VOVE ID

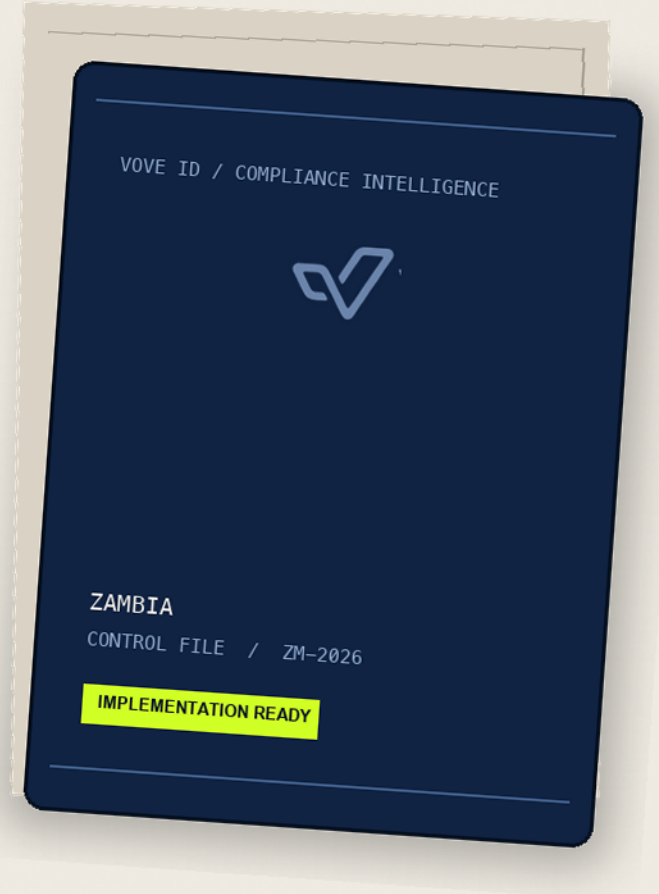
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

ZAMBIA

ZAMBIA / ZM



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Zambia KYC, KYB & AML Compliance Checklist

A practical implementation checklist for financial institutions, payment providers, virtual-asset businesses and other reporting entities operating in Zambia.

Financial intelligence unit	**Financial Intelligence Centre (FIC)**
STR deadline	**Within three working days of forming suspicion**
Currency transaction reporting	**USD 10,000 or more, including linked transactions where applicable**
AML record retention	**At least 10 years from the applicable transaction, occasional transaction or relationship-termination date**
FATF public list	**Not listed in the FATF public statements issued on 19 June 2026**

Scope and legal framework

Financial Intelligence Centre Act No. 46 of 2010, as amended by Act No. 4 of 2016 and Act No. 16 of 2020; Financial Intelligence Centre (General) Regulations, 2022 (S.I. No. 54 of 2022); Financial Intelligence Centre (Prescribed Threshold) Regulations, 2022 (S.I. No. 53 of 2022); Anti-Terrorism and Non-Proliferation Act No. 30 of 2024 and related statutory instruments; Companies Act No. 10 of 2017, as amended by the Companies (Amendment) Act No. 12 of 2020; National Payment Systems Act No. 1 of 2007; Banking and Financial Services Act No. 7 of 2017; Data Protection Act No. 3 of 2021, applicable regulations and the 2025 data-protection code

FATF context

Zambia is not listed in either FATF public statement issued on 19 June 2026: Jurisdictions under Increased Monitoring or High-Risk Jurisdictions subject to a Call for Action. Continue risk-based country screening against each current FATF statement and any applicable sanctions lists.

IMPORTANT

Operational guidance, not legal advice. Requirements vary by reporting-entity category, licence, product and supervisor. Confirm the current consolidated legislation, FIC directions, BoZ conditions, PACRA filings and data-protection instruments 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. REGULATORY PERIMETER AND REGISTRATION

Regulatory perimeter and registration

Establish the entity's reporting, licensing and supervisory perimeter before launching or changing a product.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map the regulatory perimeter	Document each legal entity, product, payment flow, delivery channel, customer segment and jurisdiction. Determine whether it is a financial institution, DNFBP, VASP or other reporting entity and identify FIC, BoZ, PACRA and any sector supervisor obligations.	Approved regulatory-perimeter memo, product inventory and licence register	FIC Act No. 46 of 2010, as amended; FIC AML/CFT Framework; BoZ regulatory framework
Maintain licences and registrations	Obtain and maintain every applicable BoZ licence, payment-system approval, PACRA registration and FIC reporting-entity registration or notification. Escalate changes in ownership, control, products or operating model before implementation.	Licences, FIC and supervisor correspondence, renewal calendar and change approvals	National Payment Systems Act No. 1 of 2007; Banking and Financial Services Act No. 7 of 2017; FIC Act
Identify the accountable supervisory authority	Assign an owner for each regulator and maintain the relevant reporting, inspection, information-request and remediation procedures.	Regulatory-obligations register, named owners and reporting calendar	FIC AML/CFT Framework; FIC General Guidelines 2017
Control outsourcing and agents	Risk-assess agents, distributors, outsourced KYC providers and technology vendors before appointment; contract for access, audit, confidentiality, AML/CFT controls and data-protection obligations.	Third-party due-diligence file, contract clauses and oversight reviews	FIC Act, section 23; FIC General Regulations 2022; Data Protection Act No. 3 of 2021

2. GOVERNANCE, COMPLIANCE OFFICER AND POLICIES

Governance, compliance officer and policies

Put accountable senior management, an independent compliance function and documented controls in place.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Designate an eligible compliance officer	Designate a compliance officer at senior-management level. Confirm the person meets the statutory experience, integrity, certification and FIC-approval requirements and has access to the books, records and employees needed to perform the role.	Appointment resolution, eligibility assessment, FIC approval or certification record and access matrix	FIC Act, section 23, as amended by Act No. 16 of 2020
Adopt an AML/CFT/CPF programme	Maintain board-approved policies covering risk assessment, CDD, beneficial ownership, PEPs, sanctions, monitoring, reporting, record keeping, confidentiality, training and independent testing.	Board minutes, current policy suite, control-owner register and annual approval record	FIC Act, section 23, as amended; FIC General Guidelines 2017
Provide protected internal escalation	Require staff to escalate knowledge, suspicion or reasonable grounds for suspicion promptly to the compliance officer, protect whistleblowing channels and preserve decision records.	Internal-reporting procedure, case log, access controls and staff acknowledgement	FIC Act; FIC Guidance Note on STR Reporting 2022
Train and independently test controls	Deliver role-based AML/CFT/CPF, sanctions and privacy training, including to agents where relevant, and arrange periodic independent audit or testing of the programme.	Training curriculum, attendance and assessment records, audit plan and remediation tracker	FIC Act, section 23; FIC Guidelines on AML/CFT Policy 2020; FIC Guidelines on Independent Audit 2021

3. ENTERPRISE AND CUSTOMER RISK ASSESSMENT

Enterprise and customer risk assessment

Use a documented risk-based approach to calibrate onboarding, monitoring and review intensity.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Assess enterprise ML/TF/PF risk	Assess inherent and residual risks across customers, products, services, transactions, delivery channels, technologies, agents and geographies. Record controls, residual-risk ratings and remediation deadlines.	Enterprise risk assessment, methodology, risk register and management approval	FIC General Regulations 2022, regs. 8-10; FIC Guidelines on ML/TF/PF Risk Assessment 2021
Risk-assess products before launch	Complete AML/CFT/CPF, fraud, sanctions and data-protection assessments before launching a product, new technology, virtual-asset service, agent channel or material change.	Product-approval checklist, risk assessment and control sign-offs	FIC General Regulations 2022; FIC AML/CFT Framework; Data Protection Act No. 3 of 2021
Risk-rate each relationship	Assign and explain customer-risk ratings using customer, ownership, PEP, sanctions, product, channel, transaction and geographic factors. Govern overrides and set risk-based refresh dates.	Scoring model, input data, approval record, override log and review schedule	FIC General Regulations 2022, regs. 8-10
Use simplified measures only when justified	Apply simplified CDD only after a documented low-risk assessment and never where suspicion, sanctions exposure or another high-risk factor requires stronger controls.	Low-risk assessment and approved simplified-control configuration	FIC General Regulations 2022, reg. 9

4. KYC AND CUSTOMER DUE DILIGENCE

KYC and customer due diligence

Identify, verify and understand customers and representatives before or when establishing the relationship, subject only to lawful risk-controlled timing exceptions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify natural persons	Obtain reliable identity information and independently verify it using appropriate documents, data or information. Record the verification method, result and any discrepancy resolution.	KYC checklist, identity documents, verification response and exception record	FIC Act, section 18; FIC General Regulations 2022, reg. 7
Identify representatives and authority	Identify and verify every person acting for a customer and verify authority through a mandate, resolution, power of attorney or comparable instrument.	Representative KYC, authority instrument and mandate matrix	FIC Act, section 18; FIC General Regulations 2022, reg. 7
Understand purpose and intended activity	Record the purpose and intended nature of the relationship, expected products, volumes, transaction values, counterparties, geographies and source of funds appropriate to the risk.	Customer profile, expected-activity baseline and source-of-funds records	FIC Act, section 18; FIC General Regulations 2022, reg. 7
Apply ongoing CDD and refresh triggers	Monitor transactions and customer information throughout the relationship, refresh CDD when risk, ownership, activity, documents or circumstances change, and investigate activity inconsistent with the profile.	Refresh schedule, trigger log, updated KYC pack and monitoring cases	FIC Act, sections 18 and 20; FIC General Regulations 2022
Handle failed CDD safely	Where required CDD cannot be completed, do not establish or continue the relationship or complete the transaction unless lawfully permitted; consider an STR without tipping off the customer.	Decline, restriction or exit record and STR decision record	FIC Act, sections 18 and 29; FIC General Regulations 2022

5. KYB AND BENEFICIAL OWNERSHIP

KYB and beneficial ownership

Verify the legal person or arrangement, its authority structure and the natural persons who ultimately own, control or benefit from it.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence and status	Obtain and independently verify incorporation or registration, legal form, registered office, principal business address, directors, tax information and current status from PACRA or the competent registry.	Registry extract, constitutional documents, tax and licence checks and status verification	FIC Act, section 18; Companies Act No. 10 of 2017; PACRA service information
Identify natural-person beneficial owners	Trace direct and indirect ownership and control through each layer to the natural persons who ultimately own, control, exercise substantial interest in or receive substantial economic benefit from the customer, including the person on whose behalf a transaction is conducted.	Ownership chart, beneficial-owner declaration, supporting filings and independent corroboration	Companies Act No. 10 of 2017, as amended; PACRA, Who is a beneficial owner?
Assess control beyond shareholding	Assess voting rights, appointment and veto rights, trustee and beneficiary powers, contractual arrangements and other material influence. Do not treat a shareholder threshold as the sole beneficial-ownership test.	Control analysis, shareholder register, agreements and governance documents	Companies Act No. 10 of 2017, section 3; PACRA, What is control of a company?
Verify directors and signatories	Identify, verify and screen directors, senior managers, authorised signatories and other persons able to instruct the relationship; confirm their authority.	KYC files, director search, screening results and board resolution	FIC Act, section 18; FIC General Regulations 2022, reg. 7
Refresh KYB on material change	Monitor for changes in legal status, ownership, control, directors, licences and expected activity, and refresh KYB promptly after a material change, doubt or suspicion.	Registry-monitoring log, event alerts and updated KYB pack	FIC Act, sections 18 and 20; Companies Act No. 10 of 2017

6. PEPS, SANCTIONS AND TARGETED FINANCIAL SANCTIONS

PEPs, sanctions and targeted financial sanctions

Identify high-risk relationships and implement immediate controls for relevant sanctions and terrorism/proliferation financing designations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify PEP exposure	Screen customers, beneficial owners, controllers and authorised persons for domestic and foreign PEP exposure, and assess known family members and close associates using a risk-based approach.	Screening results, relationship map, PEP assessment and review log	FIC Act, section 19; FIC PEP Guidance Note
Apply enhanced PEP controls	For a high-risk or PEP relationship, obtain appropriate senior-management approval, establish source of wealth and source of funds, and apply enhanced ongoing monitoring.	Senior approval, source evidence, enhanced-monitoring plan and case reviews	FIC Act, section 19; FIC General Regulations 2022, reg. 10; FIC PEP Guidance Note
Screen sanctions and designation lists	Screen customers, beneficial owners, controllers, payers, payees and relevant counterparties against applicable UN, domestic and other legally applicable sanctions lists at onboarding, on list updates and before relevant transactions.	List inventory, screening timestamps, match-adjudication records and alert queue	Anti-Terrorism and Non-Proliferation Act No. 30 of 2024; FIC Act, section 23
Freeze, stop and report where required	Maintain an escalation process to validate matches, implement required freezing or transaction restrictions without delay, preserve evidence and report or seek directions from the competent authority as the applicable law requires.	Match case file, freeze or restriction record, authority correspondence and release controls	Anti-Terrorism and Non-Proliferation Act No. 30 of 2024; Anti-Terrorism S.I. No. 1 of 2024

7. PAYMENTS, WIRE TRANSFERS AND VIRTUAL ASSETS

Payments, wire transfers and virtual assets

Configure payment and virtual-asset controls to preserve required originator and beneficiary information and meet licensing obligations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Preserve transfer information	For applicable wire transfers and virtual-asset transfers, collect, verify where required and transmit the prescribed originator and beneficiary information; reject, suspend or investigate incomplete information in line with risk and law.	Payment-message specification, validation rules, rejection queue and sampled transfer records	FIC Prescribed Threshold Regulations 2022, reg. 6; FIC General Regulations 2022
Configure prescribed thresholds	Implement the Schedule to the Prescribed Threshold Regulations for customer identification, wire or virtual-asset transfer, currency transaction and border-reporting controls. Aggregate linked transactions where the law requires and maintain a documented FX-conversion method.	Threshold matrix, system configuration, aggregation logic and periodic control testing	FIC Prescribed Threshold Regulations 2022, regs. 5-8 and Schedule
Report currency transactions	Submit a currency transaction report for a cash or monetary transaction of USD 10,000 or more, including linked transactions where applicable, within three working days of the transaction using the prescribed FIC channel.	Threshold alert, linked-transaction analysis, CTR and submission receipt	FIC Prescribed Threshold Regulations 2022, reg. 7 and Schedule; FIC reporting guidance
Meet BoZ payment-system conditions	For a payment-system provider or participant, maintain the applicable BoZ approval or licence, KYC/client-verification procedures, AML training and agent oversight required for the service.	BoZ licence or approval, payment-system compliance assessment and agent-training records	National Payment Systems Act No. 1 of 2007; BoZ payment-system licensing requirements
Apply VASP controls where relevant	Treat virtual-asset activity as a regulated-risk area: confirm current BoZ and FIC requirements, complete licensing or registration steps, and implement the applicable CDD, travel-rule, monitoring and reporting controls before operating.	VASP legal assessment, regulator correspondence, transfer-control design and approval record	FIC General Regulations 2022; FIC VASP Sector Guidelines 2022; BoZ VASP public notices

8. TRANSACTION MONITORING AND SUSPICIOUS REPORTING

Transaction monitoring and suspicious reporting

Detect unusual activity, investigate promptly and report suspicion without tipping off.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor expected versus actual activity	Use risk-based manual or automated scenarios that consider unusual cash use, structuring, rapid movement of funds, changes in customer behaviour, high-risk geographies, fraud indicators and virtual-asset exposure.	Scenario inventory, tuning rationale, alert cases and quality-assurance results	FIC Act, sections 20 and 23; FIC General Guidelines 2017
File STRs within the statutory deadline	Where there are reasonable grounds to suspect proceeds of crime, terrorism, terrorist financing or proliferation financing, take reasonable measures to ascertain the transaction purpose and file an STR with FIC within three working days of forming the suspicion. Apply the same discipline to attempted transactions where required.	Suspicion timestamp, investigation record, compliance-officer decision, STR and FIC receipt	FIC Act, sections 29 and 45; FIC Guidance Note on STR Reporting 2022
Use the prescribed reporting channel and retain case evidence	Use the FIC online reporting portal or another prescribed submission route, include complete supporting information and retain reports, working papers and follow-up responses securely.	Portal role register, submission receipt, report copy and supporting case file	FIC reporting page; FIC Guidance Note on STR Reporting 2022
Prevent tipping off	Restrict access to internal alerts, STR decisions and FIC correspondence. Do not disclose to a customer or unauthorised person that an STR, inquiry or investigation exists.	Role-based access controls, confidentiality procedure and training records	FIC Act, section 34; FIC Guidance Note on STR Reporting 2022

9. RECORD KEEPING AND REGULATORY COOPERATION

Record keeping and regulatory cooperation

Retain complete, reconstructable records and respond promptly to lawful FIC and supervisory requests.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep AML records for at least 10 years	Retain CDD information, account files, business correspondence, transaction records and analysis results for at least 10 years following relationship termination or the occasional transaction, and retain transaction records for at least 10 years following completion.	Retention schedule, immutable archive settings, retrieval test and destruction approvals	FIC Act, section 22, as amended; Zambia Mutual Evaluation Report 2019
Maintain reconstructable transaction records	Keep records sufficient to reconstruct individual domestic and cross-border transactions, including parties, dates, amounts, currencies, instruments and relevant instructions.	Transaction schema, archive sample and reconstruction test	FIC Act, section 22; FIC Prescribed Threshold Regulations 2022
Respond to lawful information requests	Maintain a controlled process to receive, validate, search, approve and respond to FIC and other competent-authority requests within the required time, preserving a complete audit trail.	Request log, legal-review record, production package and response receipt	FIC Act; FIC General Regulations 2022, regs. 4-5
Preserve records subject to investigation	Suspend normal deletion for records subject to an STR, freeze, investigation, legal hold or authority request until release is authorised.	Legal-hold procedure, preservation notices and release approvals	FIC Act, sections 22 and 25; FIC General Regulations 2022

10. DATA PROTECTION AND PRIVACY

Data protection and privacy

Process KYC, KYB, screening and monitoring data lawfully, securely and only for defined purposes.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document lawful and transparent processing	Map personal-data processing for onboarding, screening, monitoring, reporting, retention and sharing; document the legal basis, purpose, data categories, recipients and retention period, and provide required privacy information.	Record of processing activities, privacy notices and legal-basis assessment	Data Protection Act No. 3 of 2021; Data Protection Commission guidance
Apply data minimisation and security controls	Collect only data needed for the compliance purpose and apply access control, encryption, logging, secure transmission, vendor controls and tested incident-response procedures.	Data inventory, access reviews, security architecture, vendor assessment and incident playbook	Data Protection Act No. 3 of 2021; Data Protection Regulations; Data Protection Code of Conduct 2025
Govern international transfers and processors	Assess cross-border transfers and outsourced processing before use, apply the required safeguards and written processor terms, and ensure third parties can support lawful data-subject and regulatory requests.	Transfer assessment, processor agreement, vendor due diligence and data-flow map	Data Protection Act No. 3 of 2021; Data Protection Regulations
Reconcile privacy with AML retention	Align deletion and data-subject request workflows with mandatory AML retention, legal holds, confidentiality and anti-tipping-off obligations; document any lawful restriction or deferred response.	Retention matrix, request-handling procedure and legal-review log	Data Protection Act No. 3 of 2021; FIC Act, sections 22 and 34

11. TESTING, ASSURANCE AND CONTINUOUS IMPROVEMENT

Testing, assurance and continuous improvement

Make compliance measurable through testing, management information and timely remediation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Test critical controls	Periodically test onboarding, identity verification, beneficial ownership, PEP and sanctions screening, thresholds, monitoring scenarios, report deadlines, record retrieval and access controls.	Control-test plan, sample results, defects and remediation tracker	FIC Guidelines on Independent Audit 2021; FIC Act, section 23
Report meaningful management information	Provide senior management and the board with risk ratings, overdue reviews, screening alerts, STR and CTR timeliness, threshold exceptions, training completion, audit findings and remediation status.	Compliance dashboard, committee minutes and action log	FIC Act, section 23; FIC Guidelines on AML/CFT Policy 2020
Track regulatory and list changes	Monitor FIC, BoZ, PACRA, Data Protection Commission and FATF publications; assess impact, update controls and retain evidence of implementation.	Regulatory-change register, impact assessments and updated procedures	FIC legislation and reporting pages; BoZ regulatory framework; FATF public statements
Remediate findings to closure	Assign each audit, inspection, incident or control failure to an accountable owner, set a risk-based deadline, validate remediation and report overdue issues to senior management.	Issue register, remediation evidence, validation results and management escalation	FIC Guidelines on Independent Audit 2021; FIC AML/CFT Framework

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.

01
Financial Intelligence Centre Zambia · Legislation library, including the FIC Act 2010, Amendment Acts 4 of 2016 and 16 of 2020, S.I. 53 and 54 of 2022, and anti-terrorism legislation
Open official source

02
Financial Intelligence Centre Zambia · Financial Intelligence Centre (Amendment) Act No. 16 of 2020
Open official source

03
Financial Intelligence Centre Zambia · Financial Intelligence Centre (General) Regulations, 2022, S.I. No. 54 of 2022
Open official source

04
Financial Intelligence Centre Zambia · Financial Intelligence Centre (Prescribed Threshold) Regulations, 2022, S.I. No. 53 of 2022
Open official source

05
Financial Intelligence Centre Zambia · AML/CFT framework
Open official source

06
Financial Intelligence Centre Zambia · Reporting guidance and sector-specific reporting materials
Open official source

07
Financial Intelligence Centre Zambia · AML/CFT General Guidelines 2017
Open official source

08
Financial Intelligence Centre Zambia · Guidance Note on Suspicious Transaction Reporting 2022
Open official source

09
Financial Intelligence Centre Zambia · VASP Sector Guidelines 2022
Open official source

10
Financial Intelligence Centre Zambia · Guidelines on AML/CFT Policy 2020
Open official source

11
Financial Intelligence Centre Zambia · Guidelines on AML/CTPF Independent Audit 2021
Open official source

12
Financial Intelligence Centre Zambia · Guidelines on ML/TF/PF Risk Assessment 2021
Open official source

13
Bank of Zambia · Regulatory framework and related financial-sector legislation
Open official source

14
Bank of Zambia · Payment-system licensing requirements
Open official source

15
Patents and Companies Registration Agency · Beneficial-owner definition under the Companies Act
Open official source

16
Patents and Companies Registration Agency · Control of a company under the Companies Act
Open official source

17
Patents and Companies Registration Agency · Annual-return compliance notice under the Companies Act
Open official source

18
Data Protection Commission Zambia · Data Protection Act No. 3 of 2021
Open official source

19
Data Protection Commission Zambia · Data protection regulations and 2025 code materials
Open official source

20
Financial Action Task Force · Jurisdictions under Increased Monitoring, 19 June 2026
Open official source

21
Financial Action Task Force · High-Risk Jurisdictions subject to a Call for Action, 19 June 2026
Open official source

22
Eastern and Southern Africa Anti-Money Laundering Group · Zambia Mutual Evaluation Report, June 2019
Open official source

Document control

Version 1.1 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

Operational guidance, not legal advice. Requirements vary by reporting-entity category, licence, product and supervisor. Confirm the current consolidated legislation, FIC directions, BoZ conditions, PACRA filings and data-protection instruments before implementation.