VOVE ID

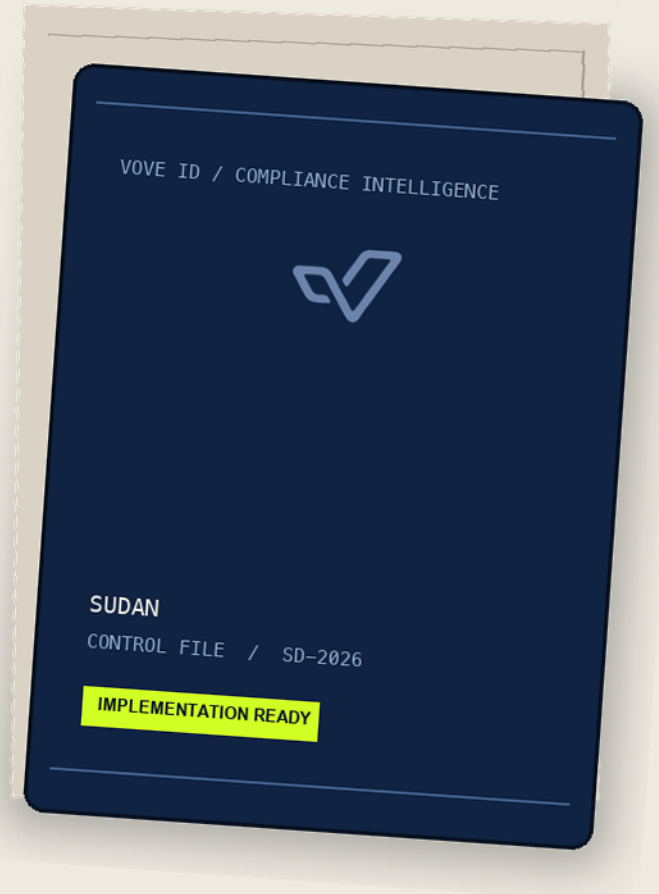
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

SUDAN

SUDAN / SD



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Sudan KYC, KYB & AML Compliance Checklist

An implementation checklist for customer identification, ownership and control, suspicious reporting, records, transfers, sanctions, payments and data safeguards under Sudan's current framework.

FIU	**Financial Information Unit established by Article 12 of the 2014 Act**
Primary AML rule	**AML and Terrorism Financing Act 2014**
CBOS rule	**Circular No. 8/2026, effective 30 April 2026**
CBOS occasional CDD	**EUR 15,000 equivalent, single or linked transactions**
CBOS ownership test	**More than 10%, then other control, then senior manager**
Suspicion reporting	**Immediately, including attempts and regardless of value**
Core retention	**At least 5 years under Article 6 and Circular 8/2026**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Anti-Money Laundering and Terrorism Financing Act 2014 is the core preventive law. For institutions supervised by the Central Bank of Sudan, Circular No. 8/2026 supplies the current detailed AML/CFT/CPF controls and expressly repeals Circular No. 8/2014 and specified later circulars. Companies Act 2015, as amended in 2025, and sector licensing instruments apply separately.

FATF context

Sudan was not named on the FATF call-for-action or increased-monitoring lists dated 19 June 2026. Sudan remains a MENAFATF member; FATF records its last mutual evaluation as 28 November 2012, followed by MENAFATF's April 2016 third follow-up. Absence from a FATF public list does not mean that Sudan, a product or a customer is low risk.

IMPORTANT

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 13 September 2026. Sudan's conflict, institutional relocation and legal transitions can affect practical access and enforcement. Confirm later Gazette amendments, FIU filing mechanics, sector rules, non-bank thresholds, company-register and beneficial-ownership procedures, sanctions-list circulation, privacy and biometric requirements, and product permissions with the competent authority and qualified Sudanese 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 statutory reporting perimeter, sector supervisor and licence before activity.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map every entity and activity to the reporting-person perimeter.	Classify financial activities, real-estate transactions, qualifying precious-metal or stone cash transactions, specified legal and accounting work, and company-service activity; confirm any later ministerial designation and the relevant supervisor.	Entity map, activity analysis, statutory category, supervisor confirmation and legal opinion.	AML and Terrorism Financing Act 2014, Article 3 definitions; Article 4
Apply Circular 8/2026 only to its stated CBOS-supervised perimeter.	For banks, exchange companies, money-transfer companies, leasing, microfinance and other CBOS-licensed financial institutions, implement Circular 8/2026; for other reporting persons obtain their supervisor's current rules rather than extending bank-specific numbers automatically.	Perimeter decision, licence, supervisor rule register and scoped control matrix.	CBOS Circular No. 8/2026, Parts II-III
Obtain each product and channel approval before launch.	Identify banking, foreign exchange, remittance, mobile-payment, payment-system, agent, outsourcing and technology activity and obtain current CBOS or other competent-authority approval before promotion or operation.	Licence, written approval, conditions, agent register, outsourcing approval and renewal calendar.	Banking Business Regulation Act 2026; CBOS electronic-payment notice; Mobile Payment Financial Institutions Regulation 2020

2. GOVERNANCE AND RISK ASSESSMENT

Governance and risk assessment

The Act requires risk controls; Circular 8/2026 adds detailed governance for CBOS-supervised institutions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented institutional risk assessment.	Assess customer, geography, product, service, delivery-channel, transaction, technology and proliferation-financing risks and update the assessment at least twice each year where Circular 8/2026 applies.	Methodology, semiannual assessments, source inputs, board approval and remediation plan.	2014 Act, Article 6(1); CBOS Circular 8/2026, Part IV, paragraphs 1-3
Maintain an independent compliance function.	Appoint a senior compliance manager and deputy with board oversight, access to necessary records, independent decision authority and CBOS approval for transfer or removal where the circular applies.	Appointments, CBOS correspondence, charter, access test, board reporting and conflicts register.	CBOS Circular 8/2026, paragraph 60(b)
Operate tested internal controls and training.	Maintain board-approved customer acceptance, CDD, sanctions, monitoring, reporting, confidentiality, records, group, audit and response procedures; train relevant staff and independently test effectiveness.	Policy suite, training records, monitoring tests, internal and external audit reports and remediation.	2014 Act, Article 6(1); CBOS Circular 8/2026, paragraphs 60-63

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Identify customers, representatives and beneficial owners from reliable independent evidence.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Perform CDD at each statutory trigger.	Identify and verify before a relationship, a covered occasional transaction, a domestic or international wire, when prior data is doubtful, or whenever ML, TF or PF suspicion exists.	Trigger matrix, identity file, verification results, timestamps and exceptions.	2014 Act, Article 5; CBOS Circular 8/2026, paragraph 7
For CBOS institutions, aggregate linked occasional transactions at EUR 15,000 equivalent.	Apply CDD before a single or apparently linked occasional transaction equals or exceeds EUR 15,000 in national or foreign currency; document the rate, aggregation logic and scope. Do not extend this bank-sector trigger to other sectors without authority.	Rate source, aggregation rules, alerts, customer file and scoped legal basis.	CBOS Circular 8/2026, paragraph 7(2)
Verify a natural person using current official evidence.	Obtain valid official identity, full name, nationality, national number, date of birth, permanent residence, contacts, employment or activity, purpose and authorised signers, then corroborate through reliable official databases where available.	Certified identity copy, verification queries, address and contact checks, discrepancy log and approval.	CBOS Circular 8/2026, paragraphs 12-13
Verify every representative and mandate.	Obtain the representative's identity and a valid power or authorisation, test its scope and retain a certified copy before allowing access or instructions.	Representative KYC, power, authority check, limits and transaction log.	2014 Act, Article 5(2); CBOS Circular 8/2026, paragraphs 4(2) and 13(2)
Do not continue when CDD cannot be completed.	Do not open the account, form the relationship or transact; terminate an existing relationship where required and consider an STR. If further CDD would tip off the customer, stop the CDD step and report instead.	Restriction, exit decision, suspicion assessment, approval and any STR receipt.	CBOS Circular 8/2026, paragraphs 9-10

KYB, registries, and beneficial ownership

Verify legal existence, authority, ownership and control; do not confuse customer-level CDD with registry filing.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person identity and authority.	Obtain current incorporation and commercial-register evidence, constitutional documents, address, purpose, directors, owners, authorised signers and sector permissions; reconcile inconsistencies before acceptance.	Registry extract, constitutional pack, officer and owner lists, mandates, licences and discrepancy log.	CBOS Circular 8/2026, paragraph 14; Companies Act 2015 as amended in 2025
Obtain a written beneficial-owner declaration.	At account opening or relationship formation, require the customer to disclose each beneficial owner in writing and corroborate the declaration through reliable independent sources.	Signed declaration, ownership chart, source documents, independent checks and refresh history.	CBOS Circular 8/2026, paragraphs 16-17
For CBOS institutions, identify natural persons owning or controlling more than 10%.	Trace direct and indirect ownership and control above 10%; if no verified owner controls through ownership, identify control by other means; if still unresolved, identify the natural person responsible for senior management.	Layered ownership chart, percentage calculations, control analysis, fallback decision and verified identities.	CBOS Circular 8/2026, paragraph 18(1)
Identify legal-arrangement parties and ultimate controllers.	Identify and verify the settlor or creator, trustee, protector if any, beneficiaries and every other natural person exercising final direct or indirect effective control.	Instrument, party register, verified identities, control analysis and change monitoring.	CBOS Circular 8/2026, paragraphs 15 and 18(3)
Treat commercial-register data as corroboration, not a substitute for CDD.	Use the General Commercial Registrar's current Companies Act process to verify existence and filings, but separately establish beneficial ownership and control; obtain current 2025 amendment and live filing procedures before relying on registry completeness.	Registry evidence, customer declaration, independent corroboration, discrepancy log and legal update check.	Companies Act 2015 as amended in 2025; Ministry of Justice commercial-registration mandate; CBOS Circular 8/2026, paragraphs 16-18

5. PEPS, EDD, AND REMOTE ONBOARDING

PEPs, EDD, and remote onboarding

Use risk systems for public-function exposure and apply proportionate enhanced measures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify PEPs, family members and close associates.	Obtain declarations, check reliable information and databases, map relationships and refresh screening throughout the relationship.	Declaration, screening, relationship map, match rationale and refresh log.	2014 Act, Articles 3 and 6(2); CBOS Circular 8/2026, paragraphs 28-30
Apply approval, source and monitoring measures to foreign PEPs.	Obtain senior-management approval before starting or continuing, establish source of wealth and funds and conduct enhanced ongoing monitoring.	Approval, source analysis, corroboration, monitoring plan and reviews.	2014 Act, Article 6(2); CBOS Circular 8/2026, paragraph 29(a)
Apply the same measures to higher-risk domestic and international-organisation PEPs.	Assess risk and apply senior approval, source verification and enhanced monitoring where the domestic or international-organisation PEP relationship is higher risk.	Risk assessment, approval, source evidence and monitoring results.	2014 Act, Article 6(2); CBOS Circular 8/2026, paragraph 29(b)
Strengthen non-face-to-face verification.	Use authenticated documents, additional identity and source evidence, trustworthy independent references, initial restrictions and enhanced monitoring proportionate to impersonation and fraud risk.	Remote-onboarding design, authentication results, restrictions, liveness or equivalent evidence and monitoring.	CBOS Circular 8/2026, paragraph 22

Monitoring and suspicious reporting

Suspicious transactions and attempts are reported immediately, regardless of value.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor relationships and investigate unusual activity.	Compare transactions and attempts with the customer's identity, purpose, ownership, expected activity, source profile and risk; investigate complex, unusual or economically unclear activity and retain the analysis.	Monitoring rules, alerts, investigation notes, source data and dispositions.	2014 Act, Articles 5-6; CBOS Circular 8/2026, paragraphs 19 and 47-48
Report suspicion and attempts immediately and regardless of value.	Timestamp reasonable suspicion and have the authorised compliance manager immediately submit the FIU form for a transaction or attempted transaction connected with crime proceeds, ML or TF; include PF suspicion under the circular's internal escalation framework.	Suspicion chronology, analysis, FIU form, secure submission record and acknowledgement.	2014 Act, Article 6(1); CBOS Circular 8/2026, paragraphs 49-51
Submit later related information immediately.	Authenticate FIU requests and promptly provide requested or newly available information linked to an earlier report using the authorised secure route.	Request, authority verification, supplement, delivery log and receipt.	2014 Act, Article 14; CBOS Circular 8/2026, paragraphs 55-57
Prevent tipping off and protect reporting information.	Restrict report and investigation access and do not tell the customer or an unauthorised person that a report has been or will be filed; document permitted communications with competent authorities and counsel.	Need-to-know matrix, access logs, communications policy, training and incident review.	2014 Act, Article 9; CBOS Circular 8/2026, paragraphs 58-59
Implement FIU stop and freeze orders exactly.	Maintain an always-available process for an FIU transaction stop of up to five days, a Prosecutor-General freeze of up to two weeks and any court extension; do not release without verified authority.	Order validation, timestamps, restriction, asset record, extension and release authority.	2014 Act, Article 15

Payments, wires, thresholds, and agents

Wire fields and payment permissions are explicit; other thresholds require scoped current instruments.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep required originator and beneficiary information with each wire.	Collect verified originator and beneficiary names, account or unique reference and the other required identifying fields; keep information through the payment chain and block an originating transfer lacking mandatory data.	Field matrix, validation rules, transfer sample, repair queue and decision log.	2014 Act, Article 7; CBOS Circular 8/2026, paragraphs 33-41
Control incomplete incoming and intermediary transfers.	Detect missing fields and apply documented risk rules to execute, reject, suspend, report or seek repair; intermediaries retain technically detached information for at least five years and provide it within one working day on request.	Detection rule, repair request, risk decision, report and retrieval test.	CBOS Circular 8/2026, paragraphs 39-44
Obtain the current cross-border declaration threshold.	Before physical movement of currency or bearer negotiable instruments, confirm the current regulation-set declaration amount and customs procedure; do not substitute the EUR 15,000 bank CDD trigger.	Current regulation, threshold configuration, declaration, source evidence and customs receipt.	2014 Act, Articles 31-32
Obtain approval for electronic-payment systems, outsourcing and connections.	Secure prior written CBOS approval for the payment service, system, outsourcing, agency and technical connection; document current 2026 banking-law and payment-rule applicability.	Approvals, architecture, contracts, licences, agent inventory and test results.	CBOS electronic-payment notice; CBOS Circular 1/2013; Banking Business Regulation Act 2026
Control mobile-payment providers and agents.	Verify the provider's licence, ensure agents follow CDD and customer-data safeguards, notify CBOS of agent changes without undue delay and monitor transactions and complaints.	Licence, agent due diligence, notifications, contracts, CDD samples, monitoring and complaints.	Mobile Payment Financial Institutions Regulation 2020, Articles 15 and 19-34

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Circular 8/2026 requires real-time screening, freezing without delay and immediate reporting for CBOS institutions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen current UN and Technical Committee sanctions lists in real time.	Screen customers, beneficial owners, directors, authorised persons, related parties and transactions against current UN Security Council decisions and Technical Committee lists and test the system periodically.	List inventory, update log, screening configuration, test results, alerts and dispositions.	CBOS Circular 8/2026, paragraph 61(1)-(2)
Freeze covered assets immediately, without delay or prior notice.	Freeze direct and indirect funds and assets owned, controlled, managed or held wholly or partly by a listed person, including persons acting for or under direction, and prevent funds or services being made available.	Match analysis, freeze timestamp, ownership and control analysis, asset inventory and system blocks.	CBOS Circular 8/2026, paragraph 61(3)-(6)
Immediately notify the Technical Committee and FIU.	After freezing, immediately provide the Technical Committee the asset and action details; immediately notify the FIU of listed current or former customers, related persons and attempted transactions involving frozen resources.	Committee report, FIU report, delivery evidence, acknowledgement and chronology.	CBOS Circular 8/2026, paragraph 61(7)-(10)
Govern false positives, exemptions, humanitarian permissions and release.	Compare all identifiers, maintain the restriction while legally required and release or permit activity only under verified Technical Committee or other competent-authority direction, including any applicable UN humanitarian exemption.	Identifier analysis, authority correspondence, licence or exemption, approval and release log.	Council of Ministers Decisions 358-360/2014; current UN Security Council resolutions; controlled legal procedure

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Records must reconstruct decisions and transactions and remain promptly available.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain CDD records for at least five years after exit or the occasional transaction.	Keep identity and beneficial-owner evidence, accounting files and correspondence for at least five years after the relationship ends or the occasional transaction date, applying the longer applicable period.	Retention schedule, trigger dates, archive samples, retrieval test and deletion controls.	2014 Act, Article 6(1); CBOS Circular 8/2026, paragraph 48(1)
Retain transaction, attempt and report records for their correct clocks.	Keep domestic and international transaction and attempt records for at least five years from execution or attempt; keep FIU reports and supporting documents for at least five years from reporting and criminal-case records until final disposal if longer.	Record-class schedule, linked case files, trigger calculation, archive and legal holds.	2014 Act, Article 6(1); CBOS Circular 8/2026, paragraph 48(2)-(5)
Make records promptly available to competent authorities.	Authenticate requests, preserve reporting confidentiality and privilege, produce responsive records promptly and record the exact disclosure and receipt.	Request register, authority check, production index, approval, delivery and receipt.	2014 Act, Articles 4, 6 and 14; CBOS Circular 8/2026, paragraph 48

10. PRIVACY, BIOMETRICS, AND TRANSFERS

Privacy, biometrics, and transfers

No comprehensive generally applicable data-protection statute or independent privacy authority was verified.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map necessity and legal authority for identity processing.	Document the AML, sector, contractual and operational basis for each identity, screening and biometric field; minimize collection, explain use and restrict incompatible reuse.	Data map, legal-basis analysis, notice, field justification, consent where relevant and change log.	Electronic Transactions Act 2007; 2014 Act, Articles 5-6; operational privacy control
Secure customer and transaction information.	Apply access controls, encryption, logging, segregation, backups, incident response and tested vendor safeguards; payment providers must apply the encryption and customer-data controls in their sector rules.	Security standard, access review, encryption evidence, vendor assessment, tests and incident log.	Electronic Transactions Act 2007, Article 28; Mobile Payment Financial Institutions Regulation 2020, Articles 15 and 19
Control biometrics and overseas hosting conservatively.	Before biometric collection or cross-border processing, assess necessity, proportionality, security, vendor access and transfer risk and obtain current local advice; do not claim an unverified breach deadline or regulator approval.	Impact assessment, architecture, contract, security controls, approval and legal update check.	Operational privacy control pending comprehensive legislation

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Maintain concise evidence packs that reproduce decisions and expose legal dependencies.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, authority, KYB, beneficial ownership, screening, risk, approvals, privacy records and exceptions under stable identifiers.	Complete sampled onboarding pack.	Operational control supporting 2014 Act, Articles 5-6 and CBOS Circular 8/2026
Maintain a reconstructable monitoring and reporting pack.	Link transactions, alerts, analysis, immediate-reporting chronology, approvals, submission, acknowledgement, follow-up, sanctions actions and access logs.	Complete sampled case pack and controlled access log.	Operational control supporting 2014 Act, Articles 6, 9 and 14-16
Maintain a launch and legal-change pack.	Record current FIU procedure, sector thresholds, licences, 2026 CBOS controls, registry evidence, sanctions instructions, privacy analysis, conflict-related operating constraints, tests and confirmations before launch and on change.	Signed launch pack, source register, uncertainty log, tests and 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.

Anti-Money Laundering and Terrorism Financing Act 2014
Central Bank of Sudan · Primary legislation
Open official source

AML/CFT/CPF regulatory and supervisory controls - Circular No. 8/2026
Central Bank of Sudan · Official binding circular
Open official source

Laws and regulations repository
Central Bank of Sudan · Official regulator repository
Open official source

Electronic Transactions Act 2007
Central Bank of Sudan · Primary legislation
Open official source

Mobile Payment Financial Institutions Regulation 2020
Central Bank of Sudan · Official regulation
Open official source

Electronic payment system operations - Circular No. 1/2013
Central Bank of Sudan · Official circular
Open official source

Current electronic-payment regulatory clarification
Central Bank of Sudan · Official regulatory statement
Open official source

Companies Act registration mandate and Ministry functions
Ministry of Justice · Official registry authority statement
Open official source

Sudan third follow-up report, April 2016
MENAFATF · Authoritative regional assessment
Open official source

Sudan FATF country page
FATF · Authoritative country record
Open official source

FATF jurisdictions under increased monitoring, 19 June 2026
FATF · Authoritative current status
Open official source

FATF high-risk jurisdictions subject to a call for action, 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 13 September 2026 / Last reviewed 13 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 13 September 2026. Sudan's conflict, institutional relocation and legal transitions can affect practical access and enforcement. Confirm later Gazette amendments, FIU filing mechanics, sector rules, non-bank thresholds, company-register and beneficial-ownership procedures, sanctions-list circulation, privacy and biometric requirements, and product permissions with the competent authority and qualified Sudanese counsel before launch.