VOVE ID

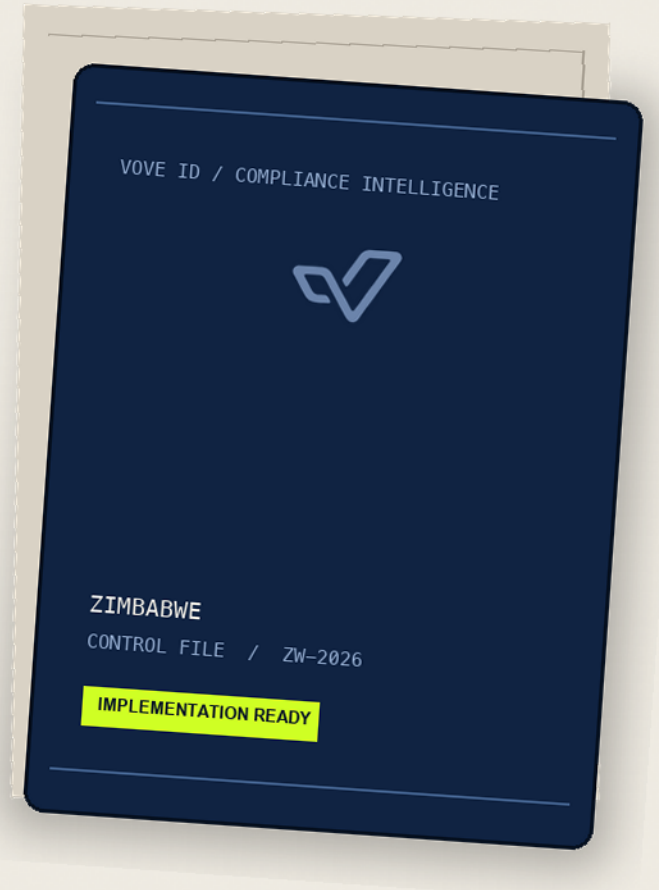
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

ZIMBABWE

ZIMBABWE / ZW



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

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

A source-backed implementation checklist for customer and business verification in Zimbabwe. It incorporates the consolidated Money Laundering and Proceeds of Crime Act through Act 7 of 2025, the RBZ 2025 banking guideline, current FIU reporting and targeted-financial-sanctions directives, company beneficial-ownership filings, payment-system oversight, the June 2026 VASP registration regime and current privacy licensing and breach rules.

Primary AML/CFT/CPF law	**Money Laundering and Proceeds of Crime Act [Chapter 9:24], consolidated through Act 7 of 2025**
Financial intelligence unit	**Financial Intelligence Unit of Zimbabwe (FIU)**
STR timing and channel	**Promptly and no later than three working days after suspicion; submit through goAML**
General occasional CDD trigger	**USD 5,000 or more, including linked transactions; suspicion and identity doubt override thresholds**
Wire CDD trigger	**USD 1,000 or more for domestic or international wires**
Core AML retention	**At least five years, with the event depending on the record class**
Company beneficial ownership	**More than 20% shares or voting rights, majority-director appointment/removal rights, or other significant influence or control; changes filed within seven days**
RBZ banking BO guide	**Identify and verify beneficial owners at 10% ownership and above, while also testing control**
Targeted financial sanctions	**Screen daily; freeze and report a confirmed match immediately and within 24 hours**
Data breach	**Notify POTRAZ within 24 hours; notify affected people within 72 hours where high risk**
VASP regime	**FIU registration under S.I. 99 of 2026; certificate valid one year; travel rule applies to all virtual-asset transfers**
FATF public lists	**Not listed in the public statements dated 19 June 2026; ESAAMLG enhanced follow-up continues**

Scope and legal framework

The Money Laundering and Proceeds of Crime Act [Chapter 9:24] is the principal AML/CFT/CPF statute for financial institutions and designated non-financial businesses and professions. FIU directives prescribe reporting and sanctions procedures, while the RBZ AML/CFT/CPF Guideline of June 2025 applies detailed expectations to banks and microfinance institutions. The Companies and Other Business Entities Act [Chapter 24:31] governs company beneficial-ownership records and filings. Payment activity is overseen under the Reserve Bank Act, National Payment Systems Act and applicable banking and payment instruments. Virtual-asset service providers are subject to S.I. 99 of 2026. The Cyber and Data Protection Act [Chapter 12:07] and S.I. 155 of 2024 govern personal-data processing, controller licensing, DPOs and breach notification.

FATF context

As at 16 July 2026, Zimbabwe was not included in either FATF public statement dated 19 June 2026. FATF removed Zimbabwe from increased monitoring in March 2022. Zimbabwe nevertheless remained in ESAAMLG enhanced follow-up after the April 2024 follow-up report upgraded Recommendation 7 to Largely Compliant. Public-list status is a dated country-risk input, not a substitute for customer-specific and transaction-specific risk assessment.

IMPORTANT

This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 16 July 2026. Confirm current gazetted law, FIU directives, RBZ conditions, company-registry forms, data-controller licensing and reporting mechanics with Zimbabwean counsel and the competent authority before launch. Sector scope matters: bank-specific guidance, company-register thresholds, AML beneficial-ownership tests and VASP rules are not interchangeable. VOVE ID can support evidence collection, screening and audit trails, but the reporting entity remains responsible for customer 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 the legal entity, product, profession and supervisor perimeter before configuring controls or launching a service.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The AML/CFT/CPF regime covers financial institutions and designated non-financial businesses and professions, including the categories defined in the Act.	Map every entity, product, customer flow, profession, branch, agent and outsourced activity to its statutory category and competent supervisor.	Signed perimeter memorandum, entity-product matrix, licences and supervisor map.	Money Laundering and Proceeds of Crime Act [Chapter 9:24] (MLPC Act), ss. 2, 13 and First Schedule
The FIU administers the reporting framework, receives reports and may issue binding directives; sector supervisors retain their licensing and supervisory roles.	Assign authority contacts, goAML credentials, alternates, reporting ownership and a controlled regulatory calendar.	Authority map, FIU registration, goAML access register, appointments and reporting calendar.	MLPC Act, ss. 4-6G and 30; FIU legal-framework and directives pages
Retail payment, switching, mobile-money and related payment activity requires the applicable RBZ approval before operation; non-bank applicants follow the current partnership and submission conditions stated by RBZ.	Obtain an RBZ classification and every required approval before pilot or live launch, and track conditions, agents, settlement, interoperability and consumer-protection duties.	RBZ approval, classification, approved product map, conditions register, bank-partner agreement and agent inventory.	National Payment Systems Act [Chapter 24:23]; RBZ National Payment Systems approval requirements; S.I. 80 of 2020
A person providing virtual-asset services must be registered with the FIU under S.I. 99 of 2026; applicants must be Zimbabwe-in corporated or operate through a Zimbabwe subsidiary.	Do not offer exchange, transfer, custody, administration or issuer-related virtual-asset services until the FIU issues the applicable registration certificate and conditions.	VASP perimeter analysis, Zimbabwe incorporation, application pack, FIU certificate, conditions and renewal calendar.	MLPC Act, s. 2 definition of financial institution; S.I. 99 of 2026, ss. 4-9

Governance, risk assessment and control ownership

Use documented ML, TF and proliferation-financing risk to design accountable, tested and resourced controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting institutions assess and mitigate customer, country, product, service, transaction and delivery-channel ML/TF/PF risk and apply proportionate measures.	Maintain enterprise and customer-risk methodologies, data inputs, inherent and residual ratings, mitigants, overrides and approval.	Risk methodology, enterprise assessment, customer model, risk register, remediation plan and approval.	MLPC Act, s. 12B; RBZ AML/CFT/CPF Guideline, paras. 2.1-2.49
Banks and microfinance institutions under the RBZ guideline review their institutional risk assessment at least annually and assess new products and technologies before launch.	Set an annual review and a pre-launch gate covering AML/CFT/CPF, fraud, sanctions, cyber and privacy risk.	Annual assessment, product assessment, control sign-offs, test results and release decision.	RBZ AML/CFT/CPF Guideline, paras. 2.8-2.9 and 3.9-3.11
An AML/CFT/CPF programme includes policies and controls, employee screening, ongoing training, technology-misuse controls and independent audit.	Approve a complete programme, name control owners, resource independent testing and track corrective action to closure.	Board-approved policies, owner register, training, screening, audit plan, reports and remediation tracker.	MLPC Act, s. 25(1); RBZ AML/CFT/CPF Guideline, Part 3
A management-level compliance officer must oversee implementation and have ready access to books, records and employees.	Document appointment, authority, independence, information access, deputies and direct reporting to senior management and the board.	Appointment resolution, charter, access matrix, resource plan and governance reports.	MLPC Act, s. 25(2)-(3); RBZ AML/CFT/CPF Guideline, paras. 3.22-3.32

Natural-person identification and CDD

Identify, verify and understand customers at every statutory trigger and before activation except for a narrow controlled timing exception.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD applies when establishing a relationship, at an occasional transaction of USD 5,000 or more including linked transactions, at a wire of USD 1,000 or more, whenever suspicion exists and whenever earlier identity evidence is doubtful.	Configure relationship, aggregation, wire, suspicion and identity-doubt triggers; never use a monetary threshold to suppress suspicion-driven CDD.	CDD trigger matrix, aggregation logic, configuration, test cases and exceptions.	MLPC Act, s. 15(1); RBZ AML/CFT/CPF Guideline, para. 3.36
Sector-specific triggers also apply: gaming operators at USD 3,000 and precious-stones or precious-metals dealers receiving currency at USD 15,000, subject to any current prescribed change.	Keep sector thresholds in a governed register and link each threshold to the correct activity and customer population.	Sector analysis, threshold register, configuration and periodic legal check.	MLPC Act, s. 15(2)
Natural-person identity is verified with an official identity document; the customer definition includes signatories, authorised persons and attempted actors.	Validate identity attributes and document authenticity, screen the person and separately verify every representative's authority.	Identity copy, authenticity result, source provenance, screening and mandate.	MLPC Act, ss. 13, 15 and 17; RBZ AML/CFT/CPF Guideline, paras. 3.34-3.50
CDD captures the purpose and intended nature of the relationship and enough information to understand the customer's business and expected activity.	Record products, volumes, values, counterparties, countries, source of funds where appropriate and an approved expected-activity baseline.	Customer profile, purpose statement, expected-activity baseline, source evidence and risk score.	MLPC Act, s. 17(e)-(f); RBZ AML/CFT/CPF Guideline, para. 3.49
Identity verification normally precedes the relationship; limited deferral is allowed only where delay is unavoidable for normal business and ML/TF/PF risk is adequately controlled.	Use a documented exception with restrictions, completion deadline and escalation; do not treat deferral as routine onboarding.	Exception approval, risk rationale, account restrictions, completion timestamp and overdue report.	MLPC Act, s. 16; RBZ AML/CFT/CPF Guideline, paras. 3.43-3.47

KYB, registries and beneficial ownership

Verify legal existence, authority and the natural persons who ultimately own or control the entity; apply the threshold appropriate to the legal context.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Legal-person CDD covers name, address, directors, incorporation, legal form, binding authority, ownership and control.	Verify these from current registry, constitutional, licence, tax and mandate evidence; reconcile inconsistencies.	Registry extract, constitutive documents, licences, directors, mandate and discrepancy log.	MLPC Act, s. 17(b); RBZ Guideline, para. 3.49
AML CDD identifies the natural-person beneficial owner; 25% or more ownership or voting control is a deemed test, but other control still applies.	Trace all layers, calculate interests, identify the transaction beneficiary and test effective control.	Ownership chart, calculations, declarations, control analysis and verified BO files.	MLPC Act, ss. 13 and 15(2)-(3)
RBZ's 2025 guide directs banks and microfinance institutions to identify and verify BOs at 10% ownership and above, alongside control tests.	Configure the 10% floor for covered institutions and investigate control, nominees and higher-risk ownership.	Scope memo, configuration, ownership chart, control analysis and tests.	RBZ Guideline, paras. 2.21 and 3.37-3.42
Company-law BO means more than 20% of shares or votes, majority-director appointment or removal rights, or other significant influence or control.	Maintain the company's current BO register using every statutory limb, not shareholding alone.	Company BO register, identity and control evidence, resident custodian and review log.	Companies and Other Business Entities Act, ss. 2 and 72
A company files current BO information and any material change with the Registrar within seven days.	Use the current form and reconcile the company register, Registrar filing and AML CDD record.	Declaration, receipt, seven-day change log and reconciliation.	Companies and Other Business Entities Act, s. 72(2); S.I. 46/2020

PEPs, enhanced due diligence and remote onboarding

Higher-risk, politically exposed and non-face-to-face relationships require additional evidence, accountable approval and closer monitoring.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Systems must determine whether a customer or beneficial owner is a PEP and distinguish foreign PEPs from domestic or international-organisation PEPs according to risk.	Screen before activation and continuously, resolve matches with reliable role evidence and extend controls to required family members and close associates.	Screening result, role and relationship evidence, match decision, risk rationale and review log.	MLPC Act, ss. 13 and 20; RBZ AML/CFT/CPF Guideline, paras. 3.64-3.68
Applicable PEP relationships require senior-management approval, reasonable measures to establish source of wealth and source of funds or assets and increased ongoing monitoring.	Obtain and corroborate source evidence, record approval before starting or continuing the relationship and configure enhanced monitoring.	Source-of-wealth and source-of-funds file, approval, monitoring plan and reviews.	MLPC Act, s. 20; RBZ AML/CFT/CPF Guideline, para. 3.68
High-risk customers, products, services and situations receive enhanced measures; simplified measures are permitted only for substantiated low risk and do not remove CDD or monitoring.	Define risk-based standard, enhanced and simplified control sets, eligibility rules, prohibited overrides and review frequency.	Risk-control matrix, low-risk rationale, EDD file, approvals and override log.	MLPC Act, ss. 12B and 20; RBZ AML/CFT/CPF Guideline, paras. 3.71-3.76
Non-face-to-face business must use measures no less effective than in-person due diligence and address impersonation and document risk.	Use risk-based document integrity, liveness or presence, independent data, device and fraud checks and governed manual review.	Remote-onboarding standard, vendor assurance, test pack, fraud logs and exceptions.	MLPC Act, s. 19; RBZ AML/CFT/CPF Guideline, paras. 3.57-3.63
If required CDD cannot be completed, do not establish or maintain the relationship and report immediately to the FIU; avoid pursuing CDD where it would tip off a suspected customer.	Route failed or unsafe CDD to decline, restriction or exit and a confidential reporting decision without alerting the customer.	Failure reason, decline or exit, immediate report or STR decision, submission and restricted access log.	MLPC Act, ss. 22 and 31; RBZ AML/CFT/CPF Guideline, paras. 3.69-3.70 and 3.130

Monitoring, suspicious reporting and confidentiality

Monitor the relationship continuously and submit complete reports through the prescribed FIU channel on time.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Ongoing due diligence keeps customer and beneficial-owner data current and examines transactions against the known customer, activities and risk profile.	Configure risk-based refresh, event triggers and transaction monitoring and investigate material deviations from expected activity.	Refresh schedule, trigger log, monitoring scenarios, alerts, cases and updated CDD.	MLPC Act, s. 26; RBZ AML/CFT/CPF Guideline, paras. 2.47-2.51 and 3.71-3.78
Complex, unusual large or purposeless transactions and unusual patterns require special attention, written findings and retention.	Document background, purpose, actors, source and destination of funds, corroboration and the final reporting decision.	Enhanced-review memorandum, transaction data, supporting evidence, decision and reviewer sign-off.	MLPC Act, ss. 24 and 26(2)
A financial institution, DNFBP and covered officers or agents report property, a transaction or an attempted transaction suspected or reasonably suspected to involve crime, terrorism, terrorist financing or proliferation.	Escalate immediately, preserve the suspicion timestamp and submit a complete STR to the FIU through goAML.	Internal report, analysis, STR, goAML receipt, case timeline and any supplement.	MLPC Act, s. 30(1); RBZ AML/CFT/CPF Guideline, paras. 3.104-3.110
An STR is due promptly and no later than three working days after suspicion is formed; attempted transactions are reportable.	Use a shorter internal SLA that leaves time for review and measure from the documented point at which suspicion was formed.	Suspicion timestamp, internal SLA, approval, submission timestamp and overdue report.	MLPC Act, s. 30(1); RBZ AML/CFT/CPF Guideline, paras. 3.105-3.108
Tipping off is prohibited and reporting information is protected; secrecy duties do not block statutory reporting.	Restrict STR access, suppress customer-facing indicators, train staff and separate lawful information requests from prohibited disclosure.	Access matrix, immutable case log, training, communications controls and access review.	MLPC Act, ss. 31-33; RBZ AML/CFT/CPF Guideline, paras. 3.126-3.132

Payments, wires, threshold reports and virtual assets

Keep CDD triggers, automatic threshold reports, wire data and virtual-asset travel-rule controls distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Qualifying wires carry accurate originator and beneficiary data; incomplete transfers require risk-based repair, rejection or suspension.	Validate fields before execution, retain data across the chain and govern missing-data decisions.	Field specification, rules, repair/reject queue, samples and logs.	MLPC Act, s. 27; RBZ Guideline, paras. 3.143-3.156
For banks, Directive 01/04/2024 sets CTR/EFT thresholds at ZiG 70,000 local or USD 5,000 equivalent foreign currency, and IFT at USD 5,000 equivalent.	Configure separate report types and currency rules and re-check the FIU for changes.	Threshold register, system and currency rules, tests and dated check.	FIU Directive 01/04/2024, para. 2.1
Banks submit weekly threshold and nil returns on or before the second working day of the week.	Reconcile, approve and submit each CTR, EFT and IFT return through goAML on time.	Reconciliation, return, approval, receipt and overdue log.	FIU Directive 01/04/2024, para. 2.2
NBFIs and DNFBPs submit CTR or nil returns at ZiG 70,000 local or USD 5,000 equivalent foreign currency monthly by the tenth day.	Confirm scope, reconcile the monthly return and retain the goAML acknowledgement.	Scope, configuration, return, reconciliation and receipt.	FIU Directive 01/04/2024, paras. 3.1-3.2
A suspicious threshold transaction requires separate STR and threshold reports.	Link but do not merge the cases; preserve separate grounds, reports and receipts.	Linked IDs, STR, threshold return, receipts and decision.	RBZ Guideline, paras. 3.133-3.135
S.I. 99/2026 applies travel data to all virtual-asset transfers, CDD at USD 1,000 or more and wallet-ownership proof above USD 1,000 for unhosted wallets.	Verify and transmit travel data, detect missing fields, prove wallet control and monitor risk.	Travel messages, KYC, wallet proof, decision and monitoring.	S.I. 99/2026, ss. 17-21

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Use current UN lists and FIU instructions to identify, freeze and report designated assets without prior notice.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
FIs, DNFBPs and other natural and legal persons apply Zimbabwe's UN target ed-financial-sanctions framework for terrorism and proliferation financing.	Maintain a legal list inventory, FIU/goAML registration, accountable sanctions owner and procedures for designation, delisting and false positives.	List inventory, subscriptions, procedure, role assignment and change log.	S.I. 76 of 2014; S.I. 110 of 2021; FIU CFT/CPF Directive PFIU3/09/24
Screen existing and potential customers, beneficial owners, transaction parties, directors and agents before onboarding or an occasional transaction and thereafter daily.	Run daily list updates and rescreening, pre-transaction checks and real-time cross-border payment screening where applicable.	List versions, screening timestamps, population reconciliation, alerts and match decisions.	FIU CFT/CPF Directive PFIU3/09/24, Part 3; RBZ AML/CFT/CPF Guideline, paras. 3.79-3.83
A confirmed match triggers freezing without delay, immediately and in any case within 24 hours, without prior notice, plus a prohibition on funds, assets, services or economic resources being made available.	Block accounts, transactions and services, identify all directly or indirectly owned or controlled assets and prevent movement until lawful release.	Match validation, freeze timestamp, asset inventory, transaction blocks, access log and release authority.	FIU CFT/CPF Directive PFIU3/09/24, Part 3; S.I. 76 of 2014; S.I. 110 of 2021
A confirmed match and action taken are reported to the FIU through goAML immediately and no later than 24 hours; a nil return is submitted when an FIU list update yields no match.	Submit the designated-person and asset particulars and action taken, file any required nil return and assess an STR separately where TF or PF is suspected.	GoAML sanctions report, receipt, nil return, STR decision and linked case record.	FIU CFT/CPF Directive PFIU3/09/24, Reporting; RBZ AML/CFT/CPF Guideline, paras. 4.11-4.17

Records, confidentiality and regulator access

Retain reconstructable records for the correct event-based period and make them available promptly to authorised authorities.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD files, account records and business correspondence are retained for at least five years after the relationship ends; transaction records are retained for at least five years from the transaction.	Map every record class to the correct start event, legal hold, access rule and deletion control.	Retention schedule, lifecycle configuration, legal-hold procedure, archive and deletion test.	MLPC Act, s. 24(2)(a)-(b)
Written findings for complex or unusual activity and copies of STRs and supporting material are retained for at least five years from the transaction or report, as applicable.	Store analysis and reports in a restricted archive linked to the relevant customer and transaction without exposing the filing.	Restricted case archive, linkage, retention configuration and access review.	MLPC Act, s. 24(2)(c)-(d); RBZ AML/CFT/CPF Guideline, paras. 3.138-3.142
Where a technical limitation separates required cross-border wire data from the related domestic transfer, the intermediary institution keeps the received information for at least ten years.	Preserve detached wire data with a reliable transaction link and test complete reconstruction.	Wire archive, linkage key, ten-year rule, retrieval and reconstruction test.	MLPC Act, s. 27(8)
Records and underlying information must be available on a timely basis to the FIU and authorised competent authorities; third-party reliance does not transfer responsibility.	Authenticate requests, apply least-privilege disclosure, retrieve promptly and log the response and chain of custody.	Request register, authentication, response package, access log and retrieval test.	MLPC Act, ss. 18 and 24; RBZ AML/CFT/CPF Guideline, para. 3.142

10. PRIVACY, BIOMETRICS AND INTERNATIONAL TRANSFERS

Privacy, biometrics and international transfers

AML necessity does not remove data-protection duties. Identity and biometric processing require lawful purpose, licensing, security, rights and transfer controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A person deciding the means, purpose or outcome of personal-data processing, the data collected or the people concerned, or processing for commercial benefit must apply for the applicable POTRAZ data-controller licence unless exempt.	Classify the controller, confirm the correct tier with POTRAZ, obtain the licence and renew it at least three months before its 12-month expiry.	Applicability analysis, DP1 application, licence, tier confirmation, fees and renewal calendar.	Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024 (S.I. 155 of 2024), ss. 3-8
A data controller appoints a qualified and certified DPO and notifies POTRAZ; DPO contact changes and termination are notified within 14 days and a replacement is appointed within 90 days.	Appoint an independent DPO, file Form DP2, publish contact routes and maintain succession and notification triggers.	Appointment, certification, DP2, POTRAZ receipt, contact notice and succession calendar.	S.I. 155 of 2024, ss. 12-14
Processing must be necessary, fair, lawful, purpose-limited, accurate, minimised and retained no longer than necessary; data subjects have information, access, objection, correction and deletion rights.	Maintain notices, purpose and basis records, data inventory, minimisation and retention rules and a tested rights-request workflow.	Privacy notice, processing inventory, lawful-basis register, retention schedule, rights log and responses.	Cyber and Data Protection Act [Chapter 12:07], ss. 7-14
Genetic, biometric and health data generally require written consent unless a statutory exception applies; POTRAZ must also be notified of biometric or genetic processing.	Document the lawful condition, collect and preserve written consent where relied on, offer withdrawal mechanics and notify POTRAZ before production.	Biometric assessment, written consent or exception memo, POTRAZ notice, withdrawal log and access controls.	Cyber and Data Protection Act, ss. 11-12; S.I. 155 of 2024, s. 10(2)(d)

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Controllers and processors use appropriate technical and organisational security and a written processing agreement; a personal-data breach is notified to POTRAZ within 24 hours of awareness.	Contract processors, test security and incident response, use Form DP3 and preserve a complete breach record and investigation.	Processor agreement, security assessment, incident log, DP3, POTRAZ receipt and investigation report.	Cyber and Data Protection Act, ss. 18-19; S.I. 155 of 2024, ss. 16-17
Where a breach is likely to create high risk for individual rights and freedoms, affected data subjects are informed within 72 hours; the controller responds to authority requests within 14 days and concludes and reports its investigation within 21 days from notification.	Classify breach risk, prepare individual notice, track authority questions and complete the investigation and final report on the statutory clocks.	Risk assessment, individual notice, delivery proof, authority responses, investigation and final report.	S.I. 155 of 2024, s. 17(3)-(5)
Foreign transfers require adequate protection or a statutory section 29 condition; S.I. 155 also requires notification to POTRAZ of intended foreign transfer or sharing.	Map hosting and support locations, assess adequacy or the transfer condition, notify POTRAZ and obtain any current required authorisation before transfer.	Transfer map, assessment, contracts, POTRAZ notification or authorisation, security controls and review.	Cyber and Data Protection Act, ss. 28-29; S.I. 155 of 2024, s. 10(2)(c)

11. IMPLEMENTATION AND AUDIT EVIDENCE PACK

Implementation and audit evidence pack

A defensible programme links every legal claim to configuration, ownership, dated sources, testing and a controlled residual-risk decision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A pre-launch gate covers perimeter, licensing, CDD, beneficial ownership, PEPs, monitoring, reporting, sanctions, records, privacy, payments and virtual assets.	Block production until accountable owners approve control design and every material gap has a closed remediation or explicit lawful launch condition.	Launch checklist, approvals, test pack, gap register and release decision.	MLPC Act; applicable FIU, RBZ, company, VASP and data-protection instruments
Agents, outsourced KYC providers, cloud services, processors and other vendors do not remove the regulated entity's accountability.	Assess providers, contract evidence access, audit, security and confidentiality, monitor performance, test retrieval and maintain an exit plan.	Due-diligence file, contract, audit and access test, monitoring reports, issues and exit plan.	MLPC Act, s. 18; S.I. 155 of 2024, s. 10(4)(f); RBZ NPS approval requirements
Thresholds, FATF lists, UN designations, FIU directives, RBZ conditions, VASP registration and privacy forms can change.	Assign owners to monitor official FIU, RBZ, Companies Office, POTRAZ, Gazette, FATF and ESAAMLG sources and assess every change against systems and existing customers.	Legal inventory, source log, change assessment, implementation ticket and approval.	Official authority and international publications listed in Sources
Independent assurance tests the complete customer lifecycle and preserves why each production rule is configured as it is.	Sample onboarding, ownership, PEP, sanctions, thresholds, wires, STRs, privacy, access and retention; report findings and verify closure.	Control-to-law map, monitoring plan, audit report, issue register, closure evidence and release history.	MLPC Act, s. 25(1)(e); RBZ AML/CFT/CPF Guideline, paras. 3.98-3.103

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.

Money Laundering and Proceeds of Crime Act [Chapter 9:24], updated through Act 7 of 2025
Financial Intelligence Unit of Zimbabwe · Primary legislation
Open official source

Zimbabwe AML/CFT legal framework
Financial Intelligence Unit of Zimbabwe · Official legal-framework register
Open official source

FIU directives register
Financial Intelligence Unit of Zimbabwe · Official directives register
Open official source

Revised thresholds for CTRs, EFTs and IFTs, Directive 01/04/2024
Financial Intelligence Unit of Zimbabwe · Binding FIU directive
Open official source

Targeted-financial-sanctions Directive PFIU3/09/24
Financial Intelligence Unit of Zimbabwe · Binding FIU directive
Open official source

High-risk and increased-monitoring jurisdictions Directive PFIU17/02/2026
Financial Intelligence Unit of Zimbabwe · Binding FIU directive
Open official source

FIU guidelines register
Financial Intelligence Unit of Zimbabwe · Official guidance register
Open official source

goAML reporting portal
Financial Intelligence Unit of Zimbabwe · Official reporting platform
Open official source

Inspection notice on goAML registration and CTR submissions, 8 May 2025
Financial Intelligence Unit of Zimbabwe · Official compliance notice
Open official source

AML/CFT/CPF Guideline, June 2025
Reserve Bank of Zimbabwe · Binding sector guideline
Open official source

RBZ National Payment Systems legal basis
Reserve Bank of Zimbabwe · Official regulator guidance
Open official source

RBZ retail payment-system approval requirements
Reserve Bank of Zimbabwe · Official licensing requirements
Open official source

National Payment Systems guidelines, directives and circulars
Reserve Bank of Zimbabwe · Official sector register
Open official source

Banking (Money Transmission, Mobile Banking and Mobile Money Interoperability) Regulations, 2020
Reserve Bank of Zimbabwe · Primary sector regulation
Open official source

Guidelines for QR Code Payments in Zimbabwe, March 2026
Reserve Bank of Zimbabwe · Current sector guideline
Open official source

Money Laundering and Proceeds of Crime (Virtual Asset Service Providers Registration) Regulations, 2026
Financial Intelligence Unit of Zimbabwe · Primary sector regulation
Open official source

Companies and Other Business Entities Act [Chapter 24:31]
Zimbabwe Legal Information Institute · Primary legislation
Open official source

Companies and Other Business Entities (Pre-Formation and Post-Formation Formalities) Regulations, 2020
Zimbabwe Investment and Development Agency eRegulations · Primary regulation and forms
Open official source

Cyber and Data Protection Act [Chapter 12:07]
Ministry of Information Communication Technology, Postal and Courier Services · Primary legislation
Open official source

Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024
POTRAZ · Primary regulation
Open official source

Data Controller Licence Application Form DP1
POTRAZ Data Protection Authority · Official form
Open official source

FATF jurisdictions under increased monitoring, 19 June 2026
FATF · Official international status statement
Open official source

FATF high-risk jurisdictions subject to a call for action, 19 June 2026
FATF · Official international status statement
Open official source

FATF Plenary outcome removing Zimbabwe from increased monitoring, March 2022
FATF · Official international status statement
Open official source

Zimbabwe follow-up report, April 2024
FATF / ESAAMLG · Official peer-review status
Open official source

Zimbabwe country and mutual-evaluation page
ESAAMLG · Official regional assessment register
Open official source

UN Security Council consolidated sanctions list
United Nations · Official sanctions list
Open official source

Document control

Version 1.0 / Published 2026 / Last reviewed 16 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 16 July 2026. Confirm current gazetted law, FIU directives, RBZ conditions, company-registry forms, data-controller licensing and reporting mechanics with Zimbabwean counsel and the competent authority before launch. Sector scope matters: bank-specific guidance, company-register thresholds, AML beneficial-ownership tests and VASP rules are not interchangeable. VOVE ID can support evidence collection, screening and audit trails, but the reporting entity remains responsible for customer acceptance, reporting, freezing and compliance decisions.