VOVE ID

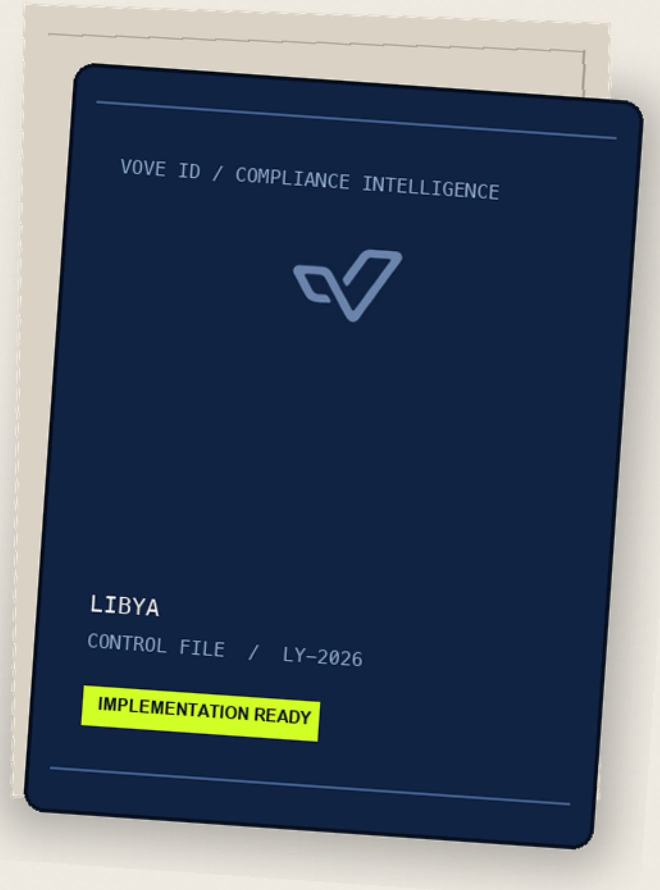
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

LIBYA

LIBYA / LY



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Libya KYC, KYB & AML Compliance Checklist

An implementation checklist for Libya's AML/CFT framework, FIU reporting, customer and beneficial-owner diligence, sanctions, records, electronic transactions, data safeguards and regulated financial services.

FIU	**Libyan Financial Information Unit**
Primary AML rule	**Resolution No. 1013 of 2017 issuing the AML/CFT Law**
Suspicion reporting	**Without delay; FIU guide says within 24 hours**
Thresholds	**Committee and sector specific; no universal amount asserted**
Core AML retention	**At least 5 years**
FATF status	**Not named on FATF public lists as at 19 June 2026**

Scope and legal framework

Presidential Council Resolution No. 1013 of 2017 issuing the Anti-Money Laundering and Terrorism Financing Law is the current operational preventive-measures baseline used by the Libyan FIU and Central Bank. It repealed Law No. 2 of 2005 while preserving non-conflicting instruments. Apply it with current FIU and sector instructions, Resolution No. 1037 of 2017 on UN Security Council measures, Law No. 6 of 2022 on Electronic Transactions, and product-specific Central Bank rules.

FATF context

Libya is a MENAFATF member. MENAFATF's 2024 annual report states that Libya's second-round mutual evaluation remained deferred because of security conditions and that a technical-compliance self-assessment covered selected recommendations. Libya 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 31 August 2026. Confirm the current legal and territorial application of national instruments, committee-set CDD and wire thresholds, FIU filing specifications, sanctions communications, registry evidence, data rules and product-specific permissions with the competent authority and qualified Libyan 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.

Scope, authorities, and licensing

Resolve the reporting entity, regulated activity, territory and supervisor before launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is in AML/CFT scope.	Map every entity, product, channel and profession to the financial-institution, DNFBP or nonprofit categories under Resolution 1013/2017; identify the FIU and each competent sector supervisor.	Applicability memo, product map and accountable-owner register.	Resolution 1013/2017, Articles 1, 12 and 15
Complete current FIU and supervisory registration.	Confirm registration required by the competent supervisor, obtain the current FIU reporting form and secure-channel instructions, and test user authority, delivery and receipts.	Registration, authority correspondence, channel test and contact log.	Resolution 1013/2017, Articles 9, 12 and 15; Libyan FIU reporting page
Obtain authorisation before regulated activity.	Classify banking, payments, e-money, remittance, foreign exchange, insurance, securities, agent, fintech and virtual-asset activities and obtain every required approval before launch.	Perimeter analysis, licences, conditions and renewal calendar.	Resolution 1013/2017, Articles 12-15 and 50; applicable Central Bank and sector rules

Governance and risk assessment

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a written ML/TF risk assessment.	Assess customers, products, delivery channels, geography, cash, agents, technology, virtual assets and proliferation exposure; update the assessment periodically and before material change.	Approved methodology, assessment, controls and version history.	Resolution 1013/2017, Article 16
Maintain senior compliance ownership and written controls.	Establish a management-level compliance arrangement and written CDD, monitoring, reporting, records, confidentiality, employee-screening, training and group controls proportionate to the business.	Appointment, policies, training, screening and board reporting.	Resolution 1013/2017, Articles 32-34
Independently test the programme.	Use an adequately resourced internal-audit or independent review function to test design and operation, document deficiencies and track remediation through closure.	Audit plan, reports, findings and closure evidence.	Resolution 1013/2017, Article 32

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 and prohibit anonymous or clearly fictitious-name accounts.	Identity file, source provenance, mandate and verification result.	Resolution 1013/2017, Article 19(1)-(2)
Understand purpose and expected activity.	Record the purpose and intended nature of the relationship, expected activity, counterparties, geography and source information sufficient for risk rating and ongoing monitoring.	Customer profile, expected-activity baseline and approval.	Resolution 1013/2017, Article 19(2)
Do not proceed where mandatory CDD fails.	Refrain from opening, establishing or executing, or terminate the relationship, when required identification or verification cannot be completed; consider a confidential suspicious report.	Decline or exit decision, investigation and restricted reporting record.	Resolution 1013/2017, Article 25

KYB, registries, and beneficial ownership

Verify legal existence, authority, ownership and control without inventing a percentage threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence, activities and authority.	Obtain current commercial-registry evidence, constitutional records, registered address, directors, senior managers, shareholders, signatories, licences and mandates; reconcile inconsistencies.	Registry extract, governing records, powers and discrepancy log.	Resolution 1013/2017, Article 19(2)-(3); Commercial Activity Law No. 23 of 2010
Apply the statutory beneficial-owner cascade.	Identify natural persons holding a controlling share or controlling through other means; use the responsible manager only when no natural person is identified through those limbs, and verify identities with reliable independent evidence.	Ownership chart, control analysis, verified identities and fallback rationale.	Resolution 1013/2017, Article 19(2)-(3)
Keep company and ownership evidence current.	Monitor changes to legal form, registration, ownership, control, directors and authority; refresh registry and customer evidence according to risk and investigate discrepancies.	Refresh schedule, extracts, declarations and discrepancy decisions.	Resolution 1013/2017, Articles 19 and 29; Commercial Activity Law No. 23 of 2010

PEPs, EDD, and remote onboarding

PEPs, higher-risk and non-face-to-face relationships require enhanced controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Detect PEP exposure.	Use appropriate risk-management systems to identify whether a customer or beneficial owner is a PEP, including relevant family members and close associates.	Screening, relationship map, match decision and refresh log.	Resolution 1013/2017, Article 23
Apply enhanced approval, provenance and monitoring.	Obtain senior-management approval, take reasonable measures to establish source of wealth and funds, and apply enhanced ongoing monitoring to PEP relationships.	Approval, provenance analysis and monitoring plan.	Resolution 1013/2017, Article 23
Control remote and biometric onboarding.	Use sufficient defined measures for non-face-to-face customers; assess impersonation, liveness, device, data minimisation and security before deployment, and preserve a reliable electronic record.	Remote-onboarding assessment, data review, tests and approvals.	Resolution 1013/2017, Articles 16 and 19(7); Electronic Transactions Law No. 6 of 2022

Monitoring and suspicious reporting

FIU reporting must be prompt, 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 information; examine complex, unusually large or unexplained activity and document conclusions.	Alerts, investigation, disposition and rule governance.	Resolution 1013/2017, Articles 19 and 31
Report suspicion and attempts promptly.	Report to the Libyan FIU without delay any suspicious transaction or attempt regardless of value; operationalise the FIU guide's expectation to submit within 24 hours after reasonable grounds arise.	Decision chronology, STR or SAR, supporting material, delivery and receipt.	Resolution 1013/2017, Article 27; FIU Suspicious Transaction Reporting Guide 2023
Prevent tipping off.	Restrict access and do not disclose a report, submitted information or related investigation to the customer or unauthorised persons.	Access logs, confidentiality procedure and training.	Resolution 1013/2017, Article 28

Payments, wires, thresholds, and agents

Amounts are set by current committee or sector instruments rather than one universal threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Configure only verified CDD thresholds.	Apply occasional-transaction CDD and aggregation only at the current amount set by the National Committee or relevant sector rule; retain the authoritative instrument and do not infer a universal threshold.	Legal mapping, configuration, test cases and approval.	Resolution 1013/2017, Articles 18-19; National Committee Decision No. 1 of 2019
Preserve required wire-transfer information.	For transfers above the current committee-set amount, obtain and verify originator and beneficiary information, carry it in the payment message, retain it and apply risk-based rules to incomplete transfers.	Threshold authority, message samples, validation rules and exceptions.	Resolution 1013/2017, Article 26; National Committee Decision No. 1 of 2019
Retain accountability for agents and third parties.	Verify permissions, conduct due diligence, contract for confidentiality, security and prompt record access, and retain primary responsibility for relied-on CDD and outsourced activity.	Due diligence, contract, monitoring and retrieval test.	Resolution 1013/2017, Articles 22 and 32; applicable Central Bank payment rules

Targeted financial sanctions

Use current UN and national designations and Libya's statutory implementation process.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen applicable designations promptly.	Obtain current UN and communicated national 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.	Resolution 1013/2017, Article 81; Resolution 1037/2017
Freeze covered funds and resources without delay.	On a confirmed designation, freeze covered funds and economic resources without prior notice, prevent prohibited availability and notify the implementing authority within three days.	Freeze procedure, timestamps, legal basis, report and authority communication.	Resolution 1013/2017, Article 81(6)-(8); Resolution 1037/2017
Govern false positives, exceptions and release.	Escalate potential matches through the current implementing-authority process; permit access, exemption, unfreezing or delisting only on documented lawful authority.	Match rationale, reports, authority instruction and reconciliation.	Resolution 1013/2017, Article 81(10); Resolution 1037/2017

Records and regulator access

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain core AML records for at least five years.	Keep identity, beneficial ownership, account, correspondence and analysis records for at least 5 years after the relationship ends or after an occasional transaction.	Schedule, configuration, archive sample and legal-hold log.	Resolution 1013/2017, Article 29(1)
Retain attempted and completed transaction records.	Keep records sufficient to reconstruct attempted and completed transactions for at least 5 years after the attempt or completion, and longer when a competent authority requires it.	Transaction archive, attempted-transaction log and retrieval test.	Resolution 1013/2017, Article 29(1)-(2)
Respond securely to competent requests.	Authenticate requests, protect reporting confidentiality, produce reconstructable records promptly and log scope, timing and receipt.	Request, approval, production index and acknowledgement.	Resolution 1013/2017, Articles 6, 12 and 30

Privacy, biometrics, and transfers

Apply Libya's electronic-transactions and sector data rules to the extent they cover the processing; do not present them as a general comprehensive privacy code.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map the applicable data rule and processing purpose.	Document statutory AML purposes, notices, data categories, access, sharing and retention; separately identify when Electronic Transactions Law Articles 73-79 or a sector rule applies.	Data inventory, applicability assessment, notices and retention map.	Electronic Transactions Law No. 6 of 2022, Articles 73-79; Resolution 1013/2017, Article 29
Protect identity and reporting data.	Apply proportionate confidentiality, access, integrity, incident and processor controls, with heightened restrictions for suspicious-report information.	Risk assessment, contracts, security tests and incident records.	Resolution 1013/2017, Article 28; Electronic Transactions Law No. 6 of 2022, Articles 75-76
Control covered cross-border personal-data transfers.	Where Article 78 applies, assess the data, purpose, duration, destination law and commitments, relevant rules and security measures before transfer; separately confirm banking-sector requirements.	Transfer analysis, safeguards, contract and approval.	Electronic Transactions Law No. 6 of 2022, Article 78; Central Bank Circular No. 18 of 2025

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, data records and exceptions under stable identifiers.	Complete sampled onboarding pack.	Operational control supporting Resolution 1013/2017, Articles 16-25 and 29
Maintain a reconstructable monitoring and reporting pack.	Link transactions, alerts, analysis, approvals, FIU reports, delivery evidence and post-filing controls while protecting confidentiality.	Complete sampled case pack and access log.	Operational control supporting Resolution 1013/2017, Articles 27-32
Maintain a launch and change-control pack.	Record licensing, threshold sources, sanctions-list sources, privacy applicability, product risk, testing and authority confirmations before launch and material changes.	Signed launch pack, legal-source register and change approvals.	Operational control supporting Resolution 1013/2017, Articles 12-16 and 50

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.

Resolution No. 1013 of 2017 issuing the Anti-Money Laundering and Terrorism Financing Law
Libya Official Gazette / Law Society of Libya · Primary national legislation
Open official source

Official Gazette, 2018 special issue No. 1
Libya Ministry of Justice / Law Society of Libya · Official gazette record
Open official source

Legislation and regulatory instruments library
Libyan Financial Information Unit · Official FIU legal materials
Open official source

Suspicious transaction reporting instructions and form
Libyan Financial Information Unit · Official FIU reporting guidance
Open official source

Financial Information Unit annual report 2018-2023
Libyan Financial Information Unit · Official FIU report
Open official source

Laws library, including Banking Law and Commercial Activity Law
Central Bank of Libya · Official legislation library
Open official source

Regulatory Rules of the Libyan National Payment Scheme
Central Bank of Libya · Official payment-system rules
Open official source

Electronic Transactions Law No. 6 of 2022
Libya House of Representatives / Law Society of Libya · Primary national legislation
Open official source

MENAFATF annual report 2024
MENAFATF · Authoritative regional assessment record
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

United Nations Security Council Libya sanctions committee
United Nations · Authoritative country sanctions materials
Open official source

Document control

Version 1.0 / Published 31 August 2026 / Last reviewed 31 August 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 31 August 2026. Confirm the current legal and territorial application of national instruments, committee-set CDD and wire thresholds, FIU filing specifications, sanctions communications, registry evidence, data rules and product-specific permissions with the competent authority and qualified Libyan counsel before launch.