VOVE ID

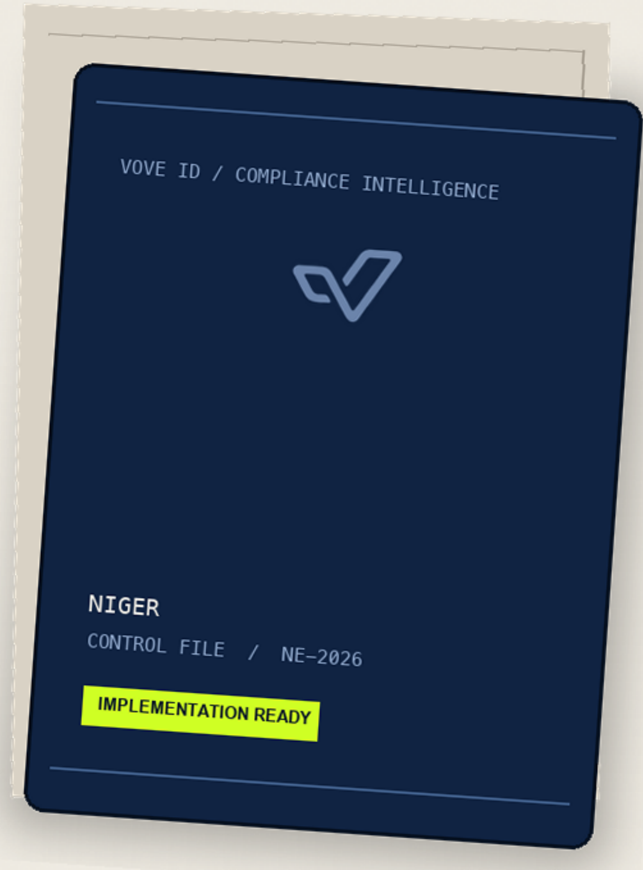
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

NIGER

NIGER / NE



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Niger KYC, KYB & AML Compliance Checklist

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

FIU	**CENTIF Niger**
Primary AML rule	**Ordinance 2024-56 of 19 December 2024**
Suspicion reporting	**Immediately, including attempted transactions**
Cash transaction report	**XOF 15 million or more, including apparently linked operations**
Core AML retention	**10 years under record-specific clocks**
FATF status	**Not named on FATF public lists at 19 June 2026**

Scope and legal framework

Ordinance No. 2024-56 of 19 December 2024 transposes the 2023 UMOA uniform AML/CFT/CPF framework in Niger. Apply it with UMOA Council Decision No. 021 of 21 December 2023, current BCEAO instructions, national implementing measures and Law No. 2022-59 on personal-data protection as subsequently amended.

FATF context

Niger was not named in FATF's high-risk or increased-monitoring statements dated 19 June 2026. Niger remains subject to GIABA enhanced follow-up; GIABA adopted Niger's fourth enhanced follow-up report in November 2025 and published it in 2026. Absence from FATF public lists is not a low-risk finding.

IMPORTANT	General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 7 September 2026. Confirm current CENTIF filing and receipt mechanics, national threshold and sanctions measures, beneficial-owner registry procedures, the competent personal-data authority and transition measures following the June 2026 institutional reorganisation, and product-specific permissions with the competent authority and qualified Nigerien 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/CPF scope.	Map every entity, product, channel, branch, agent and profession to the financial-institution, DNFBP or other covered categories and identify CENTIF and the competent supervisor.	Applicability memo, product map, licences and accountable-owner register.	Ordinance 2024-56, Articles 2-4 and 107
Establish the current CENTIF reporting route.	Designate authorised reporters, obtain the current declaration form or electronic procedure, test secure delivery and preserve acknowledgements.	Appointment, user authority, channel test and receipt log.	Ordinance 2024-56, Articles 60, 64 and 95-103; CENTIF declaration page
Obtain authorisation before regulated activity.	Classify banking, payment, e-money, money-transfer, agent, foreign-exchange, insurance, securities, fintech and virtual-asset activities and obtain every required approval before launch.	Perimeter analysis, licences, conditions and renewal calendar.	Ordinance 2024-56, Articles 2-4 and 58-59; BCEAO Instruction 001-01-2024

Governance and risk assessment

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain internal organisation and controls proportionate to risk.	Approve policies for CDD, beneficial ownership, PEPs, sanctions, monitoring, reporting, records, training and independent testing.	Policy suite, approvals, control library, training and audit reports.	Ordinance 2024-56, Articles 12-14; BCEAO Instruction 001-03-2025
Identify, assess and document ML, TF and PF risks.	Assess customers, geographies, products, transactions, channels, agents and new technologies before launch and on material change.	Risk assessment, methodology, source data, change log and approvals.	Ordinance 2024-56, Article 15
Apply proportionate group and outsourcing controls.	Map group standards, local-law conflicts, outsourced functions, data access and testing while retaining accountability.	Group policy, conflict register, vendor reviews and assurance results.	Ordinance 2024-56, Articles 12-14 and 35-38

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify the customer before a relationship or assisted transaction.	Capture identity attributes, verify reliable independent evidence, understand purpose and intended nature and establish expected activity.	CDD file, source provenance, verification, purpose and risk decision.	Ordinance 2024-56, Articles 16-17
Apply CDD to transfers, suspicion, identity doubt and applicable occasional or linked transactions.	Configure relationship, transfer, cash-aggregation, suspicion and identity-quality triggers; never treat a threshold as a safe harbour.	Trigger matrix, aggregation, alerts and CDD timestamps.	Ordinance 2024-56, Articles 17 and 49; UMOA Decision 021
Control delayed and remote verification.	Permit delay only under the statutory conditions, complete it as soon as possible and before the first transaction, and apply sufficient remote-onboarding safeguards.	Deferral rationale, restrictions, completion time, remote tests and exceptions.	Ordinance 2024-56, Articles 18 and 22

KYB, registries, and beneficial ownership

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence and every representative's authority.	Obtain current RCCM and constitutional evidence, addresses, directors, licences and mandates and reconcile discrepancies.	Registry extract, statutes, managers, licences, mandate and discrepancy log.	Ordinance 2024-56, Articles 17 and 26
Apply the beneficial-owner cascade.	For companies, identify natural persons holding directly or indirectly more than 25% of capital or voting rights, then test control by other means and only then the senior-managing-official fallback.	Ownership chart, control analysis, verified identities and fallback rationale.	Ordinance 2024-56, definitions and Article 26
Identify role holders in trusts and comparable arrangements.	Identify and verify settlor, trustee, protector, beneficiaries or class and every other natural person exercising ultimate control.	Instrument, role register, identity files and control analysis.	Ordinance 2024-56, definitions and Article 26
Keep shareholder and beneficial-owner information accurate and current.	Maintain event-driven updates, reconcile customer declarations with available RCCM and beneficial-owner information and complete filings under the live national procedure.	Registers, update log, filings, supporting documents and discrepancies.	Ordinance 2024-56, Articles 76-79 and 122

5. PEPS, EDD, AND REMOTE ONBOARDING

PEPs, EDD, and remote onboarding

Higher-risk relationships require enhanced, evidenced controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Detect PEP and connected-person exposure.	Screen customers and beneficial owners for foreign, domestic and international-organisation PEP status, family and close associates.	Screening, relationship map, match decision and refresh log.	Ordinance 2024-56, Article 29
Apply approval, source and monitoring controls.	Obtain senior-management approval, establish source of wealth and source of funds and apply enhanced ongoing monitoring where required.	Approval, provenance analysis and monitoring plan.	Ordinance 2024-56, Articles 29-30
Govern third-party reliance.	Assess eligibility, obtain required CDD information immediately, contract for document access and test retrieval; retain ultimate responsibility.	Due diligence, agreement, retrieval test and exceptions.	Ordinance 2024-56, Articles 35-38

Monitoring and suspicious reporting

CENTIF reporting must be immediate, complete and confidential.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor and examine unusual activity.	Scrutinise transactions against the customer profile and document the background and purpose of complex, unusually large or apparently purposeless activity.	Alerts, investigation, written findings and disposition.	Ordinance 2024-56, Articles 19-21
Report suspicion and attempts immediately.	Timestamp when suspicion or reasonable grounds arose and report suspected sums, transactions and attempts to CENTIF using the current route; supplement without delay.	Decision chronology, report, supporting material, delivery and receipt.	Ordinance 2024-56, Article 60
Do not proceed where mandatory CDD fails.	Do not open or execute, or terminate an existing relationship, when required diligence cannot be completed and submit an STR.	Decline or exit decision, investigation and restricted reporting record.	Ordinance 2024-56, Article 25
Prevent tipping off and govern execution holds.	Restrict report access, withhold suspicious activity before reporting unless statutory post-execution conditions apply, and disclose nothing to the customer.	Hold decision, exception rationale, access logs and communications record.	Ordinance 2024-56, Articles 61 and 63

Payments, wires, thresholds, and agents

Keep CDD triggers, special examination and automatic reports distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report cash transactions of XOF 15 million or more.	Aggregate apparently linked operations, configure the exact in-scope entity and transaction logic and obtain current CENTIF submission instructions.	Threshold configuration, tests, reports, receipts and exceptions.	Ordinance 2024-56, Article 72; UMOA Decision 021, Article 8
Apply identification and special-examination thresholds accurately.	For financial institutions, identify multiple daily or unusually frequent cash transactions above XOF 9 million; specially examine cash or bearer-title payments at XOF 50 million or more and unusual or unjustified operations at XOF 10 million or more.	Threshold register, aggregation tests, CDD and examination reports.	Ordinance 2024-56, Articles 17 and 21; UMOA Decision 021, Articles 3-4
Preserve required wire-transfer information.	Carry required originator and beneficiary information throughout the chain and define reject, suspend, execute, investigate and follow-up rules for deficient transfers.	Field matrix, validation, repair queue, samples and decisions.	Ordinance 2024-56, Articles 39-47

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Screen, freeze, restrict and report without delay under current designation procedures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen current authoritative designation lists.	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.	Ordinance 2024-56, Articles 89 and 124
Freeze designated property without delay and prior notice.	Maintain a continuously available path to freeze direct, indirect, owned or controlled assets and prevent funds, services or resources being made available.	Freeze procedure, timestamps, asset record and transaction blocks.	Ordinance 2024-56, Article 89
Report funds, freezes, measures and attempts immediately.	Notify CENTIF and the competent authority through current national procedures and release nothing without lawful authority.	Notifications, receipts, directions and release decision.	Ordinance 2024-56, Articles 90-91

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Records must reconstruct customers, ownership, transactions and decisions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain customer records for 10 years after closure or relationship end.	Map identity, profile and analysis records to the relationship-based clock and apply legal holds.	Schedule, archive sample, deletion control and hold log.	Ordinance 2024-56, Article 23
Retain transaction and correspondence records for 10 years after execution.	Use transaction-based clocks and preserve enough information to reconstruct each operation.	Archive configuration, reconstruction test and retrieval log.	Ordinance 2024-56, Article 23
Make records available to competent authorities.	Authenticate requests, protect STR confidentiality, produce controlled records within the required time and log disclosure and receipt.	Request register, approval, production index and acknowledgement.	Ordinance 2024-56, Articles 24 and 103

Privacy, biometrics, and transfers

AML processing remains subject to Niger's personal-data framework.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map lawful purpose, data, security and regulatory formalities.	Inventory identity, ownership, screening, biometric, monitoring and reporting data; document purpose, basis, recipients, access, retention and the applicable declaration or authorisation route.	Processing register, basis assessment, notices, access matrix and authority record.	Law 2022-59 as amended
Apply heightened controls to sensitive and biometric processing.	Confirm the competent authority and exact current procedure before deploying facial, fingerprint, liveness-template, national-identifier or offence-data processing; minimise data and test security.	Legal assessment, impact review, authority decision, access review and tests.	Law 2022-59 as amended; June 2026 institutional transition
Control cross-border personal-data transfers.	Map hosting, support and vendor destinations, assess safeguards and obtain any required authorisation from the currently competent authority before transfer.	Transfer map, safeguards, contracts, authority record and access logs.	Law 2022-59 as amended, cross-border transfer provisions

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 Ordinance 2024-56, Articles 12-26
Maintain a reconstructable monitoring and reporting pack.	Link transactions, alerts, analysis, approvals, CENTIF reports, delivery evidence and post-filing controls while protecting confidentiality.	Complete sampled case pack and access log.	Operational control supporting Ordinance 2024-56, Articles 19-25 and 60-64
Maintain a launch and change-control pack.	Record licensing, thresholds, sanctions lists, registry and privacy formalities, product risk, testing and authority confirmations before launch and material changes.	Signed launch pack, legal-source register and change approvals.	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.

Ordinance No. 2024-56 of 19 December 2024 - national implementation notice
Office National d'Edition et de Presse · Official state-publisher implementation context
Open official source

2023 UMOA uniform AML/CFT/CPF law
BCEAO · Primary regional legal framework
Open official source

UMOA Decision No. 021 of 21 December 2023 setting implementation thresholds
BCEAO · Primary regional decision
Open official source

BCEAO Instruction No. 001-03-2025 on AML/CFT/CPF organisation and control
BCEAO · Primary regulator instruction
Open official source

BCEAO Instruction No. 003-03-2025 on customer identification and knowledge
BCEAO · Primary regulator instruction
Open official source

BCEAO Instruction No. 001-01-2024 on payment services
BCEAO · Primary regulator instruction
Open official source

Niger AML/CFT institutional framework and CENTIF role
Ministry of Finance, Niger · Official government authority page
Open official source

Consolidated Law No. 2022-59 on personal-data protection
Former HAPDP official legislation repository · Primary privacy legislation
Open official source

Law No. 2022-59 amendments and historical privacy procedures
Former HAPDP official legislation repository · Official legal and procedure archive
Open official source

Niger fourth enhanced follow-up report (2026)
GIABA · Authoritative regional assessment
Open official source

Niger country assessment and follow-up
FATF · Authoritative public statement
Open official source

FATF high-risk and monitored jurisdictions current at 19 June 2026
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 7 September 2026 / Last reviewed 7 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 7 September 2026. Confirm current CENTIF filing and receipt mechanics, national threshold and sanctions measures, beneficial-owner registry procedures, the competent personal-data authority and transition measures following the June 2026 institutional reorganisation, and product-specific permissions with the competent authority and qualified Nigerien counsel before launch.