VOVE ID

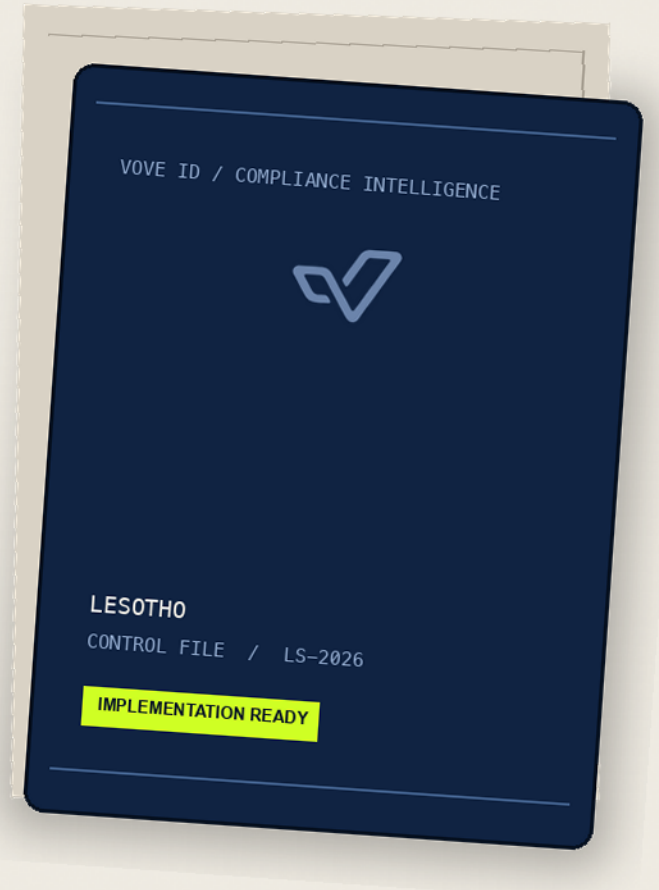
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

LESOTHO

LESOTHO / LS



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Lesotho KYC, KYB & AML Compliance Checklist

An implementation checklist for Lesotho's AML/CFT framework, FIU reporting, customer and beneficial-owner diligence, sanctions, company transparency, records, privacy and regulated financial services.

FIU	**Financial Intelligence Unit of Lesotho**
Primary AML rules	**MLPCA 2008 as amended; MLPCR 2019**
Suspicion reporting	**Immediately to the FIU; in any case no later than 7 days**
Thresholds	**Sector and transaction specific; do not use one universal amount**
Core AML retention	**At least 5 years after relationship end or occasional transaction**
FATF status	**Not named on FATF public lists as at 19 June 2026**

Scope and legal framework

The Money Laundering and Proceeds of Crime Act 2008, as amended in 2016, and the Money Laundering and Proceeds of Crime Regulations 2019 form the core AML/CFT framework. Apply them with the Companies Act 2011 and Companies (Beneficial Ownership) Regulations 2024, Data Protection Act 2012, Financial Institutions Act 2012, Payment Systems Act 2014 and current sector instruments.

FATF context

Lesotho is assessed through ESAAMLG and remains in enhanced follow-up after its September 2023 mutual evaluation. It was not named on FATF's high-risk or increased-monitoring lists current at 19 June 2026. Absence from those lists is not a low-risk finding.

IMPORTANT

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 29 August 2026. Confirm current FIU registration and filing specifications, prescribed transaction-reporting thresholds, sanctions communications, Data Protection Commission procedures, and product-specific permissions with the competent authority and qualified Lesotho 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 entity, activity and supervisor before launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is accountable.	Map every entity, product, channel and agent to the Act, the 2019 Regulations and applicable financial-institution, DNFBP or designated-business categories; identify the FIU and sector supervisor.	Applicability memo, product map and accountable-owner register.	MLPCA 2008, section 2 and Schedule 1; MLPCR 2019, regulations 1 and 22
Register with the FIU when the prescribed obligation applies.	Obtain the current FIU form and submission route; register within the applicable period and notify changes within 60 days without assuming an unverified portal.	Registration, receipt, change log and channel test.	MLPCR 2019, regulation 21
Obtain authorisation before regulated activity.	Classify banking, payments, e-money, money transfer, exchange, microfinance, insurance, securities, agent and virtual-asset activities and obtain every required approval before launch.	Perimeter analysis, authority correspondence and licence register.	Financial Institutions Act 2012; Payment Systems Act 2014; applicable CBL and sector instruments

2. GOVERNANCE AND RISK ASSESSMENT

Governance and risk assessment

Controls must be risk-based, documented and independently tested.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented ML/TF risk assessment.	Assess customers, products, channels, geography, cash, agents, technology and proliferation exposure; apply enhanced measures where risk is higher and never simplify when suspicion exists.	Approved methodology, assessment, controls and version history.	MLPCR 2019, regulations 5 and 10
Maintain written controls and senior compliance ownership.	Designate a knowledgeable senior officer and maintain CDD, PEP, reporting, records, confidentiality, employee-screening and training controls proportionate to risk.	Appointment, policies, training, screening and remediation log.	MLPCR 2019, regulations 12-14
Independently test the programme.	Maintain an independent audit function and supervise branches, subsidiaries and representative offices for compliance.	Audit plan, reports, findings and closure evidence.	MLPCR 2019, regulation 15

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

CDD uses reliable independent evidence and continues through the relationship.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify the customer and representative.	Use reliable independent documents, data or information; verify any representative's identity and authority before reliance.	Identity file, source provenance, mandate and verification result.	MLPCR 2019, regulations 3 and 6; MLPCA 2008, sections 16-17
Understand purpose and expected activity.	Record relationship purpose, intended nature, expected volumes, counterparties, geography and source of funds sufficient for risk rating and monitoring.	Customer profile, expected-activity baseline and approval.	MLPCR 2019, regulation 4
Do not proceed where mandatory CDD fails.	Do not open or establish the relationship when identity, beneficial ownership, ownership/control structure or purpose cannot be completed; terminate existing relationships in the circumstances prescribed and consider confidential reporting.	Decline or exit decision, investigation and restricted reporting record.	MLPCR 2019, regulation 7

KYB, registries, and beneficial ownership

CDD control analysis and company-register disclosure are related but distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence, governance and authority.	Obtain a current company extract, incorporation and governing records, registered and principal addresses, directors, shareholders, signatories, licences and mandates; reconcile inconsistencies.	Registry extract, constitutional records, powers and discrepancy log.	MLPCR 2019, regulation 3(4); Companies Act 2011
Identify natural-person beneficial owners for CDD.	Identify the natural persons with controlling ownership, then control by other means, and use relevant senior management only when no natural person is identified through ownership or control; apply the trust and legal-arrangement tests separately.	Ownership chart, control analysis, verified identities and fallback rationale.	MLPCR 2019, regulation 6(5)-(6)
Apply the company-register test and deadlines separately.	For a Lesotho company, identify each natural person meeting any 2024 test, including direct or indirect ownership of more than 10% of shares or votes, appointment/removal power, influence or ultimate effective control; maintain and file confirmed particulars within the applicable 7-day periods and record changes.	Company BO register, identity evidence, filing receipt and change log.	Companies (Beneficial Ownership) Regulations 2024, regulations 3-8

PEPs, EDD, and remote onboarding

PEPs and higher-risk or remote relationships require enhanced controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Detect PEP exposure.	Use appropriate systems to identify domestic, foreign and international-organisation PEP exposure in customers, beneficial owners and connected persons.	Screening, relationship map, match decision and refresh log.	MLPCA 2008, section 2; MLPCR 2019, regulations 12 and Schedule 5
Apply enhanced approval, provenance and monitoring.	For PEP and other higher-risk relationships, obtain senior approval, establish source of wealth and funds to the extent required by risk, and conduct enhanced ongoing monitoring.	Approval, provenance analysis and monitoring plan.	MLPCR 2019, regulations 5 and 10; Schedule 5
Control remote and biometric onboarding.	Assess identity, impersonation, device, liveness, minimisation, sensitive-data and security risks before deployment; document a valid processing basis and exceptions.	Remote-onboarding assessment, privacy review, tests and approvals.	MLPCR 2019, regulations 5 and 12; Data Protection Act 2012, sections 15-22 and 29-37

Monitoring and suspicious reporting

FIU reporting must be immediate, complete and confidential.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor activity against the customer profile.	Scrutinise transactions throughout the relationship for consistency with customer, business, risk and source-of-funds knowledge and investigate unusual activity.	Alerts, investigation, disposition and rule governance.	MLPCR 2019, regulation 4(b)
Report suspicion and attempts immediately.	Submit the prescribed report to the FIU immediately upon forming suspicion and in any case no later than 7 days, regardless of amount; include attempted transactions and explain any delay in writing.	Decision chronology, report, delay explanation if any, receipt and supplements.	MLPCR 2019, regulation 19(1)-(10)
Prevent tipping off.	Restrict access and do not disclose the report, its contents or filing; do not seek abnormal information from the customer in a way that would reveal the process.	Access logs, confidentiality procedure and training.	MLPCR 2019, regulation 19(11)-(14); MLPCA 2008, section 22

Payments, wires, thresholds, and agents

Thresholds are scoped by sector and instrument, not universal.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Configure only verified thresholds.	Apply the M25,000 casino and specified designated-business cash triggers and M100,000 precious-metal or precious-stone cash trigger only to their stated categories; obtain current FIU or supervisor instruments for any other prescribed threshold.	Legal mapping, configuration, test cases, filings and receipts.	MLPCR 2019, regulations 22-23
Preserve required wire-transfer information.	Carry complete originator and beneficiary information, monitor missing data, and reject, suspend or escalate incomplete transfers under the applicable ordering, intermediary and beneficiary rules.	Message samples, validation rules, exceptions and escalation.	MLPCR 2019, regulations 40-45
Retain accountability for agents and third parties.	Verify permissions, conduct due diligence, contract for confidentiality, security and prompt record access, and keep ultimate responsibility for relied-on CDD.	Due diligence, contract, monitoring and retrieval test.	MLPCR 2019, regulations 9 and 12; CBL Agent Banking Regulations 2024

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Use current UN and communicated domestic lists under the statutory process.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen applicable designations.	Regularly obtain current UN lists and screen customers, beneficial owners, controllers, representatives and relevant transactions at onboarding, list updates and before execution.	List inventory, update logs, screening configuration and dispositions.	MLPCR 2019, regulations 27(2)-(3) and 27(10)
Freeze covered property without delay or notice.	On a designation and freezing order, freeze covered funds or assets without delay and prior notice and prevent funds, assets, economic resources or services from being made available.	Freeze procedure, timestamps, legal basis and authority communication.	MLPCR 2019, regulations 28-30
Govern false positives, exceptions and release.	Escalate matches through the current FIU, supervisor or competent-authority process; permit access or release only on documented lawful authority and preserve the full rationale.	Reports, match rationale, authority instruction and reconciliation.	MLPCR 2019, regulations 31-33

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Records must reconstruct the customer, transaction, ownership and decision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain AML records for at least five years.	Retain CDD, account, correspondence, analysis and domestic or international transaction records for at least 5 years from relationship termination or the occasional transaction, and longer when directed for up to a further 5 years.	Schedule, configuration, archive sample and legal-hold log.	MLPCR 2019, regulation 11
Retain company BO history for the separate period.	Keep required company beneficial-owner information for at least 10 years after a person ceases to be a beneficial owner and preserve dissolved-company information as required.	BO history, filing records and retention test.	Companies (Beneficial Ownership) Regulations 2024, regulations 12-13
Respond securely to competent requests.	Authenticate requests, protect FIU-report confidentiality, produce records swiftly and reproducibly, and log scope, timing and receipt.	Request, approval, production index and acknowledgement.	MLPCR 2019, regulations 11 and 16-17

10. PRIVACY, BIOMETRICS, AND TRANSFERS

Privacy, biometrics, and transfers

Identity processing must comply with the Data Protection Act and AML holds.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document a lawful, minimal and transparent processing basis.	Map purpose, legal basis, data, notice, recipients, rights and retention; notify the Data Protection Commission before processing where section 25(5) applies.	Data inventory, legal assessment, notices and Commission record.	Data Protection Act 2012, sections 15-19 and 25
Protect data and govern processors and incidents.	Apply reasonable technical and organisational safeguards, bind agents by written confidentiality and security terms, and notify the Commission and affected subjects as soon as reasonably possible after a qualifying compromise.	Risk assessment, contracts, security tests and incident records.	Data Protection Act 2012, sections 20-23
Control sensitive data and cross-border processing.	Treat biometrics and other sensitive data under the Act's prohibitions and exceptions; document legal authority and take reasonable steps concerning an overseas agent's compliance before transfer or access.	Sensitive-data assessment, transfer analysis and approval.	Data Protection Act 2012, sections 22 and 29-37

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Maintain concise packs that reproduce decisions and support supervision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, KYB, beneficial ownership, screening, risk, approvals, privacy records and exceptions under stable identifiers.	Complete sampled onboarding pack.	Operational control supporting MLPCR 2019, regulations 3-15
Maintain a reconstructable monitoring and reporting pack.	Link transactions, alerts, analysis, approvals, reports and post-filing controls while protecting confidentiality.	Complete sampled case pack and access log.	Operational control supporting MLPCR 2019, regulation 19

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 2008
LesLII / Office of Parliamentary Counsel of Lesotho · Primary national legislation - consolidation notes outstanding 2016 amendment
Open official source

Money Laundering and Proceeds of Crime (Amendment) Act 2016
LesLII / Office of Parliamentary Counsel of Lesotho · Primary amending legislation
Open official source

Money Laundering and Proceeds of Crime Regulations 2019
LesLII / Office of Parliamentary Counsel of Lesotho · Primary national regulations
Open official source

Companies Act 2011
LesLII / Office of Parliamentary Counsel of Lesotho · Primary company legislation
Open official source

Companies (Beneficial Ownership) Regulations 2024
Lesotho Digital Business Registrations / Registrar of Companies · Primary company regulations
Open official source

Data Protection Act 2012
LesLII / Office of Parliamentary Counsel of Lesotho · Primary privacy legislation
Open official source

Central Bank of Lesotho legislation and regulations
Central Bank of Lesotho · Official financial regulator materials
Open official source

Financial Intelligence Unit of Lesotho
Financial Intelligence Unit of Lesotho · Official FIU materials
Open official source

Lesotho second-round mutual evaluation report
ESAAMLG · Authoritative country assessment
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 29 August 2026 / Last reviewed 29 August 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 29 August 2026. Confirm current FIU registration and filing specifications, prescribed transaction-reporting thresholds, sanctions communications, Data Protection Commission procedures, and product-specific permissions with the competent authority and qualified Lesotho counsel before launch.