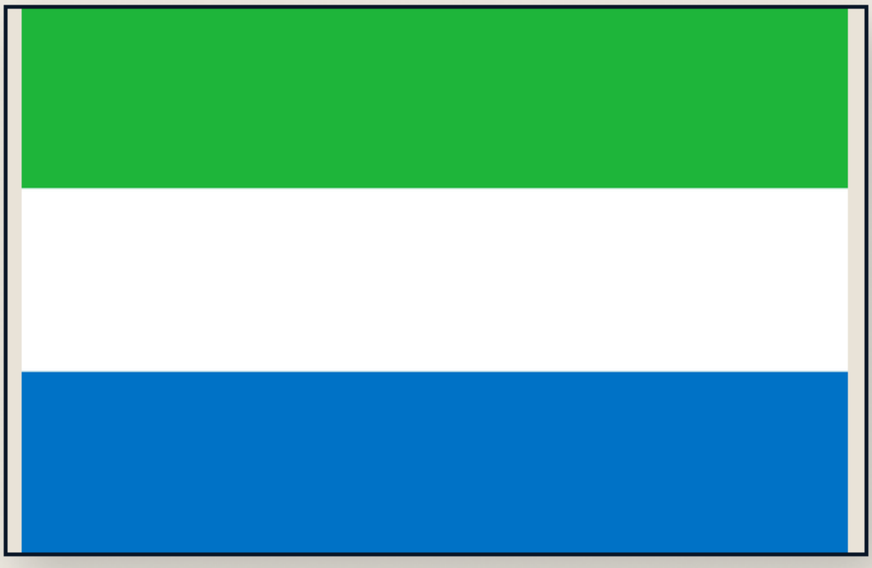
VOVE ID

VOVE COUNTRY CONTROL FILE

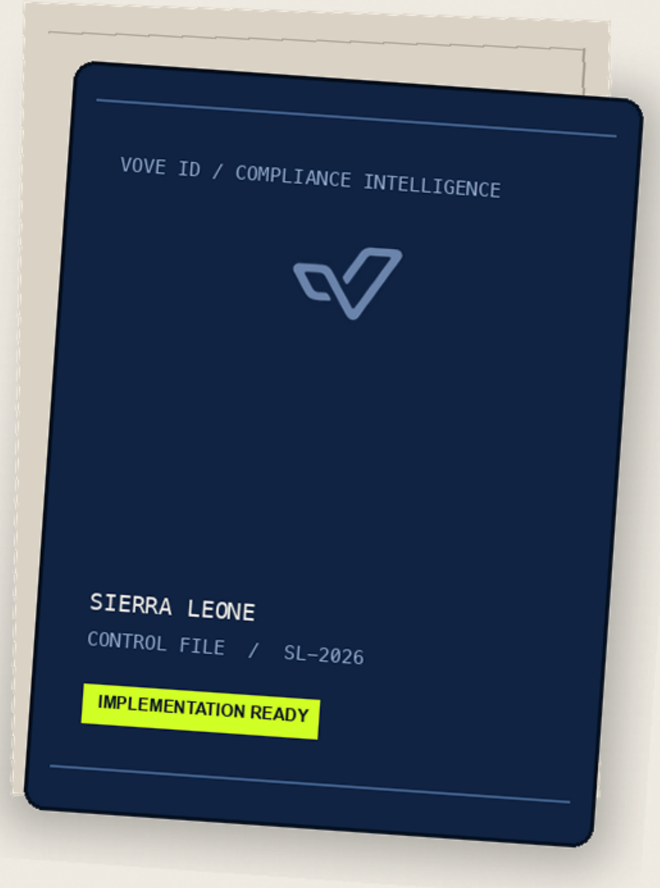
KYC / KYB / AML

2026 EDITION

SIERRA LEONE



SIERRA LEONE / SL



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Sierra Leone KYC, KYB, AML, CFT, CPF and Data Governance Compliance Checklist 2026

An implementation checklist for customer and business verification in Sierra Leone under the 2024 AML/CFT/CPF Act, payment-system rules, sanctions controls and company-registration requirements.

Primary AML/CFT/CPF law	**Act 4 of 2024, Gazette 44 of 6 June 2024**
Financial intelligence unit	**Financial Intelligence Agency (FIA)**
STR timing	**As soon as practicable and no later than two days after suspicion or information**
Occasional-transaction CDD	**SLE 30,000 or more, including linked transactions within 24 hours**
Wire-transfer CDD	**SLE 3,000 or more for domestic or international wires**
Core AML retention	**At least five years, with the start event determined by record class**
Sanctions asset report	**As soon as reasonably practicable and within two working days under section 42**
Beneficial ownership	**Natural persons who ultimately own/control or exercise ultimate effective control; no universal AML percentage**
Payments and VASPs	**Activity-specific BSL or relevant-supervisor authority required before operations**
FATF public lists	**Not named in FATF statements dated 19 June 2026; GIABA enhanced follow-up continues**

Scope and legal framework

The Anti-Money Laundering and Combating of Financing of Terrorism and Financing the Proliferation of Weapons of Mass Destruction Act, 2024 (Act 4 of 2024) is the principal AML/CFT/CPF statute, continues the Financial Intelligence Unit as the Financial Intelligence Agency and repeals the 2012 Act subject to savings. The National Payment Systems Act, 2022 regulates payment services under BSL. NIB administers business and company registration. The current company-law transition and sector-specific privacy rules must be confirmed before implementation.

FATF context

As at 18 July 2026, Sierra Leone was not named in FATF's 19 June 2026 public statements on jurisdictions under increased monitoring or jurisdictions subject to a call for action. Sierra Leone remains in GIABA enhanced follow-up; the 2025 fifth enhanced follow-up report assesses technical compliance rather than FATF public-list status.

IMPORTANT	This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 18 July 2026. Confirm FIA directives, reporting channels and threshold-report specifications; BSL licensing and product conditions; NIB company-law commencement, forms and beneficial-ownership procedures; sanctions instructions; and applicable privacy requirements with Sierra Leone counsel and the competent authority before launch. VOVE ID supports evidence collection and audit trails; the reporting entity remains responsible for acceptance, reporting, restraint and compliance decisions.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

1. SCOPE, AUTHORITIES AND REGULATED ACTIVITIES

Scope, authorities and regulated activities

Resolve entity, activity and supervisor scope before launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial institutions and listed DNFBPs are reporting entities under the 2024 Act.	Map each entity, product, profession, branch, agent and outsourced service to the First Schedule and its supervisor.	Perimeter memorandum, entity-product map, licences and supervisor register.	2024 Act, ss.1-2 and First Schedule
The FIA receives, analyses and disseminates reports and may issue binding guidelines and directives.	Register compliance contacts and obtain the current FIA reporting access, formats and instructions.	FIA correspondence, access records, contacts and regulatory calendar.	2024 Act, ss.3, 20 and 167
Payment services, money transmission, financial services and VASP activity require applicable authority before operations.	Obtain a written BSL or relevant-supervisor perimeter decision and every licence or registration before pilot or launch.	Classification, application, licence, conditions and approved product map.	2024 Act, ss.59 and 103; National Payment Systems Act 2022

Governance, risk assessment and control ownership

Build documented, risk-based and accountable controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting entities identify and assess customer, product, delivery, geography and technology risks and apply mitigation.	Maintain enterprise, product and customer risk assessments and assess new products before launch.	Methodology, assessments, approvals, overrides and remediation.	2024 Act, ss.51-53
Risk assessments are refreshed on events and at the Act's risk-tier intervals and submitted after completion.	Confirm the applicable tier, calendar the statutory review and one-calendar-month submission, and preserve receipts.	Risk classification, calendar, assessment, submission and receipt.	2024 Act, s.53(1)-(3)
A senior compliance officer and internal AML/CFT/CPF programme, training and independent assurance are required.	Appoint an empowered officer, approve procedures, train relevant staff and test the lifecycle.	Appointment, charter, procedures, training and audit reports.	2024 Act, ss.70-72, 159-160

3. NATURAL-PERSON IDENTIFICATION AND CDD

Natural-person identification and CDD

Apply every statutory trigger without treating thresholds as safe harbours.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identity verification applies at account or relationship opening, SLE 30,000 occasional activity, SLE 3,000 wires, suspicion and identity doubt.	Configure all triggers, including linked occasional transactions within 24 hours and amount-independent suspicion.	Trigger matrix, aggregation tests, cases and exceptions.	2024 Act, ss.55-56 and 60
Natural persons are verified from reliable independent official documents and address evidence.	Capture and authenticate identity, address, occupation and national-identification or passport evidence.	Identity file, authenticity result, address proof and screening decision.	2024 Act, ss.56(1)-(2), 57(3)(c)
Purpose, intended nature, expected activity and source/destination information are understood proportionately.	Create an expected-activity profile and investigate material deviations.	Purpose statement, profile, source evidence, alerts and reviews.	2024 Act, ss.55, 57(3), 68
Deferred verification is exceptional, risk-controlled and cannot exceed two calendar months.	Restrict activity, set a shorter completion SLA and close or consider an STR if evidence remains incomplete.	Exception approval, restrictions, completion or closure and STR decision.	2024 Act, s.57(6)-(8)

KYB, authority and beneficial ownership

Verify existence, authority and ultimate natural-person ownership or control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Legal-entity CDD verifies legal existence, registered office, directors, powers, owners, beneficiaries and control structure.	Obtain current NIB evidence and constitutive records and reconcile directors, mandates and ownership.	Registry extract, certificate, constitution, annual return, directors and discrepancy log.	2024 Act, ss.1, 56(3)-(4), 57(3)(d)
Representatives require verified identity and authority.	Verify each representative separately and validate the mandate before activity.	Identity file, mandate, board authority and verification result.	2024 Act, ss.55(5)(a), 57(3)(d)(iii)
Beneficial owners are natural persons who ultimately own or control or exercise ultimate effective control.	Trace every ownership layer, test non-ownership control and verify each identified natural person without inventing a universal percentage.	Ownership chart, source records, control analysis and BO identity files.	2024 Act, s.1 definitions of beneficial owner and customer due diligence; s.57
Trust information covers settlor, trustees, protector, beneficiaries or class and every natural person exercising ultimate effective control.	Verify the trust instrument, roles, powers and relevant natural persons.	Trust deed, role register, control analysis and identity files.	2024 Act, s.57(13)

PEPs, enhanced due diligence and remote onboarding

Apply stronger controls to higher risk and non-face-to-face relationships.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Systems determine whether customers, beneficial owners and relevant insurance beneficiaries are PEPs.	Screen before activation and continuously and resolve family and close-associate exposure.	Screening, match decision, role and relationship evidence.	2024 Act, ss.1 and 63
PEPs require senior-management approval, reasonable source-of-wealth and source-of-funds measures and enhanced monitoring.	Corroborate source evidence, document approval and configure enhanced monitoring.	Source file, approval, monitoring plan and reviews.	2024 Act, s.63
Remote CDD must be no less effective than in-person CDD and use additional independent or confirmatory evidence.	Use document-integrity, liveness/presence, independent-data, device and fraud controls proportionate to risk.	Remote standard, test results, fraud logs and exceptions.	2024 Act, s.62
Third-party reliance does not transfer ultimate responsibility and requires immediate information and documents without delay.	Assess supervision and jurisdiction, contract for access and test document retrieval.	Due diligence, agreement, retrieval tests and monitoring.	2024 Act, s.61

Failed CDD, monitoring and suspicious reporting

Block unsafe activity and report suspicion promptly and confidentially.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Failed CDD prevents account establishment or continuation and may require an STR.	Block activation or terminate under controlled procedures and send the case to confidential reporting review.	Failure reason, block, closure, STR decision and receipt.	2024 Act, ss.55(6), 57(2), 65, 153
Ongoing monitoring keeps customer and BO information current and examines complex, unusual and large activity.	Configure risk and event refresh, transaction scenarios and documented investigation of unusual activity.	Refresh schedule, alerts, cases, findings and updated CDD.	2024 Act, ss.68 and 53(4)
Suspected transactions, attempts, information or facts linked to ML, TF or PF are reportable to FIA.	Escalate immediately, preserve the suspicion timestamp and submit the prescribed STR.	Internal report, analysis, STR, receipt and timeline.	2024 Act, ss.76-78
An STR is due as soon as practicable and no later than two days after suspicion or information.	Use a shorter internal SLA measured from the recorded formation or receipt time.	Trigger timestamp, approval, submission time and SLA monitoring.	2024 Act, s.76(1)
Tipping off is prohibited and good-faith reporting is protected.	Restrict access and govern customer communications and lawful disclosures.	Access logs, communication plan, training and disclosure register.	2024 Act, ss.80-83

Wires, thresholds, payments and agents

Keep CDD, internal lists and FIA-prescribed reports distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Wire transfers carry required originator and beneficiary information and deficient messages require governed action.	Validate fields through the chain and execute, reject, suspend or report under risk-based procedures.	Field matrix, validation, repair/reject queue and samples.	2024 Act, ss.67 and 69
The Act requires an internal list for currency-exchange and money-transmission cash transactions of SLE 3,000 or more.	Maintain the list and do not misstate it as a universal FIA filing threshold; apply current FIA cash/foreign-report thresholds separately.	Scope memo, internal list, FIA directive and report receipts.	2024 Act, ss.66(4) and 76(6)
Licensed payment providers and operators comply with AML rules and ensure agent compliance.	Include agents in the programme, maintain a current list and monitor outsourced controls.	Licence, agent register, contracts, monitoring and remediation.	National Payment Systems Act 2022, ss.22 and 36; 2024 Act, ss.59(4), 69(13)
VASPs must identify risks, obtain relevant-supervisor registration and licence before operating and transmit originator/beneficiary information.	Do not launch until the competent supervisor confirms perimeter, authority and transfer-data requirements.	Legal classification, registration, licence, travel-rule design and tests.	2024 Act, s.103

Targeted financial sanctions

Screen current domestic, UN and ECOWAS designations and act promptly.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Business relationships and dealings with sanctioned persons, entities, groups and specified sanctioned-country interests are prohibited.	Screen customers, BOs, representatives, counterparties, vessels and transactions at onboarding and list change.	List provenance, screening logs, match decisions and population reconciliation.	2024 Act, ss.35-39
Suspected sanctioned ownership or control is referred immediately in writing to the Director-General or competent authority.	Maintain a 24/7 escalation route, hold relevant activity and seek written verification without alerting the subject.	Match analysis, request, hold and response.	2024 Act, s.41
Assets held for sanctioned persons or entities are reported as soon as reasonably practicable and within two working days.	Inventory affected assets and report through the current FIA or competent-authority procedure.	Asset inventory, trigger time, report and receipt.	2024 Act, s.42

Records, access and assurance

Retain reconstructable evidence under the correct clock.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD, transaction, unusual-activity findings and STR records are kept for at least five years under class-specific clocks.	Map each record class to transaction completion, relationship end or report date and apply legal holds.	Retention schedule, configuration, samples and deletion tests.	2024 Act, s.66
Records must reconstruct transactions and be immediately or swiftly available to FIA and competent authorities.	Index linked identity, transaction, investigation and reporting evidence and test retrieval.	Request register, retrieval tests, access controls and response package.	2024 Act, ss.66 and 69(11)
Governed backups and authentication are required for machine-readable or electronic records.	Test backup, recovery, integrity and authorised access for the full retention period.	Architecture, backup tests, audit logs and recovery evidence.	2024 Act, s.66(5)

Privacy, identity data and transfers

Apply verified sector rules and cautious data governance while national privacy law remains in transition.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Payment providers process and retain necessary personal data and follow statutory consent, fraud-prevention and disclosure rules.	Document necessity and permissions, minimise fields and prohibit unauthorised sale or sharing.	Data inventory, notices, permissions, access logs and sharing register.	National Payment Systems Act 2022, s.21
Sensitive identity and biometric processing requires documented necessity, security and access governance even where no comprehensive statute is asserted.	Complete legal, privacy and security assessments before biometric use and contractually control processors.	Assessment, data flow, access controls, testing and vendor assurance.	Recommended control; sector duties and applicable law must be confirmed
Cross-border transfers, incidents and deletion require a verified legal basis and sector procedure.	Confirm current Sierra Leone requirements with counsel and regulators before implementation; do not invent a notification deadline.	Legal memo, transfer map, incident playbook, contracts and decisions.	Controlled uncertainty; National Payment Systems Act 2022, s.21 where applicable

Practical evidence packs and change control

Make decisions reconstructable and keep time-sensitive rules current.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A complete customer file links identity, KYB, ownership, screening, risk, approval, monitoring and reporting decisions.	Block activation when mandatory evidence or approval is missing and preserve the release decision.	Control checklist, linked file, approvals and release log.	2024 Act, Part IX
FIA directives, thresholds, sanctions lists, FATF status, company law, licensing and privacy requirements require ongoing monitoring.	Assign owners and review FIA, BSL, NIB, Gazette, FATF and GIABA sources on a governed schedule.	Legal inventory, source log, change assessments and implementation tickets.	Official sources listed below

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.

AML/CFT/CPF Act, 2024 (Act 4 of 2024)
Sierra Leone Gazette text via SierraLII · Primary legislation reproduction
Open convenience reproduction

National Payment Systems Act, 2022
Sierra Leone Gazette text via SierraLII · Primary legislation reproduction
Open convenience reproduction

Bank of Sierra Leone
Bank of Sierra Leone · Official regulator
Open official source

BSL legislation and regulatory framework
Bank of Sierra Leone · Official regulator
Open official source

National Investment Board Act, 2022
Sierra Leone Gazette text via SierraLII · Primary legislation reproduction
Open convenience reproduction

NIB business registration and corporate affairs
National Investment Board · Official company registry guidance
Open official source

NIB business forms including beneficial ownership
National Investment Board · Official company registry guidance
Open official source

Sierra Leone fifth enhanced follow-up report, 2025
GIABA · Authoritative regional assessment
Open official source

Jurisdictions under Increased Monitoring - 19 June 2026
FATF · Authoritative public statement
Open official source

High-Risk Jurisdictions subject to a Call for Action - 19 June 2026
FATF · Authoritative public statement
Open official source

Document control

Version 1.0 / Published 2026 / Last reviewed 18 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 18 July 2026. Confirm FIA directives, reporting channels and threshold-report specifications; BSL licensing and product conditions; NIB company-law commencement, forms and beneficial-ownership procedures; sanctions instructions; and applicable privacy requirements with Sierra Leone counsel and the competent authority before launch. VOVE ID supports evidence collection and audit trails; the reporting entity remains responsible for acceptance, reporting, restraint and compliance decisions.