VOVE ID

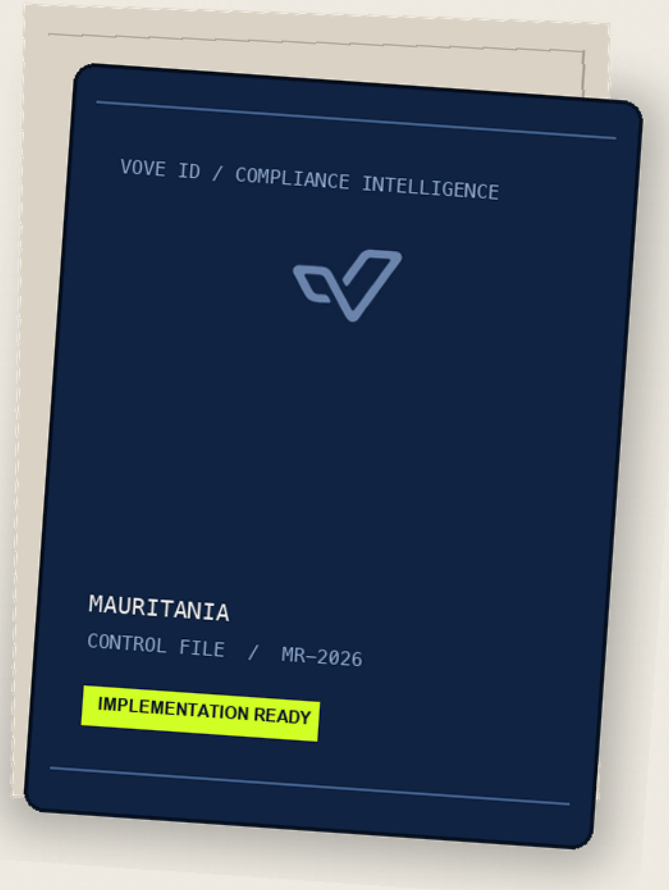
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

MAURITANIA

MAURITANIA / MR



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Mauritania KYC, KYB & AML Compliance Checklist

An implementation checklist for Mauritania's AML/CFT/CPF framework, financial-intelligence reporting, customer and beneficial-owner diligence, sanctions, records, privacy and regulated financial services.

FIU	**Mauritanian Financial Intelligence Unit**
Primary AML rule	**Law No. 2019-017 and Decree No. 2019-197, as amended in 2026**
Suspicion reporting	**Immediately, including attempted transactions**
Core AML retention	**At least 10 years after the relevant relationship or occasional transaction ends**
Targeted sanctions	**Freeze within 8 hours of publication; notify within 24 hours**
FATF status	**Not publicly listed as at 19 June 2026**

Scope and legal framework

Law No. 2019-017 of 20 February 2019 is the principal AML/CFT law. Apply it with Decree No. 2019-197 and the 2026 amendments made by Decrees Nos. 115, 116 and 117, current Central Bank and sector rules, Law No. 2017-020 on personal-data protection and current decisions of the Personal Data Protection Authority.

FATF context

Mauritania was not named in FATF's high-risk or increased-monitoring statements dated 19 June 2026. MENAFATF began preparations for a new mutual evaluation in 2025. Absence from FATF public lists is not a low-risk finding and does not replace the entity's own country-risk assessment.

IMPORTANT	General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 6 September 2026. Confirm the current Financial Intelligence Unit filing route, thresholds established by competent authorities, beneficial-owner filing procedures, sanctions notices, APD formalities and product-specific permissions with the relevant authority and qualified Mauritanian 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, activity and supervisor before launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is in AML/CFT scope.	Map every entity, product, branch, agent and profession to the financial-institution, designated non-financial business or profession, non-profit or other covered category and identify the FIU and competent supervisor.	Applicability memo, product map, licences and accountable-owner register.	Law 2019-017, Articles 1 and 6; Decree 2019-197, as amended
Establish the current FIU reporting route.	Designate authorised reporters, obtain the current form or secure procedure directly from the FIU, test delivery and preserve acknowledgements.	Appointments, reporter authority, channel test and receipt log.	Law 2019-017, Articles 15 and 29; Decree 2019-198, as amended by Decree 2026-116
Obtain authorisation before regulated activity.	Classify banking, payment, e-money, money-transfer, foreign-exchange, insurance, securities, fintech, agent and virtual-asset activities and obtain every required approval before launch.	Perimeter analysis, licences, conditions and renewal calendar.	Law 2019-017, Articles 1, 6 and 24-28; Central Bank official regulatory portal

Governance and risk assessment

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain risk-based internal controls.	Approve policies for CDD, beneficial ownership, PEPs, sanctions, monitoring, reporting, records, training, employee screening and independent testing.	Policy suite, approvals, control library, training and audit reports.	Law 2019-017, Article 6; Decree 2019-197, as amended
Identify, assess and document ML/TF risks.	Assess customers, countries, products, services, transactions, channels and new technologies before use and update the assessment continuously.	Risk assessment, methodology, source data, change log and approvals.	Law 2019-017, Article 6(1)
Apply enhanced measures to high-risk countries and situations.	Use the entity assessment, FIU directions and current FATF statements to trigger proportionate enhanced diligence and any required countermeasures.	Country-risk method, list updates, EDD decisions and monitoring results.	Law 2019-017, Articles 10-11

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Identify and verify customers, actors and beneficial owners at every applicable trigger.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify customers using reliable evidence.	Capture identity attributes, verify reliable independent documents or data, understand purpose and intended nature and establish expected activity before or during the legally permitted onboarding sequence.	CDD file, source provenance, verification, purpose and risk decision.	Law 2019-017, Article 6; Decree 2019-197, as amended
Apply CDD to occasional transactions, suspicion and identity doubt.	Configure the precise relationship, occasional-transaction, wire-transfer, suspicion and identity-quality triggers in the current implementing rules; never treat a threshold as a safe harbour.	Trigger matrix, aggregation tests, alerts and CDD timestamps.	Decree 2019-197, as amended by Decree 2026-115
Control remote and technology-enabled onboarding.	Assess impersonation, document, liveness, device and channel risks before use; apply stronger verification where risk is elevated and preserve the decision trail.	Channel assessment, verification results, fraud controls and exceptions.	Law 2019-017, Articles 6 and 10

KYB, registries, and beneficial ownership

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence and authority.	Obtain current commercial-register and constitutional evidence, registered and operating addresses, directors, licences and mandates; reconcile inconsistencies.	Registry extract, statutes, managers, licences, mandate and discrepancy log.	Law 2019-017, beneficial-owner definition and Article 6; Decree 2019-197, as amended
Identify and verify ultimate natural-person ownership and control.	Trace every ownership layer, identify each natural person who ultimately owns or controls the customer or on whose behalf a transaction occurs, and document control exercised by other means.	Ownership chart, control analysis, verified identities and rationale.	Law 2019-017, Article 1 definition of beneficial owner; Decree 2019-197, as amended
Do not rely on registry data alone.	Compare customer declarations, constitutional documents and available registry information and investigate discrepancies before acceptance and during refresh.	Source comparison, discrepancy decisions, update log and approvals.	Law 2019-017, Articles 6 and 10

PEPs, EDD, and reliance

Higher-risk relationships require enhanced, evidenced controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Detect PEP exposure.	Use appropriate tools to identify whether customers or beneficial owners hold or held prominent domestic, foreign or international-organisation functions, and assess family members and close associates under current rules.	Screening, relationship map, match decision and refresh log.	Law 2019-017, Article 9; Decree 2019-197, as amended
Apply proportionate enhanced diligence.	Obtain required senior approval, establish source of wealth and source of funds where applicable and intensify ongoing monitoring.	Approval, provenance analysis and enhanced-monitoring plan.	Law 2019-017, Articles 6(2), 9 and 10
Retain responsibility when using third parties or outsourcing.	Assess legal eligibility and control access to CDD records, service levels, confidentiality, audit rights, exit and regulator access; keep the reporting entity accountable.	Due diligence, agreement, retrieval test and assurance results.	Law 2019-017, Articles 6 and 12; Decree 2019-197, as amended

Monitoring and suspicious reporting

FIU reporting must be immediate, complete and confidential.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor and examine unusual activity.	Scrutinise activity against the customer profile and document the background and purpose of complex, important, unusual or apparently purposeless transactions.	Alerts, investigation, written findings and disposition.	Law 2019-017, Article 10
Report suspicion and attempts immediately.	Timestamp when suspicion or reasonable grounds arose and immediately report suspected funds, transactions and attempts to the FIU using its current route; provide requested supplements.	Decision chronology, report, supporting material, delivery and receipt.	Law 2019-017, Article 15
Prevent tipping off.	Restrict knowledge of reports and related action and disclose nothing to the customer or another unauthorised person.	Access controls, disclosure protocol, logs and training.	Law 2019-017, Article 16
Govern FIU suspension orders.	Maintain a continuously available process to implement an FIU suspension of up to five working days and a competent-authority extension of up to ten working days.	Escalation tree, timestamps, hold record and release authority.	Law 2019-017, Article 31

Payments, wires, thresholds, and agents

Keep CDD triggers, special examination and authority-set reports distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Do not invent a universal transaction-report threshold.	Obtain current threshold decisions and forms from the FIU, Committee or supervisor, document entity and transaction scope, aggregation, currency and filing mechanics before configuration.	Authoritative instrument, threshold register, tests, reports and receipts.	Law 2019-017, Article 33(14); Decree 2019-197, as amended
Preserve required wire-transfer information.	Capture required originator and beneficiary information, keep it through the payment chain and define reject, suspend, execute and follow-up rules for deficient transfers.	Field matrix, validation, repair queue, samples and decisions.	Law 2019-017, Article 13; Decree 2019-197, as amended
Control agents and payment intermediaries.	Confirm licensing and appointment requirements, allocate controls contractually, train and monitor agents and retain immediate access to customer and transaction evidence.	Approval, agent register, contracts, training, monitoring and remediation.	Law 2019-017, Articles 6 and 24-28; Central Bank official portal

Targeted financial sanctions

Screen, freeze, restrict and report within the current national deadlines.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen current authoritative designations.	Screen customers, beneficial owners, controllers, representatives and relevant transactions at onboarding, on list changes and before execution.	List inventory, update logs, screening configuration and dispositions.	Law 2019-017, Article 14; Decrees 2019-199 and 2026-117
Freeze designated property within eight hours of publication.	Freeze without prior notice all direct or indirect owned or controlled funds and other assets within eight hours and prevent funds, services or resources being made available.	Freeze procedure, publication and action timestamps, asset record and blocks.	National Counter-Terrorism Committee freeze procedure, Articles 16 and 18; Decree 2026-117
Notify freezes, releases and attempted transactions.	Notify the National Counter-Terrorism Committee of the value, type, date and time within 24 hours and report measures and attempted transactions through the current procedure.	Notifications, receipts, directions and release decision.	National Counter-Terrorism Committee freeze procedure, Article 19; Decree 2026-117

Records and regulator access

Records must reconstruct customers, ownership, transactions and decisions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain AML records for at least ten years.	Retain accounts, transactions, correspondence, identity copies, CDD and enhanced-diligence files and analyses for at least ten years from the end of the relationship or occasional transaction, using the applicable record-specific clock.	Schedule, archive sample, deletion control and legal-hold log.	Law 2019-017, Article 12(1)-(3)
Reconstruct transactions and provide records diligently.	Preserve sufficient information to reconstruct individual transactions and make controlled records available promptly to competent authorities.	Reconstruction test, retrieval log, request validation and disclosure receipt.	Law 2019-017, Article 12(2)
Apply extensions and holds.	Extend retention when requested by the public prosecutor for an investigation or prosecution and suspend deletion for other valid legal holds.	Request, hold instruction, affected records and release approval.	Law 2019-017, Article 12(4)

Privacy, biometrics, and transfers

AML processing does not displace personal-data obligations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map purpose, legal basis, notice, minimisation, security and retention.	Document each KYC, screening, monitoring, reporting and fraud use; limit access and fields, give applicable information and align deletion with AML holds.	Processing register, notices, access matrix, retention map and security tests.	Law 2017-020, Articles 5-11 and 43-47
Complete APD formalities before processing.	Determine whether declaration, authorisation or an exemption applies; obtain the required receipt or approval before implementation and repeat formalities after material change.	Assessment, filing, receipt or authorisation, exemption rationale and change log.	Law 2017-020, Articles 32-45; APD formalities portal
Obtain prior authorisation for biometric and specified sensitive processing.	Do not deploy biometric, national-identifier, criminal-record or file-interconnection processing until the APD authorisation analysis and required approval are complete.	Data inventory, impact and necessity assessment, APD application and approval.	Law 2017-020, Article 37
Control international transfers and overseas cloud services.	Apply the current APD adequate-country list and obtain prior authorisation where the destination is not listed; separately apply current overseas-cloud conditions.	Transfer map, destination assessment, authorisation, contract and cloud review.	Law 2017-020, Articles 21 and 73; amended APD Decisions 004/2025 and 005/2025

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Keep evidence retrievable, versioned and suitable for supervisory review.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a customer and beneficial-owner evidence pack.	Link identity and KYB evidence, ownership analysis, risk scoring, PEP and sanctions results, approvals, refreshes and exceptions to one auditable record.	Versioned case file with provenance, timestamps and approvals.	Law 2019-017, Articles 6, 9-12
Maintain a reporting and sanctions evidence pack.	Separate restricted FIU reports from ordinary case material while preserving decision chronology, delivery evidence, freeze actions and lawful releases.	Restricted reporting register, receipts, freeze log and access audit.	Law 2019-017, Articles 14-17 and 31; national freeze procedure
Schedule legal and control refreshes.	Monitor official gazettes, FIU, Central Bank, APD, FATF, MENAFATF, UN and sector authorities and retest controls after changes.	Regulatory inventory, alerts, review calendar, test results and remediation.	Law 2019-017, Article 6; current competent-authority publications

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.

Law No. 2019-017 on AML/CFT
National Counter-Terrorism Committee · Primary legislation
Open official source

Official legal-document collection, including Decrees 2019-197 and 2026-115 to 117
Inspection Générale d'État · Official legal repository
Open official source

Targeted-financial-sanctions freeze procedure
National Counter-Terrorism Committee · Official procedure
Open official source

National Counter-Terrorism Committee powers
National Counter-Terrorism Committee · Official procedure
Open official source

Central Bank of Mauritania
Central Bank of Mauritania · Primary regulator
Open official source

Law No. 2017-020 on personal-data protection
Personal Data Protection Authority · Primary legislation
Open official source

Prior declaration and authorisation formalities
Personal Data Protection Authority · Official procedure
Open official source

Amended Decision 004/2025 on international transfers
Personal Data Protection Authority · Regulator decision
Open official source

MENAFATF mutual-evaluation preparatory visit
MENAFATF · FATF-style regional body
Open official source

Jurisdictions under increased monitoring - 19 June 2026
FATF · Authoritative international status
Open official source

High-risk jurisdictions subject to a call for action - 19 June 2026
FATF · Authoritative international status
Open official source

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

Document control

Version 1.0 / Published 6 September 2026 / Last reviewed 6 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 6 September 2026. Confirm the current Financial Intelligence Unit filing route, thresholds established by competent authorities, beneficial-owner filing procedures, sanctions notices, APD formalities and product-specific permissions with the relevant authority and qualified Mauritanian counsel before launch.