions, complete it as soon as reasonably practicable and control the risks before verification finishes.	Verification chronology, permitted-deferral rationale, limits, approval, completion evidence and overdue restrictions	Law 001/2025, art. 16
Stop or exit when CDD cannot be completed	When required CDD cannot be completed, do not open the account, begin the relationship or perform the transaction; terminate an existing relationship where required; and consider filing an STR where necessary. If CDD itself would tip off a suspected customer, stop the CDD process and file an STR.	Rejected or terminated case, reason, compliance decision, STR assessment, filing receipt and non-tipping-off controls	Law 001/2025, arts. 19-20
Make remote verification equivalent to face-to-face	Identify and verify a non-face-to-face customer using procedures equivalent to face-to-face controls and implement measures against single or multiple fraudulent applications. Add document authenticity, biometric or equivalent, device, contact and behavioural controls proportionate to risk.	Remote-control design, document result, liveness or equivalent evidence, device signals, fraud rules, exceptions and quality review	FIC Regulation 002/FIC/2023, art. 11

3. KYB AND BENEFICIAL OWNERSHIP

KYB and beneficial ownership

Verify legal existence and authority, trace ownership and effective control, and reconcile AML analysis with RDB filings.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person or arrangement	Verify legal name, form, existence, registered and principal addresses, governing instruments, senior managers, registration, tax identifiers, licences and representative authority using RDB, ORG and other reliable independent sources.	Registry extract, governing documents, tax and licence checks, managers, representative authority and discrepancy log	Law 001/2025, arts. 13-14; RDB/ORG records
Identify the ultimate natural-person owner or controller	Identify and take reasonable measures to verify the natural persons who ultimately hold a controlling ownership interest. If ownership does not reveal the beneficial owner or creates doubt, identify natural persons exercising control by other means; if none is identified, record the relevant senior managing official as the statutory fallback.	Ownership chart to natural persons, controlling-interest rationale, other-control analysis, verification and fallback record	Law 001/2025, arts. 2 and 14
Identify all legal-arrangement parties	For a trust, identify and verify the settlor, trustee, protector where applicable, beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control. Apply equivalent analysis to a similar arrangement.	Trust or arrangement instrument, party register, identity verification, control map and beneficiary-class analysis	Law 001/2025, art. 14
Apply the current AML beneficial-owner cascade	Law No. 001/2025 sets no percentage. Operationalise FIC Guidelines No. 002/2025 by identifying natural persons with more than 25% of shares, at least 25% of voting rights, control by other means and, only if no natural person is identified, the senior-management fallback. Use a conservative at-least-25% implementation where systems need one threshold and document the official-text distinction.	Ownership and voting chart, threshold logic, other-control analysis, verification, fallback record and legal rationale	AML Law 001/2025, art. 14; FIC Guidelines 002/2025
File, reconcile and refresh beneficial ownership	For RDB/ORG filing, apply the registry guidance's at-least-25% ownership step plus control by other means. Keep the RDB and AML analyses separate and reconcile discrepancies. Update beneficial-owner information within 15 days after a change, after identifying outdated information, or after a specified risk trigger. Refresh higher-, medium- and lower-risk BO files at least every one, two and three years respectively, and maintain the internal register and supporting evidence.	Separate AML and registry analyses, RDB filing, 15-day change, stale-data and risk-trigger workflow, 1/2/3-year review calendar, internal register and reconciliation	FIC Guidelines 002/2025, section 6.3; RDB BO Guidelines
Verify licences and operating reality	Confirm the entity holds every required sector licence; business registration alone does not authorise financial services. Compare directors, locations, websites, settlement accounts, contracts and transaction activity to the claimed business and escalate shell or nominee indicators.	NBR or CMA licence check, RDB record, operating-footprint evidence, account match, adverse information and decision	NBR Consumer Protection Booklet; applicable licensing law

4. RISK, PEPS AND TARGETED FINANCIAL SANCTIONS

Risk, PEPs and targeted financial sanctions

Operate documented enterprise and customer risk assessment, mandatory PEP controls and immediate 2025 TFS measures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Assess enterprise-wide ML/TF/PF risk	Identify, assess, understand and document risks from customers, beneficial owners, countries, products, services, transactions, delivery channels, technologies, agents and outsourcing. Update the assessment after material change and use Rwanda's national risk assessment as an input.	Approved methodology, data inputs, assessment, residual-risk decisions, update log and remediation plan	Law 001/2025; Payment Service Provider Regulation 2023, art. 46; Rwanda NRA 2024
Assign and explain relationship risk	Assign a documented rating using ownership, PEP, sanctions, business, product, channel, transaction and geographic factors. Ensure risk drives CDD depth, approval, monitoring and review frequency and that overrides are controlled.	Scoring methodology, input data, rating, override record, approval and next-review date	Law 001/2025; FIC Regulation 002/FIC/2023
Identify PEPs and connected persons	Use risk-management systems to identify whether a customer or beneficial owner is a foreign or domestic PEP or a person entrusted by an international organisation, and identify covered family members and close associates. Repeat screening throughout the relationship.	PEP screening, relationship map, source data, alert decisions and rescreening	Law 001/2025, art. 22
Apply mandatory PEP controls	Obtain senior-management approval before establishing or continuing the relationship, take reasonable measures to establish source of wealth and source of funds and apply enhanced ongoing monitoring proportionate to risk.	Senior approval, source-of-wealth and source-of-funds substantiation, EDD file and monitoring plan	Law 001/2025, art. 22
Screen UN and domestic lists continuously	Screen customers, beneficial owners, controllers, representatives and transaction parties against current UN and Rwanda domestic designation lists before onboarding, before relevant transactions and immediately after FIC list notices. Subscribe to and operationalise current FIC public notices.	Authoritative-list inventory, notice subscription, update log, screening results, alert decisions and QA	Law 001/2025; FIC Regulation 001/FIC/2025; FIC Public Notices
Execute the exact TFS without-delay sequence	After FIC notification, complete screening within five hours. If there is no match, report that outcome within two hours after screening. If there is a match, apply the targeted financial sanctions and prohibitions and report within six hours after screening. Complete the full designation-to-screening-to-freezing-and-reporting process within 24 hours after designation. Without prior notice freeze or seize linked assets, prohibit direct or indirect availability and submit the required STR or SAR when designated assets are identified.	Designation, notification and screening timestamps, two-hour no-match report or six-hour match action, asset scope, freeze record, STR or SAR receipt and release authority	FIC Regulation 001/FIC/2025; January 2026 Without-Delay Guidance

5. ENHANCED DUE DILIGENCE AND HIGHER-RISK CONTROLS

Enhanced due diligence and higher-risk controls

Apply proportionate additional measures to higher-risk customers, jurisdictions, structures, products and counterparties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply EDD when risk or suspicion is elevated	Obtain additional identity, ownership, business, purpose, source-of-funds and source-of-wealth information; require senior approval; deepen and increase monitoring; and document why residual risk remains acceptable.	EDD checklist, corroborating records, approval, monitoring plan and review date	Law 001/2025, art. 18; FIC Regulation 002/FIC/2023, art. 8
Apply high-risk-country measures without blanket de-risking	Apply enhanced CDD and any FIC or supervisory countermeasures to relationships and transactions involving identified high-risk countries. Document the current authority, risk basis and humanitarian or legitimate-activity safeguards.	Country-risk methodology, FIC notice, EDD, countermeasure decision and exception governance	FIC Regulation 002/FIC/2023, arts. 16 and 24
Control correspondent banking	Before entering a cross-border correspondent or similar relationship, understand the respondent's business, ownership, reputation, supervision and AML controls; establish responsibilities; obtain senior approval; and prohibit shell-bank exposure and uncontrolled payable-through access.	Correspondent questionnaire, public-source checks, control assessment, approval, agreement and review	Law 001/2025, art. 23; FIC Regulation 002/FIC/2023, art. 17
Control third-party reliance	Rely on another party only under the statutory conditions, obtain CDD information immediately, ensure records can be supplied within 24 hours after request and retain ultimate responsibility. Apply group controls where reliance is intra-group.	Reliance due diligence, agreement, information receipt, 24-hour retrieval test, monitoring and exit plan	Law 001/2025, art. 28
Investigate complex and unusual transactions	Pay special attention to complex, unusual and large transactions with no apparent lawful or economic purpose. Examine background, source and purpose, document findings and submit the required report to FIC when the applicable rule requires.	Alert, investigation chronology, customer explanation, corroboration, written findings and FIC receipt	FIC Regulation 002/FIC/2023, art. 12

6. MONITORING, WIRES AND PAYMENT-SERVICE CONTROLS

Monitoring, wires and payment-service controls

Keep CDD current, monitor activity and preserve complete originator and beneficiary information through every payment role.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor transactions throughout the relationship	Monitor actual activity against the customer's purpose, business, source, expected behaviour and risk. Use appropriately calibrated scenarios, link related transactions and provide investigators with complete data and case context.	Monitoring coverage, data lineage, scenario inventory, alert cases, tuning, QA and metrics	Law 001/2025; Payment Service Provider Regulation 2023, art. 46
Refresh on risk and trigger events	Update identity, beneficial ownership, business, expected activity, PEP, sanctions and risk information according to materiality and risk and after ownership changes, unusual activity, document expiry, new products or adverse information.	Risk-based review schedule, trigger feed, updated CDD, rescreening, rating and overdue controls	Law 001/2025, art. 17; FIC Regulation 002/FIC/2023, art. 15
Capture complete wire information	Apply the required originator and beneficiary data to domestic and cross-border wire transfers, with the exact threshold treatment in the current FIC rule. Preserve account or unique-reference traceability and required identity and address or equivalent data.	Payment-message specification, validation, domestic and cross-border samples, traceability and exception report	Law 001/2025, arts. 25-27; FIC Regulation 002/FIC/2023, arts. 18 and 22
Apply ordering, intermediary and beneficiary duties	Detect missing wire information and apply role-specific verification, retention, suspension, rejection, monitoring and STR decisions. Where one provider controls both sides, consider all information from the ordering and beneficiary sides when deciding whether to report.	Role matrix, missing-data rules, repair and reject queue, decision records, retention and STR receipt	Law 001/2025, arts. 25-27; FIC Regulation 002/FIC/2023, arts. 19-21
Obtain approval for agents and material outsourcing	Obtain prior National Bank of Rwanda approval before using a payment agent and prior written approval before outsourcing an important operational function. Perform due diligence, contract for AML, privacy, records, audit and incident rights, train and monitor approved agents and providers, and retain accountability for outsourced controls.	NBR approvals, due-diligence file, contract, agent and provider registers, training, monitoring, incidents and termination log	Law 061/2021 governing payment systems, arts. 29-30
Perform PSP CDD before service and retain payer/payee identity	A payment service provider must perform CDD and KYC before providing service and retain identification information for the payer and payee regardless of their location. Map this requirement into onboarding, payment-message, retention and retrieval controls.	Pre-service CDD gate, payer and payee fields, retention configuration and retrieval test	Payment Service Provider Regulation 2023, art. 45
Prevent shell-bank relationships	A payment service provider and financial institution must not deal with shell banks or shell financial institutions or permit its accounts to be used by them. Screen counterparties and escalation indicators before and during the relationship.	Counterparty policy, ownership and physical-presence checks, attestations, screening and review	Payment Service Provider Regulation 2023, art. 46; Law 001/2025

7. REPORTING, RECORDS, PRIVACY AND ASSURANCE

Reporting, records, privacy and assurance

Meet FIC reporting clocks, preserve ten-year evidence and operate Rwanda's controller and processor registration, breach and transfer controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
File suspicious activity within 24 hours	Promptly submit an STR or suspicious-activity report to FIC within 24 hours using the template and electronic or other channel set by FIC. Report regardless of amount when the suspicion test is met and maintain strict non-tipping-off controls.	Case chronology, compliance decision, FIC report, submission receipt, access log and communication controls	FIC Regulation 002/FIC/2023, art. 29; Law 001/2025, arts. 32 and 34
Submit threshold reports within two working days	Under the published operational rule, report financial-institution cash at or above FRW 10 million, subject to the stated inter-financial-institution exception; an occasional-customer transaction above FRW 10 million; casino cash at or above FRW 3 million; precious-metals or stones dealer cash at or above FRW 15 million; and wire transfers at or above FRW 1 million. Preserve those greater-than versus at-least operators. Linked transactions are reportable when their combined total exceeds the applicable threshold. File the FIC template within two working days from the transaction day and confirm continued applicability under Law No. 001/2025.	Threshold and equality register, combined-total linked logic, reports, two-working-day timeline, receipts and legal confirmation	FIC Regulation 002/FIC/2023, arts. 31-32
Retain retrievable records for at least ten years	Keep domestic and international transaction records, CDD files, business correspondence, analysis results, STRs and other FIC reports and supporting documents for at least ten years after the transaction, relationship termination or occasional transaction. Ensure swift retrieval for competent authorities.	Retention schedule, repository controls, sample retrieval, legal holds, access logs and deletion evidence	Law 001/2025, art. 21
Register controllers and processors and appoint DPOs when triggered	Before operating as a data controller or processor, register with the Data Protection and Privacy Office and maintain a valid certificate. Apply for renewal within 45 working days before expiry and report changes. Appoint a personal-data protection officer when one of Article 40's statutory triggers applies, rather than treating appointment as universal. A non-established organisation processing data of people in Rwanda must designate a written representative in Rwanda.	Registration certificate, renewal diary, change notifications, Article 40 DPO assessment and appointment where triggered, local representative and processing inventory	Law 058/2021, arts. 29-36 and 40; DPO Registration Guide
Apply lawful, transparent and secure processing	Map processing to a lawful basis, give required notices, limit data to stated purposes, maintain accuracy, define retention, support data-subject rights, log processing, protect data with appropriate technical and organisational measures and contractually govern processors.	Lawful-basis register, notices, records of processing, rights log, security tests, access review and processor agreements	Law 058/2021, arts. 4-17, 37-42 and 46-47
Meet the 48-hour and 72-hour breach clocks	Communicate a personal-data breach to the supervisory authority within 48 hours after awareness and submit the detailed breach report no later than 72 hours. A processor must notify the controller within 48 hours. Communicate high-risk breaches to affected data subjects unless a statutory exception applies.	Incident chronology, 48-hour notice, 72-hour report, processor notice, subject communication and remediation	Law 058/2021, arts. 43-45; DPO Breach Report Form

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Separate cross-border transfer grounds from offshore storage approval	For a transfer outside Rwanda, document one of Article 48's alternative lawful grounds and the applicable safeguards; supervisory authorisation is not the only possible transfer basis. Separately, obtain the valid Article 50 certificate authorising storage of personal data outside Rwanda. Record destination, purpose, recipient, security, contracts and the selected statutory route.	Data map, Article 48 transfer assessment, safeguards, Article 50 storage certificate, contracts, security assessment and transfer register	Law 058/2021, arts. 48 and 50; DPO transfer, storage and retention guidance

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.

Law No. 001/2025 on prevention and punishment of money laundering, terrorist financing and proliferation financing
Financial Intelligence Centre Rwanda · primary
Open official source

Regulation No. 002/FIC/2023 relating to AML/CFT/CPF
Financial Intelligence Centre Rwanda · primary
Open official source

Regulation No. 001/FIC/2025 on targeted financial sanctions
Financial Intelligence Centre Rwanda · primary
Open official source

FIC Guidelines No. 002/2025 on Transparency and Beneficial Ownership
Financial Intelligence Centre Rwanda · primary
Open official source

Guidance on implementation of the without-delay principle for TFS, January 2026
Financial Intelligence Centre Rwanda · primary
Open official source

FIC Guideline No. 001/2025 on AML/CFT/CPF Independent Audit
Financial Intelligence Centre Rwanda · primary
Open official source

FIC record-keeping guidance, January 2026
Financial Intelligence Centre Rwanda · primary
Open official source

Law No. 002/2025 amending the law governing the Financial Intelligence Centre
Financial Intelligence Centre Rwanda · primary
Open official source

FIC public notices on current targeted financial sanctions
Financial Intelligence Centre Rwanda · primary
Open official source

FIC mandate and reporting responsibilities
Financial Intelligence Centre Rwanda · primary
Open official source

2024 National Money Laundering and Terrorist Financing Risk Assessment
Financial Intelligence Centre Rwanda · primary
Open official source

Regulation governing payment service providers, 2023
National Bank of Rwanda · primary
Open official source

Law No. 061/2021 governing the payment system
National Bank of Rwanda · primary
Open official source

Payment systems legal instruments
National Bank of Rwanda · primary
Open official source

Beneficial Ownership Guidelines
Rwanda Office of the Registrar General · primary
Open official source

Beneficial Ownership Requirements and Forms
Rwanda Office of the Registrar General · primary
Open official source

Beneficial Owners Register
Rwanda Development Board · primary
Open official source

Rwanda personal-data and privacy law guidance
Data Protection and Privacy Office · primary
Open official source

Personal-data sharing, transfer, storage and retention guidance
Data Protection and Privacy Office · primary
Open official source

Controller and processor registration guide
Data Protection and Privacy Office · primary
Open official source

Personal Data Breach Report Form
Data Protection and Privacy Office · primary
Open official source

Jurisdictions under Increased Monitoring, 19 June 2026
FATF · primary
Open official source

AML Compliance in Rwanda 2026
VOVE ID · contextual
Open contextual guide

KYB in Rwanda 2026
VOVE ID · contextual
Open contextual guide

Document control

Version 1.0 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general compliance information, not legal advice. Law No. 001/2025 is the current national AML/CFT/CPF baseline and repealed Law No. 028/2023. FIC Regulation No. 002/FIC/2023 is cited because FIC continues to publish it for operational reporting, CDD, wire and threshold rules; confirm its current application and any replacement or amendment directly with FIC. Add the current sector rules of the National Bank of Rwanda, Capital Market Authority, insurance, gaming, professional or other competent supervisor before implementation.