VOVE ID

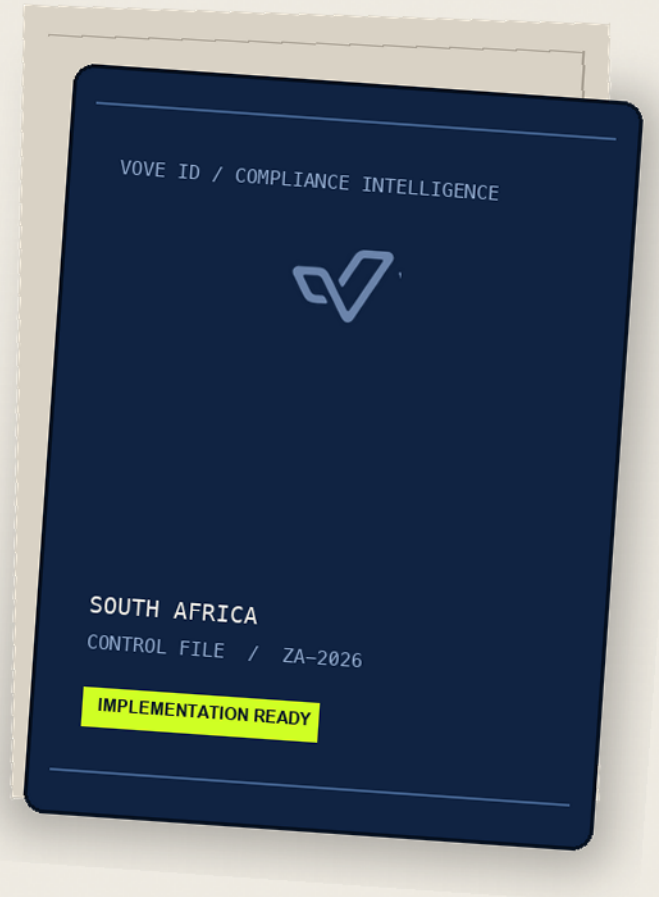
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

SOUTH AFRICA

SOUTH AFRICA / ZA



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

South Africa KYC, KYB and AML compliance checklist

A general FIC Act implementation baseline for Schedule 1 accountable institutions, with fintech and crypto-asset notes. It is not a complete sector checklist; banks, payment businesses, financial services providers, insurers, CASPs and other institutions must also apply their Prudential Authority, FSCA, SARB, FIC or other sector requirements.

Registration	**FIC goAML within 90 days of operations**
Core framework	**FIC Act and Schedule 1**
Record retention	**Generally 5 years**
Suspicion reporting	**Without delay; no later than 15 days**

Scope and legal framework

Financial Intelligence Centre Act, 2001, as amended; Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004; Money Laundering and Terrorist Financing Control Regulations; General Laws (Anti-Money Laundering and Combating Terrorism Financing) Amendment Act, 2022; and the Protection of Personal Information Act, 2013.

FATF context

South Africa was removed from FATF increased monitoring on 24 October 2025 after completing its action plan. FATF states that South Africa should continue working with FATF and ESAAMLG to sustain improvements; institutions should keep their country-risk methodology current.

IMPORTANT

This is a general South Africa baseline, not legal advice or a complete sector checklist. Being a fintech or technology provider does not by itself determine Schedule 1 status. Confirm the regulated activity, accountable-institution category, supervisor, product rules and current FIC directives 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. APPLICABILITY AND GOVERNANCE

Applicability and governance

Confirm accountable-institution status and make the risk-based compliance programme operational and accountable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map Schedule 1 status	Map each service and product against Schedule 1 of the FIC Act. Do not infer accountable-institution status from the fintech label alone; record the activity, item number, license and any exclusions.	Accountable-institution and licensing assessment	FIC Act, Schedule 1
Identify every supervisor	Map every activity to its Schedule 1 item and Schedule 2 supervisory body. The FSCA supervises items 4, 5 and 12. SARB acts through the Prudential Authority for items 6, 7, 7A, 8, 19 and 23; through Financial Surveillance for items 10, 13 and 19; and through its other statutory functions for item 23. The FIC directly supervises listed sectors including items 1, 2, 3, 9, 11, 14, 20, 21 and 22 and where no other supervisory body applies. A CASP conducting item 22 activity is accountable to the FIC; if it also provides crypto-asset advice or intermediary services, item 12 FSCA licensing and coordinated oversight may also apply.	Schedule-item, license and supervisor register	FIC Act, Schedules 1-2; FIC supervision mapping
Register under every applicable item	Register through goAML within 90 days after commencing business as an accountable institution under every applicable Schedule 1 item. Notify the FIC in writing of changes to registration particulars within 90 days.	FIC registrations and change log	FIC Act, s.43B; FIC registration notice
Keep accountability at the highest level	The board, senior management or other person or group exercising the highest authority must approve the RMCP. The board of a legal person, or senior management where there is no board, remains accountable for institutional and employee compliance. A legal person must maintain a compliance function and assign a person with sufficient competence and seniority to ensure its effectiveness; ultimate accountability is not an operational task that can be delegated away.	Approval, appointment, mandate and governance minutes	FIC Act, s.42A
Maintain an operational RMCP	Develop, document, maintain, implement and regularly review the RMCP. Address every section 42 component or document why it is not applicable, make the RMCP available to relevant employees and provide it to the FIC or supervisor on request. Cover institutional risk, CDD, BO, TFS, PEP, monitoring, reporting, records, training and governance.	Approved RMCP mapped to actual controls	FIC Act, s.42; Revised GN 7A
Apply the sector overlay	Add applicable PA, FSCA, SARB, exchange-control, payment, insurance, credit, CASP or professional-sector requirements and resolve differences in favor of the binding rule.	Sector-overlay matrix	Applicable sector law and supervisor guidance

2. KYC FOR NATURAL PERSONS

KYC for natural persons

Establish and verify identity using methods proportionate to risk and documented in the RMCP.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Prohibit anonymous or fictitious clients	Do not establish a business relationship or conclude a single transaction with an anonymous client or a client using an apparent false or fictitious name.	Onboarding rule and exception report	FIC Act, s.20A
Establish the client's identity	Collect sufficient identity particulars for the customer type and risk, including full legal name, date of birth, identification number or passport details, nationality, address and contact information as defined by the RMCP and applicable sector rule.	Completed customer profile	FIC Act, s.21; RMCP
Verify identity reliably	Verify identity using reliable independent sources and methods defined in the RMCP, documenting authenticity checks, exceptions and the basis for any non-face-to-face approach.	Verification result and audit trail	FIC Act, s.21; GN 7A
Verify representatives and underlying clients	Where a person acts for another, establish and verify the representative and the person on whose behalf they act, and confirm authority.	Authority evidence and relevant KYC files	FIC Act, ss.21 and 21B
Understand purpose and source of funds	Record the nature and intended purpose of the relationship, expected activity and source of funds expected to be used.	Purpose and expected-activity profile	FIC Act, s.21A
Resolve failed CDD	If required CDD cannot be completed, do not establish the relationship, conclude or give effect to the transaction, or continue the relationship; terminate according to the RMCP and consider a section 29 report.	Decline or exit and reporting decision	FIC Act, s.21E

3. KYB FOR LEGAL PERSONS AND ARRANGEMENTS

KYB for legal persons and arrangements

Verify the entity and authority, then identify the natural persons who ultimately own or control it.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence and status	Obtain and independently verify the registered name, registration number, legal form, status, governing documents and registered address through CIPC or another reliable registry.	Current registry result and formation documents	FIC Act, ss.21 and 21B; RMCP
Understand activity and financial profile	Record the business activity, operating address, expected products, transaction volumes, counterparties, geographies and source of funds.	Business and expected-activity profile	FIC Act, s.21A
Verify authority and required connected persons	Establish and verify every person acting for a client or on whose behalf a client acts, and confirm authority. Identify and take reasonable steps to verify all natural-person beneficial owners under section 21B. Obtain director and controller information needed to understand the structure, but verify additional directors or controllers only where they are representatives, beneficial owners, required by the RMCP because of risk, or covered by a sector rule.	Mandate, structure analysis and required KYC	FIC Act, ss.21 and 21B
Apply the beneficial-owner cascade	Identify natural persons exercising controlling ownership, then control through other means, and only where no such person can be identified after reasonable measures, the person exercising control over management.	Ownership and control chart with BO rationale	FIC Act, s.21B; PCC 59
Use 5% as a control indicator, not a safe harbor	PCC 59 strongly recommends identifying persons with 5% or more ownership interest, but the AML test remains control-based. Do not stop where lower ownership, agreements, voting rights or other means create control.	Threshold and other-control analysis	PCC 59, paras. 2.18-2.19
Check CIPC BO information	Compare customer declarations with available CIPC BO and securities information. Newly incorporated entities must file BO information within 10 business days after incorporation and amended information within 10 business days after a change. CIPC applies a 5% minimum threshold with broader effective-control indicators; declarations and the applicable securities or beneficial-interest register are also filed annually with the annual return within 30 business days after the incorporation anniversary. Do not treat CIPC information or 5% ownership as conclusive for AML CDD.	CIPC result, discrepancy record and filing evidence	CIPC BO guidance; PCC 59
Resolve trusts and layered structures	Trace ownership and control through intermediate companies, partnerships, trusts or nominees and obtain reliable evidence for trustees, founders, beneficiaries, protectors and other controlling persons as applicable.	Full structure chart and arrangement documents	FIC Act, s.21B; PCC 59

4. RISK ASSESSMENT, PEPS AND SANCTIONS

Risk assessment, PEPs and sanctions

Apply the RMCP's risk methodology while treating targeted financial sanctions as a non-risk-based prohibition.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Assign and explain customer risk	Assess customer, ownership, product, service, delivery channel, geography and transaction risk under the RMCP and retain the rationale and approval.	Risk assessment and decision	FIC Act, s.42; GN 7A
Identify prominent persons	Determine whether customers or beneficial owners are foreign or domestic politically exposed persons or prominent influential persons, including relevant immediate family and known close associates.	PEP/PIP result and relationship mapping	FIC Act, ss.21F-21G and Schedules 3A-3C
Apply risk-specific prominent-person controls	For foreign PEPs, obtain senior approval, establish source of wealth and funds and enhance monitoring. Apply those measures to domestic PEPs and prominent influential persons where the relationship is higher risk.	Approval, source analysis and monitoring plan	FIC Act, ss.21F-21G; PCC 51
Screen UN and domestic designations	Scrutinise prospective and existing clients, beneficial owners, representatives, persons on whose behalf clients act and transaction parties against the current FIC-hosted UN Security Council TFS list and applicable section 23 POCDATARA court orders. Screening is mandatory regardless of customer risk and must occur at onboarding, during the relationship and whenever designations or orders change.	Time-stamped list and order screening with match decision	FIC Act, ss.26A and 28A; POCDATARA, s.23; PCC 44A
Freeze and prohibit immediately	On a true match, immediately and without waiting for consent, another court order or prior reporting, cease all activity and freeze property in the institution's possession or control. Do not deal with, release or make property, funds, financial services or other services available to the designated person, persons acting for them or related controlled property. Lift the freeze only after delisting, a domestic order is set aside or a valid section 26C permission applies.	Freeze, block, non-dealing and authorization record	FIC Act, ss.26B-26C; POCDATARA; PCC 44A
File the correct TFS report	File a TPR without delay and no later than five days after awareness that the institution possesses or controls section 28A property, including attempted transactions. File a section 29 report where activity is suspicious but designation or property connection is not established as fact.	TPR or STR decision, filing and timeline	FIC Act, ss.28A-29; PCC 44A
Screen employees	Screen prospective and current employees for competence and integrity periodically using a documented risk-based approach. Scrutinise employee information against applicable TFS information when section 26A notices are issued. Retain the methodology and outcomes and make them available to the FIC or supervisor on request.	Employee-screening policy, results and review log	FIC Directive 8; PCC 55
Use adverse information proportionately	Review reliable adverse information where relevant, distinguish allegation from verified fact and record its effect on risk and approval.	Adverse-information disposition	RMCP risk-based control

5. ENHANCED DUE DILIGENCE

Enhanced due diligence

Increase information, verification, approval and monitoring where the documented risk is higher.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Collect additional customer and BO information	Obtain further identity, ownership, business, geography and transaction information needed to understand and mitigate the higher risk.	EDD information pack	FIC Act risk-based framework; RMCP
Corroborate material claims	Use additional reliable sources to verify identity, legal existence, ownership, control, expected activity and explanations for unusual features.	Independent corroboration record	GN 7A; PCC 59
Establish source of funds and wealth	Establish and, where risk warrants, corroborate source of funds and source of wealth, including mandatory prominent-person measures.	Source evidence and plausibility analysis	FIC Act, ss.21A and 21F-21G
Obtain senior approval where required	Require documented approval for foreign PEP and applicable higher-risk domestic PEP or prominent-influential-person relationships and for other cases specified by the RMCP or sector rule.	Approval and conditions	FIC Act, ss.21F-21G; RMCP
Increase ongoing monitoring	Set tighter review cycles, transaction scrutiny, alert thresholds and escalation requirements proportionate to higher risk.	EDD monitoring plan	FIC Act, s.21C; RMCP

6. ONGOING DUE DILIGENCE AND FINTECH CONTROLS

Ongoing due diligence and fintech controls

Keep customer knowledge current, connect monitoring to the expected profile and apply technology-specific directives.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor throughout the relationship	Conduct ongoing due diligence and scrutinise transactions for consistency with the institution's knowledge of the customer, business, risk profile, source of funds and expected activity.	Monitoring rules, alerts and case outcomes	FIC Act, s.21C
Refresh on risk and trigger events	Keep CDD and BO information current at a risk-based frequency and when ownership, authority, activity, product, geography, behavior or prior information changes.	Review schedule and event-driven reviews	FIC Act, ss.21C-21D; RMCP
Examine unusual activity	Investigate activity lacking an apparent lawful purpose, inconsistent with the expected profile or otherwise unusual, and preserve the rationale for reporting or closing the case.	Investigation notes and decision	FIC Act, s.29; GN 4B
Meet Directive 5 ATMS clocks	Where a reporter uses an automated transaction monitoring system, treat alert generation as knowledge of potentially reportable activity and begin investigating within 48 hours, excluding Saturdays, Sundays and public holidays. Submit a section 29 report as soon as possible and no later than 15 days after alert generation. Prevent backlogs, document decisions and preserve manual reporting and monitoring for system gaps.	Alert timeline, investigation and filing record	FIC Directive 5; PCC 45
Govern ATMS effectiveness	Assign skilled staff and responsibilities; test detection effectiveness, data integrity, scenarios, thresholds and rules; perform risk-based tuning; document and test configuration changes; obtain prior highest-authority approval for significant changes; and obtain highest-authority review and approval of ATMS effectiveness at least annually. Include the methodology and workflow in the RMCP.	Tests, changes, annual approval and RMCP mapping	FIC Directive 5; PCC 45
Apply Directive 9 to in-scope CASPs	Directive 9 applies to item 12 and item 22 accountable institutions acting as ordering, intermediary or recipient CASPs for domestic or cross-border crypto-asset transfers and has applied since 30 April 2025. In a business relationship, any value above zero qualifies. Ordering CASPs must transmit required originator and beneficiary information securely before or simultaneously with the transfer; use the reduced treatment only for qualifying single transactions below R5,000 and verify the originator where suspicion exists.	Travel-rule messages, threshold logic and exceptions	FIC Directive 9
Control counterpart CASPs and incomplete data	Conduct due diligence on counterpart CASPs, preserve required information through intermediary and recipient stages, and maintain risk-based procedures for incomplete information and unhosted wallets in the RMCP. An ordering CASP must not execute a transfer when it cannot comply with Directive 9 paragraphs 4.1 to 4.7.	Counterparty due diligence and transfer decisions	FIC Directive 9

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Submit the 2026 risk and compliance return	Check Directive 11 scope. The 30 June 2026 deadline for item 2 trust and company service providers, item 9 casinos, item 11 non-bank credit providers, item 14 Postbank, item 21 South African Mint and item 22 CASPs is now overdue; remediate immediately if outstanding. Item 1 legal practitioners, item 3 estate agents, item 20 high-value goods dealers and item 9 non-casino gambling institutions must submit by 31 July 2026 through the prescribed platform under PCC 60 and current FIC instructions.	Scope assessment, submission and remediation record	FIC Directive 11; 2026 RCR notice; PCC 60
Maintain continuity across KYC and monitoring	Ensure monitoring and case decisions can retrieve the onboarding purpose, expected activity, BO structure, risk rating and prior reviews instead of treating KYC as a static file.	Linked customer, monitoring and case audit trail	Recommended implementation control; FIC lifecycle obligations

7. REPORTING, RECORDS, PRIVACY AND ASSURANCE

Reporting, records, privacy and assurance

File each report within its own trigger and deadline, prevent tipping off and preserve retrievable evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
File STRs and SARs	Section 29 applies broadly to persons carrying on, managing or employed by a business. Report suspicious or unusual transactions or activities through goAML as soon as possible and without delay, but no later than 15 days excluding Saturdays, Sundays and public holidays after awareness of the reportable fact; internal review time is included. A report does not itself stop a transaction, although a section 34 FIC intervention may prohibit continuation for up to five days.	STR/SAR reference and decision timeline	FIC Act, ss.29 and 34; GN 4B; FIC reporting FAQ
Prevent tipping off	Do not disclose that a section 29 report has been or will be filed or reveal its contents, and limit access to reports and investigations.	Access controls and communications guidance	FIC Act, ss.29 and 38
File cash threshold reports	Report physical cash received or paid of R50,000 or more as soon as possible and no later than three business days after awareness. Do not treat electronic transfers as cash and do not assume CTR filing replaces an STR or TPR.	CTR logic, filings and reconciliation	FIC Act, s.28; GN 5C
File IFTRs where the institution is in scope	Authorised dealers, authorised dealers with limited authority, financial services providers with a direct-reporting dispensation and Postbank must report each qualifying inbound or outbound cross-border electronic transfer of R20,000 or more. Submit as soon as possible and no later than three days excluding Saturdays, Sundays and public holidays after awareness that the transfer occurred, ordinarily when value becomes available to the beneficiary. Apply per transfer without aggregation and include qualifying Common Monetary Area transfers.	IFTR scope assessment, filings and reconciliation	FIC Act, s.31; GN 9
Escalate missed reports	If the institution discovers that a required CTR, TPR, STR/SAR or IFTR was not submitted, immediately notify the FIC in writing through the prescribed channel, request engagement on mitigation and continue remediating the missed report. Notification does not condone the failure, extend the original deadline or prevent enforcement.	FIC notification, late filing and remediation record	FIC Directive 3A
Retain retrievable records	Keep CDD records for five years after relationship termination, transaction records for five years after the transaction and section 29 reporting records for five years after submission; ensure free and easy access, legibility and prompt production.	Retention schedule and retrieval test	FIC Act, ss.22-24; FIC reference guide
Apply POPIA controls	Register the Information Officer, document the eight lawful-processing conditions, minimization, transparency, security safeguards, operator governance, rights, cross-border transfers, retention, impact assessments, prior authorization where required and security-compromise response. Preserve FIC Act records where legally required.	Information Officer record, processing register and privacy controls	POPIA; Information Regulator guidance

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Train, test and remediate	Provide ongoing employee training sufficient to enable compliance with the FIC Act and RMCP. Test control effectiveness at documented intervals and remediate weaknesses. Independent assurance is a recommended implementation control unless a binding sector rule, licence condition or governance standard makes it mandatory.	Training, testing record and remediation log	FIC Act, s.43; RMCP

SOURCES AND FURTHER READING

Verify against current official material

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

Financial Intelligence Centre Act booklet, current consolidated material
Financial Intelligence Centre · primary
Open official source

Compliance obligations and supervisory scope
Financial Intelligence Centre · primary
Open official source

Reference guide for accountable institutions
Financial Intelligence Centre · primary
Open official source

Revised Guidance Note 7A on risk management and compliance programmes
Financial Intelligence Centre · primary
Open official source

PCC 59 on beneficial ownership
Financial Intelligence Centre · primary
Open official source

Targeted financial sanctions obligations and list
Financial Intelligence Centre · primary
Open official source

PCC 44A on targeted financial sanctions and domestic designations
Financial Intelligence Centre · primary
Open official source

Schedule 2 supervision and enforcement mapping
Financial Intelligence Centre · primary
Open official source

Crypto asset service provider sector obligations
Financial Intelligence Centre · primary
Open official source

Suspicious transaction reporting period
Financial Intelligence Centre · primary
Open official source

Cash threshold reporting obligations
Financial Intelligence Centre · primary
Open official source

Guidance Note 9 on international funds transfer reporting
Financial Intelligence Centre · primary
Open official source

Directive 9 travel rule for crypto asset transfers
Financial Intelligence Centre · primary
Open official source

Directive 5 on automated transaction monitoring systems
Financial Intelligence Centre · primary
Open official source

PCC 45 on implementation of Directive 5
Financial Intelligence Centre · primary
Open official source

Directive 8 and PCC 55 on employee screening
Financial Intelligence Centre · primary
Open official source

Directive 3A on failures to submit regulatory reports
Financial Intelligence Centre · primary
Open official source

2026 risk and compliance return deadlines
Financial Intelligence Centre · primary
Open official source

Beneficial ownership filing guidance
Companies and Intellectual Property Commission · primary
Open official source

POPIA compliance and Information Officer guidance
Information Regulator South Africa · primary
Open official source

FATF increased monitoring statement, 24 October 2025
Financial Action Task Force · primary
Open official source

South Africa AML Operations in 2026: Why KYC Alone Fails Under FICA
VOVE ID - contextual reading · context
Open official source

Document control

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

This is a general South Africa baseline, not legal advice or a complete sector checklist. Being a fintech or technology provider does not by itself determine Schedule 1 status. Confirm the regulated activity, accountable-institution category, supervisor, product rules and current FIC directives before implementation.