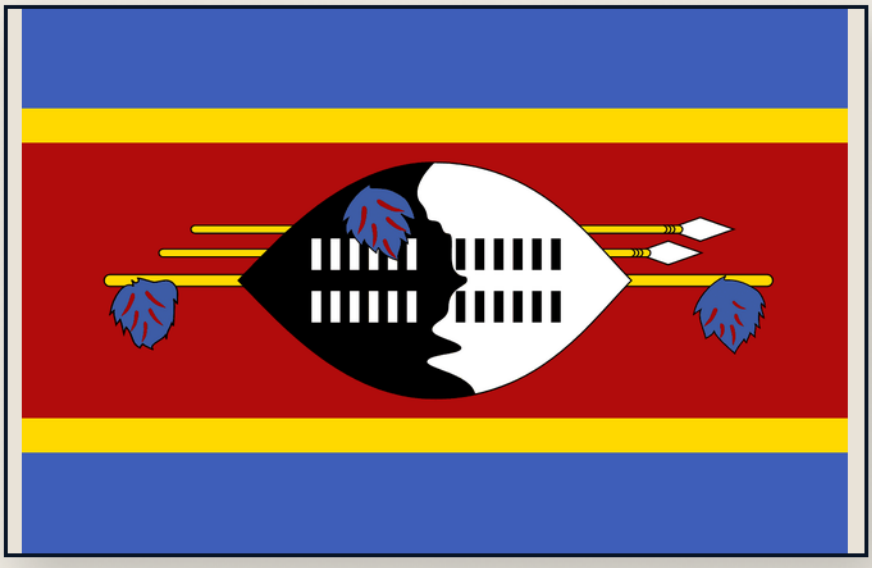
VOVE ID

VOVE COUNTRY CONTROL FILE

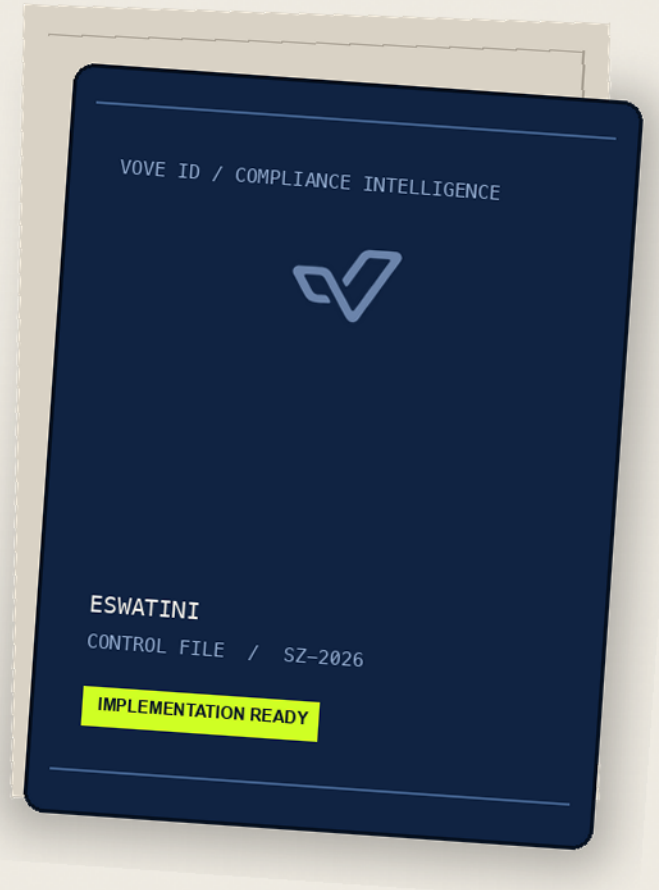
KYC / KYB / AML

2026 EDITION

ESWATINI



ESWATINI / SZ



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Eswatini KYC, KYB & AML Compliance Checklist

An implementation checklist for Eswatini customer and beneficial-owner diligence, reporting, sanctions, records, financial licensing, payments and data protection.

FIU	**Eswatini Financial Intelligence Centre (EFIC)**
Primary AML law	**Act No. 6 of 2011, amended in 2016 and 2024**
STR timing	**Promptly - defined by the 2024 amendment as as soon as possible, no later than 5 days**
Cash reporting	**E25,000 or more, including qualifying same-day aggregation; within 2 working days**
Core retention	**At least 5 years from the statutory trigger; longer on authority request**
FATF status	**Not named on FATF public lists as at 19 June 2026**

Scope and legal framework

The Money Laundering and Financing of Terrorism (Prevention) Act No. 6 of 2011, amended in 2016 and by the Anti-Money Laundering, Counter Financing of Terrorism and Proliferation Financing (Miscellaneous Amendments) Act 2024, is the core preventive law. The Eswatini Financial Intelligence Centre (EFIC) is the FIU. The Central Bank of Eswatini (CBE), Financial Services Regulatory Authority (FSRA) and other sector authorities supervise their respective accountable institutions. The Data Protection Act 2022 governs personal information.

FATF context

Eswatini is assessed through ESAAMLG. It was not named on FATF's high-risk or increased-monitoring lists current at 19 June 2026. This is not a low-risk finding: the August 2025 enhanced follow-up report addressed technical compliance and did not reassess the low effectiveness ratings from the 2022 mutual evaluation.

IMPORTANT

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 25 August 2026. Confirm current EFIC portal access and directives, gazetted thresholds, supervisor rules, company and beneficial-ownership filing mechanics, sanctions updates, product permissions and data-protection procedures with the competent authority and qualified Eswatini counsel before launch.

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.

1. SCOPE, AUTHORITIES, AND LICENSING

Scope, authorities, and licensing

Resolve the accountable-institution category, supervisor and product permission before launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each entity and activity is an accountable institution.	Map each product, entity and channel to Schedule 3 and document the competent AML supervisor; distinguish CBE-regulated banking, remittance and payment activity from FSRA and other sectors.	Perimeter memo, Schedule 3 mapping and supervisor confirmation.	MLTFP Act 2011, sections 2 and 3 and Schedule 3, as amended in 2016 and 2024
Register and maintain reporting access with EFIC.	Complete the current accountable-institution registration process, nominate authorised contacts and test access to the applicable EFIC reporting workspace before accepting customers.	Registration confirmation, authorised-user list and access test.	MLTFP Act, sections 19 and 31; EFIC compulsory-registration directive and reporting portal
Obtain activity-specific financial permission.	Confirm CBE, FSRA or other sector approval for banking, remittance, payment, mobile-money, insurance, securities, credit and virtual-asset activity; sandbox participation is not a production licence.	Licence analysis, application, approval and conditions register.	Financial Institutions Act 2005; National Payment Systems Act 2023; MLTFP Act section 18bis as amended in 2024; applicable FSRA laws

2. GOVERNANCE AND RISK ASSESSMENT

Governance and risk assessment

Controls must be risk-based, resourced and demonstrable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify, understand and mitigate ML, TF and PF risk.	Maintain an approved assessment covering customers, products, geography, transactions, delivery channels, new technology and national risk findings; refresh it on material change.	Methodology, assessment, approvals and change log.	MLTFP Act sections 6, 6ter and 6quat, as amended in 2024
Maintain accountable compliance governance.	Appoint an AML reporting officer, resource the control function, train relevant staff, independently test the programme and track remediation.	Appointment, policies, training records, audit plan and remediation log.	MLTFP Act section 18; CBE Financial Integrity supervision materials
Control group, branch and third-party reliance.	Apply group-wide AML/CFT programmes, protect shared information, address stricter Eswatini requirements in foreign operations and retain ultimate responsibility for relied-on CDD and records.	Group policy, transfer controls, third-party diligence and retrieval tests.	MLTFP Act sections 6(6), 6septies, 8(7)-(8) and 18(2bis)-(2ter), as amended

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Identify and verify before or during every statutory trigger.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify customers, beneficial owners and representatives.	Use reliable independent sources to verify the customer, every beneficial owner and anyone acting for the customer; authenticate authority before access or execution.	Identity record, verification provenance, mandate and result.	MLTFP Act section 6bis(1)-(2), as amended in 2024
Apply CDD to relationships, transactions, electronic transfers, suspicion and doubts.	Configure triggers for entering or continuing a relationship, any transaction without a relationship, electronic funds transfers, suspicion, and doubts about earlier identification; do not reuse the former E2,500 occasional-transaction exemption removed in 2024.	Trigger logic, completed CDD file and exception log.	MLTFP Act section 6bis(1) and 2024 amendment sections 3 and 7
Do not proceed when CDD cannot be completed.	Do not open or maintain the account, start the relationship or perform the transaction; terminate where required and file an STR, unless continuing CDD would tip off the customer, in which case stop that process and report promptly.	Failure decision, termination record, STR and restricted-access chronology.	MLTFP Act sections 6bis(2bis) and 13bis, inserted in 2024

KYB, registries, and beneficial ownership

Legal existence and natural-person control require separate proof.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Understand and verify each legal person or arrangement.	Obtain name, legal form, nature of business, proof of existence, registered and principal addresses, directors, binding powers, owners, beneficiaries and control structure; verify representatives.	Registry evidence, constitution, licences, powers and reconciliation.	MLTFP Act section 6bis(2)(c), as amended in 2024
Trace beneficial ownership through ownership and other control.	Identify and verify natural persons who ultimately own or control directly or indirectly, including through a chain or other means; if none is identified, verify senior management and record the basis.	Ownership and control chart, source records, identities and fallback rationale.	MLTFP Act sections 2 and 6bis(1), as amended in 2024
Apply the legal-arrangement tests.	For trusts and similar arrangements identify and verify settlors, trustees, protectors, beneficiaries or classes and every other natural person exercising ultimate effective control.	Trust instrument, party identities, control analysis and reliable-source checks.	MLTFP Act definition of beneficial owner and sections 6bis(2quin) and 6sext, inserted in 2024

5. PEPS, EDD, AND REMOTE ONBOARDING

PEPs, EDD, and remote onboarding

Higher-risk and non-face-to-face cases need enhanced, documented controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Detect domestic, foreign and international-organisation PEP exposure.	Screen customers, beneficial owners and connected persons at onboarding and throughout the relationship, including existing customers who become PEPs.	Screening, relationship map, match decision and refresh log.	MLTFP Act section 2 PEP definition and section 6bis(2)(c)-(d), as amended in 2024
Apply approval, wealth, funds and enhanced monitoring controls.	Obtain senior-management approval, establish source of wealth and source of funds and conduct enhanced ongoing monitoring for PEPs and other higher-risk areas.	Approval, provenance analysis and monitoring plan.	MLTFP Act sections 6bis(2)(d), 6bis(2ter)-(2quat) and 6ter
Assess remote onboarding and new technology before use.	Document identity, impersonation, device, fraud, cybersecurity, privacy and ML/TF/PF risks before launch; use proportionate liveness and exception controls and confirm supervisor expectations.	Pre-launch assessment, tests, approval and exceptions.	MLTFP Act section 6(1), as amended in 2024; Data Protection Act 2022 sections 14-17

6. MONITORING AND SUSPICIOUS REPORTING

Monitoring and suspicious reporting

Reporting must be prompt, confidential and reconstructable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing due diligence and transaction monitoring.	Test activity against customer knowledge, commercial activity, risk profile and source of funds; investigate inconsistencies and refresh CDD.	Alerts, investigation, disposition and profile refresh.	MLTFP Act section 11, substituted in 2024
Report suspicious transactions, attempts and relevant information promptly.	File with EFIC as soon as possible and no later than five days after suspicion forms; include grounds and attempted activity. Use the current authorised workspace and do not use email where the 2025 SharePoint directive applies.	Decision log, STR, submission proof and receipt.	MLTFP Act sections 2 and 12, as amended in 2024; EFIC STR Directive 01/2025
Prevent tipping off and protect reporting information.	Restrict report and inquiry access, avoid customer disclosure, and stop CDD that would tip off while filing the required STR.	Access controls, logs, escalation procedure and training.	MLTFP Act sections 13bis, 15, 16 and 30

Payments, wires, thresholds, and agents

Keep cash reporting distinct from CDD and wire-transfer rules.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report qualifying cash of E25,000 or more.	File a CTR within two working days for physical cash received or paid at or above E25,000, including qualifying same-direction aggregation within one calendar day; monitor structuring separately for suspicion.	Aggregation logic, CTR, transmission proof and review samples.	MLTFP Act section 12bis; EFIC Cash Threshold Reporting Guideline, effective 1 October 2024
Carry complete originator and beneficiary information on wires.	Collect, verify, transmit and retain required payer and payee information; use risk-based rules to execute, reject or suspend deficient transfers and follow up missing data.	Payment messages, validation rules, exception decisions and records.	MLTFP Act sections 7 and 10, substituted in 2024
Apply licence, agent and transfer controls to payments and virtual assets.	Obtain CBE or other competent approval, diligence agents and outsourcers, preserve record access, and apply the 2024 originator, beneficiary, screening and freezing rules to virtual-asset transfers; confirm the operative VASP licensing framework before launch.	Permission, contracts, monitoring, travel-rule records and authority confirmation.	National Payment Systems Act 2023; MLTFP Act sections 7(18)-(19), 18bis(d) and 18ter, inserted in 2024

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Use current lists and act within the domestic 24-hour definition of without delay.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen UN and EFIC sanctions updates continuously.	Screen customers, beneficial owners, controllers, representatives and transactions against the current UN consolidated list and EFIC updates, with event-driven rescreening.	List inventory, update timestamps, configuration and dispositions.	Anti-Money Laundering (UNSCR) Regulations 2016; EFIC TFS directives; UN consolidated list
Freeze and prohibit designated dealings without delay.	For a confirmed designation, apply the domestic freeze and transaction prohibition within 24 hours, preserve timestamps and do not wait for ordinary transaction processing.	Match analysis, freeze record, timestamps and blocked-transaction log.	MLTFP Act section 2 definition of without delay and section 7(17)-(18), as amended in 2024; UNSCR Regulations 2016
Report and govern false positives, exemptions and release.	Follow the current EFIC and UNSCR Implementation Committee route, document the legal basis for each hold or release, and act only on competent authority.	Report, authority correspondence, exemption or release decision and reconciliation.	UNSCR Regulations 2016, including regulations 4, 20-21, 29 and 31-32; current EFIC TFS directive

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Records must reconstruct customers, ownership, transactions and decisions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain the full statutory record set for at least five years.	Keep CDD, account files, business correspondence, transactions, analysis, reports and FIU enquiries for at least five years from the applicable identity, transaction, account-closure or relationship-cessation trigger.	Schedule, archive sample, trigger mapping and deletion control.	MLTFP Act section 8(1)-(2), including paragraph (e) inserted in 2024
Extend records when a competent authority requires it.	Suspend disposal for specified records on an EFIC, law-enforcement or supervisor request and retain ultimate responsibility where storage is outsourced.	Hold notice, custodian instructions and retrieval test.	MLTFP Act section 8(6)-(8)
Produce records immediately and securely.	Authenticate requests, protect STR confidentiality, export reproducibly and log scope, timing and acknowledgement.	Request, approval, production index and receipt.	MLTFP Act section 8(3)-(5)

Privacy, biometrics, and transfers

Reconcile AML duties with the Data Protection Act 2022.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Use a lawful basis, notice, minimisation and retention controls.	Document the legal basis and purpose for each identity-data use, provide required collection information, collect only adequate and relevant data and delete or de-identify when no longer authorised, subject to AML holds.	Data inventory, legal-basis map, notice and retention schedule.	Data Protection Act 2022 sections 9-13
Secure sensitive and biometric information and processors.	Identify foreseeable risk, apply and test reasonable safeguards, restrict sensitive-data processing and bind processors by written confidentiality and security obligations.	Risk assessment, security tests, access matrix and processor contract.	Data Protection Act 2022 sections 14-16 and 22-31
Notify compromises and control cross-border transfers.	Notify the Commission and affected data subjects as soon as reasonably possible when unauthorised access or acquisition is reasonably believed; assess SADC necessity or non-SADC adequacy and document any statutory derogation or Commission authorisation.	Incident chronology, notices, transfer assessment and safeguards.	Data Protection Act 2022 sections 17 and 32-33

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Maintain compact evidence that reproduces regulated decisions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, KYB, beneficial ownership, screening, risk, approvals, privacy notices and exceptions under stable identifiers.	Complete sampled onboarding pack.	Operational control supporting MLTFP Act sections 6-8 and Data Protection Act sections 9-16
Maintain a reconstructable monitoring and reporting pack.	Link transactions, alerts, analysis, approvals, CTRs, STRs, sanctions actions and post-filing controls while protecting confidentiality.	Complete sampled case pack and access log.	Operational control supporting MLTFP Act sections 8 and 11-16

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 Financing of Terrorism (Prevention) Act No. 6 of 2011 - consolidated issue
Government of Eswatini · Primary legislation
Open official source

Money Laundering and Financing of Terrorism (Prevention) (Amendment) Act No. 5 of 2016
Government of Eswatini Gazette · Primary legislation
Open official source

Anti-Money Laundering, Counter Financing of Terrorism and Proliferation Financing (Miscellaneous Amendments) Act 2024
Government of Eswatini / EFIC · Primary legislation
Open official source

Anti-Money Laundering (United Nations Security Council Resolutions) Regulations 2016
Government of Eswatini Gazette · Primary regulations
Open official source

Cash Threshold Reporting Guideline - September 2024
Eswatini Financial Intelligence Centre · Official regulatory guidance
Open official source

STR Directive 01/2025 - mandatory SharePoint filing
Eswatini Financial Intelligence Centre · Official regulatory directive
Open official source

EFIC compliance guidance and current directives
Eswatini Financial Intelligence Centre · Official regulator portal
Open official source

Eswatini fourth enhanced follow-up report - August 2025
FATF / ESAAMLG · Authoritative country assessment
Open official source

Eswatini mutual evaluation report - June 2022
ESAAMLG / EFIC · Authoritative country assessment
Open official source

Data Protection Act 2022
Government of Eswatini Gazette · Primary legislation
Open official source

Financial Regulation and Financial Integrity Division
Central Bank of Eswatini · Official regulator guidance
Open official source

National Payment Systems and licensed payment service providers
Central Bank of Eswatini · Official regulator guidance
Open official source

FATF high-risk and monitored jurisdictions
FATF · Authoritative current status
Open official source

United Nations Security Council consolidated sanctions list
United Nations · Authoritative sanctions list
Open official source

Document control

Version 1.0 / Published 25 August 2026 / Last reviewed 25 August 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 25 August 2026. Confirm current EFIC portal access and directives, gazetted thresholds, supervisor rules, company and beneficial-ownership filing mechanics, sanctions updates, product permissions and data-protection procedures with the competent authority and qualified Eswatini counsel before launch.