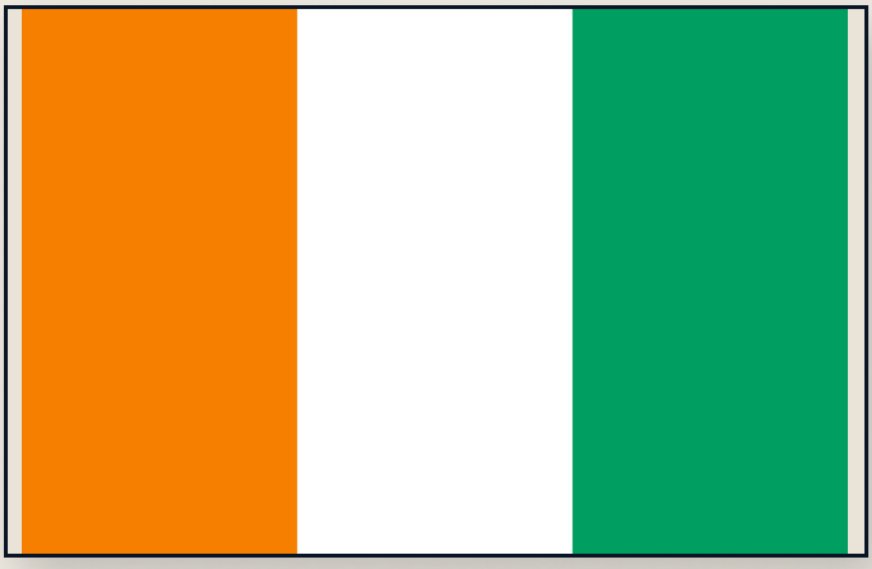
VOVE ID

VOVE COUNTRY CONTROL FILE

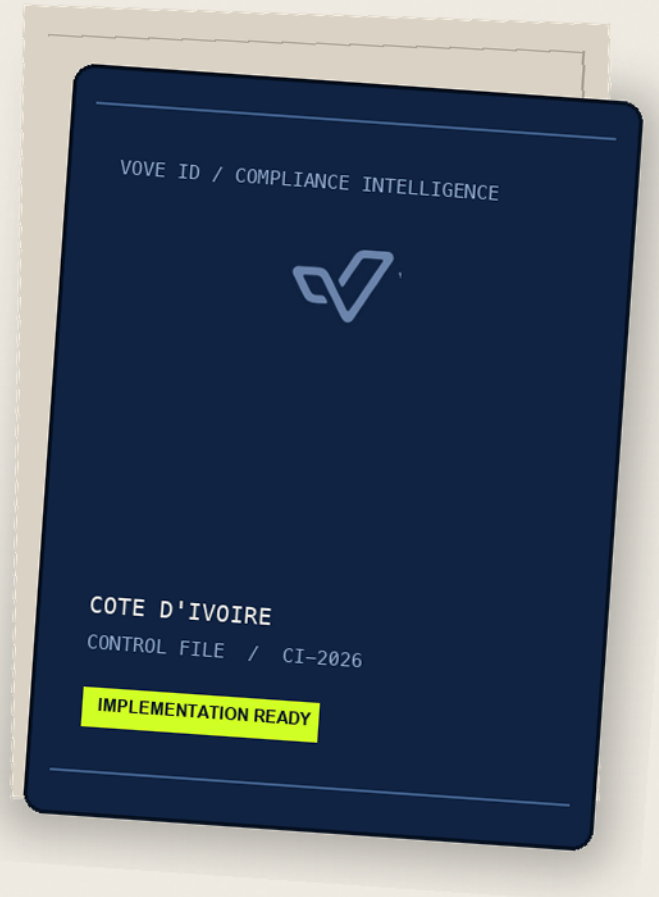
KYC / KYB / AML

2026 EDITION

COTE D'IVOIRE



COTE D'IVOIRE / CI



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Côte d'Ivoire KYC, KYB & AML Compliance Checklist

A practical implementation checklist for fintechs, payment institutions and other reporting persons operating in Côte d'Ivoire. It translates Ordinance No. 2023-875, the 2022-2024 supervision and targeted-financial-sanctions framework, the BCEAO's 2024 payment-services rules and 2025 AML/KYC instructions, beneficial-ownership requirements and ARTCI personal-data rules into operational controls and reviewable evidence.

Financial intelligence unit	**CENTIF-CI**
Current AML law	**Ordinance No. 2023-875 of 23 November 2023**
Suspicion reporting	**Immediately to CENTIF-CI**
Record retention	**10 years**
Payment institutions	**9 authorised in Côte d'Ivoire at 28 February 2026**
FATF public list	**Under increased monitoring as of 19 June 2026**

Scope and legal framework

Ordinance No. 2023-875 of 23 November 2023 on anti-money laundering, counter-terrorist financing and counter-proliferation financing, ratified by Law No. 2024-363 of 11 June 2024; Ordinance No. 2022-237 of 30 March 2022 and implementing Decree No. 2024-58 of 14 February 2024 on administrative sanctions and supervision; Decree No. 2024-216 of 17 April 2024 on targeted financial sanctions as amended by Decree No. 2024-997 of 20 November 2024; Law No. 2024-362 and Decree No. 2024-583 on the beneficial-ownership register; BCEAO Instruction No. 001-01-2024 on payment services, Instruction No. 001-03-2025 on AML/CFT/CPF governance and internal control, and Instruction No. 003-03-2025 on identification, identity verification and customer knowledge; Law No. 2013-450 of 19 June 2013 on personal-data protection and its implementing measures.

FATF context

Côte d'Ivoire was on FATF's list of jurisdictions under increased monitoring on 13 February 2026, commonly called the grey list. FATF expressly stated that increased monitoring does not call for blanket enhanced due diligence or de-risking. On 19 June 2026, Côte d'Ivoire remained on the public list, while FATF made the initial determination that it had substantially completed its action plan and warranted an on-site assessment. Removal is not effective unless and until FATF formally announces it.

IMPORTANT

This checklist is general compliance information, not legal advice. Ordinance No. 2023-875 is the current AML/CFT/CPF baseline; it displaced contrary provisions of former Law No. 2016-992 and this checklist does not use that superseded law as authority. Confirm sector-specific rules, applicable UMOA threshold decisions, reporting forms, supervisory directions and licence conditions directly with CENTIF-CI, the BCEAO, the UMOA Banking Commission, ARTCI and the competent national authority before implementation.

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.

1. SCOPE, AUTHORITIES AND REGULATORY PERIMETER

Scope, authorities and regulatory perimeter

Map every regulated activity, reporting-person category and competent authority before onboarding customers or launching a financial product.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Confirm reporting-person status for every entity and activity	Document whether each entity is a financial institution, fintech, payment institution, electronic-money institution, money-transfer provider, foreign-exchange operator, virtual-asset service provider or designated non-financial business or profession. Apply the AML/CFT/CPF duties to all in-scope activities, including activities performed through mandated intermediaries, agents and distributors.	Legal-perimeter memo, entity chart, product inventory, reporting-person analysis and accountable owner	Ordinance 2023-875, arts. 2-4; BCEAO Instructions 001-03-2025 and 003-03-2025, art. 3
Map each competent regulator and supervisor	Record CENTIF-CI as the financial intelligence unit and identify the sector supervisor for each activity, including the BCEAO and UMOA Banking Commission for relevant financial institutions and payment services and ARTCI for personal-data processing. Apply Ordinance No. 2022-237 only after checking its Article 3 exclusions for specified financial-sector categories; Decree No. 2024-58 designates particular EPNFD (DNFBP), non-profit organisation, manual foreign-exchange and decentralised financial-system supervisors.	Supervisor matrix, Article 3 exclusion analysis, licence register, regulator contacts, filing inventory and escalation route	Ordinance 2023-875, arts. 95-100 and 107; Ordinance 2022-237, art. 3; Decree 2024-58
Obtain the correct financial-services authorisation	Do not treat company registration as permission to provide regulated financial services. Obtain the BCEAO or other competent authorisation for the actual service, verify the authorised scope and conditions, and reconcile the entity against the current official register before launch and periodically thereafter.	Licence or approval, permitted-services schedule, official-register extract, renewal calendar and regulatory correspondence	BCEAO Instruction 001-01-2024, arts. 2, 4 and 17; BCEAO authorised-payment register
Stop unauthorised payment activity	Ensure any structure providing payment services is authorised under Instruction No. 001-01-2024. The BCEAO required non-compliant structures to cease providing payment services from 1 May 2025; do not onboard an unlicensed provider merely because it has a commercial registration or technology contract.	Counterparty licence check, launch gate, provider inventory, cessation controls and legal sign-off	BCEAO Instruction 001-01-2024; BCEAO Notice 004-03-2025
Treat virtual-asset activity as a separately regulated perimeter	Identify any custody, exchange, transfer, issuance support or other virtual-asset service. Obtain the prior approval required by the competent authority and apply the AML/CFT/CPF framework; do not assume a payment or fintech authorisation covers virtual-asset services.	Virtual-asset perimeter analysis, approval, wallet and product map, control assessment and launch decision	Ordinance 2023-875, arts. 58-59

2. GOVERNANCE, RISK AND INDEPENDENT ASSURANCE

Governance, risk and independent assurance

Build a senior-owned, risk-based programme with capable systems, trained staff, independent testing and regulator-ready reporting.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Approve a complete AML/CFT/CPF control framework	Maintain formal, regularly updated policies, procedures and controls covering customer and beneficial-owner identification, risk management, CDD, monitoring, records, internal control, compliance, data protection, recruitment and continuing staff training. Obtain senior-management approval and apply the framework across relevant branches, subsidiaries and agents.	Approved policy suite, regulatory mapping, version history, group standard, local addenda and staff attestations	Ordinance 2023-875, arts. 12-14
Complete and maintain a documented enterprise risk assessment	Assess customer, country, geographic, product, service, transaction and delivery-channel risks, including new products, business practices and technologies before launch. Document inherent risk, control effectiveness, residual risk, mitigation and acceptance, and align the assessment with national and regional risk information.	Risk methodology, data inputs, approved assessment, pre-launch assessments, residual-risk decisions and remediation plan	Ordinance 2023-875, art. 15
Give the AML function authority and independence	Designate the internal AML/CFT/CPF function and its responsible officer, ensure direct access to the deliberative body, operational independence, adequate people and tools, and continuity. Communicate authorised CENTIF declarants and relevant changes to CENTIF-CI and the supervisor without delay.	Appointment, organisation chart, direct-access protocol, resources, deputy arrangements and regulator notifications	Ordinance 2023-875, arts. 12 and 100; BCEAO Instruction 001-03-2025, arts. 4-8
Operate capable monitoring and screening systems	For institutions within the 2025 BCEAO instruction, support customer and account profiling, real-time customer and transaction screening, account-movement monitoring, alert generation, aggregation of all accounts and transactions for the same customer, and detection of unusual or suspicious activity. Incorporate risk-profile changes within one month and targeted-sanctions changes without delay.	System architecture, data lineage, scenario inventory, sanctions-update log, one-month profile-change samples and effectiveness review	BCEAO Instruction 001-03-2025, art. 6
Train annually and audit at least annually	Deliver a documented AML/CFT/CPF training and awareness programme at least annually to relevant staff, governance bodies and mandated intermediaries. Independently audit the programme according to risk and at least once each year; submit findings to the deliberative body and track remediation to verified closure.	Annual curriculum, attendance, effectiveness results, audit plan, report, board review and closure proof	BCEAO Instruction 001-03-2025, arts. 9-11
Submit the annual BCEAO control report on time	Prepare the annual report on the internal AML/CFT/CPF framework, including organisation, resources, training, controls, customer identification, retention, detection, suspicious reporting, weaknesses, statistics, audit conclusions and the next-year plan. Submit it to the BCEAO and competent supervisor within two months after financial year-end.	Approved annual report, data reconciliation, submission receipts and regulator follow-up	BCEAO Instruction 001-03-2025, art. 12

3. CUSTOMER DUE DILIGENCE AND ONBOARDING

Customer due diligence and onboarding

Identify customers, representatives and beneficial owners from reliable independent sources before service and maintain the file throughout the relationship.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify before the relationship	Before establishing a relationship or assisting with a transaction, identify permanent and occasional customers and beneficial owners, verify collected identifiers from reliable and independent documents, data or information, and understand the purpose and intended nature of the relationship.	Identity record, verification response, source provenance, purpose profile, expected activity and reviewer approval	Ordinance 2023-875, arts. 16-17
Apply every statutory CDD trigger	Apply identification and verification at account opening, custody of securities or valuables, safe-deposit allocation, establishment of a business relationship, occasional transactions, domestic or international funds transfers, whenever suspicion exists, for linked manual-exchange or multiple-cash activity when the competent threshold is met, and when a person claims to act for the customer. Configure thresholds only from the current controlling UMOA decisions.	CDD-trigger matrix, linked-transaction logic, threshold source register, completed cases and quality testing	Ordinance 2023-875, art. 17; UMOA Decisions 021/21/12/2023 and 003/28/03/2024
Collect the BCEAO-prescribed individual identifiers	For an individual, collect name, given names, date and place of birth, nationality, home address and identity-document number. Verify against a valid official photographic identity document, using a combination of official documents where necessary, and use sufficiently recent address evidence under the BCEAO instruction.	Identity fields, valid document image, authenticity result, address evidence, expiry control and exception decision	BCEAO Instruction 003-03-2025, arts. 5-6
Verify authority to act	Identify and verify any representative as a customer and obtain certified evidence of the mandate. Confirm that the proposed relationship and transactions are within the representative's delegated powers and screen both representative and principal.	Representative identity, certified mandate, power comparison, principal record and screening results	Ordinance 2023-875, art. 17(j); BCEAO Instruction 003-03-2025, art. 11
Use deferred verification only within the narrow exception	Complete verification before the relationship, throughout it and at the occasional transaction. Defer completion only when it is completed as soon as possible and no later than before the first transaction, is essential not to interrupt normal business and the risks are effectively managed; adopt specific controls for any access before verification.	Deferral rationale, approval, product restrictions, completion deadline, verification timestamp and overdue block	Ordinance 2023-875, art. 18
Reject or exit when CDD cannot be completed	If required CDD cannot be completed, do not open the account, refuse the occasional transaction or terminate the existing relationship, as applicable, and file a suspicious transaction report concerning the customer. If completing CDD would alert a suspected customer, the ordinance permits stopping those CDD steps and requires a report to CENTIF-CI.	Rejected or exited case, reason, account restrictions, STR decision, filing receipt and non-tipping-off controls	Ordinance 2023-875, art. 25

4. KYB AND BENEFICIAL OWNERSHIP

KYB and beneficial ownership

Verify legal existence and authority, trace ultimate natural-person ownership and control, and reconcile customer evidence with the official beneficial-ownership register.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person identity and operating reality	Collect and independently verify legal name, legal form, constitutional documents, registered and principal business address, directors, shareholders or members, relevant managers, registration, tax identifiers, licences and authorised representatives. Compare registry information with the entity's actual business, website, accounts and transaction footprint.	Recent registry extract, constitutional documents, director and shareholder lists, licence checks, operating evidence and discrepancy log	Ordinance 2023-875, art. 26; BCEAO Instruction 003-03-2025, arts. 7-8
Apply the natural-person ownership and control cascade	Identify and reasonably verify the natural persons who ultimately hold a controlling ownership interest. If ownership does not reveal the beneficial owner or creates doubt, identify control by other means; only when no natural person is identified through either step, record the relevant senior managing official as the statutory fallback and document why.	Ownership chart to natural persons, control analysis, identity verification, fallback rationale and compliance approval	Ordinance 2023-875, art. 26
Apply the current more-than-25% operational definition correctly	For institutions subject to BCEAO Instruction No. 003-03-2025, identify natural persons who directly or indirectly hold more than 25% of a company's capital or voting rights, or more than 25% of interests in a collective-investment structure, together with the instruction's other-control and legal-arrangement tests. Do not use the percentage as a safe harbour where another person exercises ultimate control; preserve the ownership, other-control and senior-managing-official cascade.	Capital and voting analysis, more-than-25% test, collective-investment analysis, other-control assessment, legal-arrangement analysis and sign-off	BCEAO Instruction 003-03-2025, art. 2
Identify every relevant legal-arrangement party	For a trust or comparable legal arrangement, identify and verify the settlor, trustee, protector where applicable, beneficiaries or class of beneficiaries and every other natural person exercising ultimate effective control, including through a chain of ownership or control.	Trust deed or equivalent, party register, identity verification, control map and beneficiary-class record	Ordinance 2023-875, art. 26; BCEAO Instruction 003-03-2025, arts. 9-10
Reconcile the customer file with the beneficial-ownership register	Maintain an internal beneficial-owner file with names, ownership, voting and control percentages. Check the official register, notify its competent authority of a divergence or reasonable doubt, and use other reliable risk-based means if the register cannot verify the customer's list. Treat registry data as evidence, not as a substitute for analysis.	Internal BO file, register extract, reconciliation, divergence notification, alternate-source checks and resolution	BCEAO Instruction 003-03-2025, art. 12; Law 2024-362; Decree 2024-583
Keep corporate and ownership information accurate and retrievable	Ensure legal persons maintain accurate, current basic and beneficial-ownership information and controls against misuse of bearer and nominee arrangements. Preserve the required ownership information for at least ten years following dissolution or the end of the relevant professional relationship.	Corporate register, change triggers, periodic review, nominee declarations, dissolution archive and retrieval test	Ordinance 2023-875, arts. 76-83

5. REMOTE ONBOARDING AND IDENTITY TECHNOLOGY

Remote onboarding and identity technology

Make non-face-to-face onboarding demonstrably reliable, risk-assessed and compliant with both BCEAO identity rules and ARTCI data requirements.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Use reliable electronic-identification schemes	For a customer not physically present or represented, use reliable electronic-identification schemes and means under the institution's responsibility while preserving the identification and verification requirements applicable to that customer type.	Scheme assessment, vendor due diligence, assurance mapping, verification output, exceptions and approval	Ordinance 2023-875, art. 22; BCEAO Instruction 003-03-2025, art. 13
Document the full remote-onboarding control design	Maintain a detailed customer journey, reliability measures, authentication and retention procedures, cybersecurity and personal-data compliance, and an internal-control gate ensuring the first transaction occurs only after verification of the customer and, where applicable, the beneficial owner.	Journey map, control specification, first-transaction gate test, security review, privacy approval and retention design	BCEAO Instruction 003-03-2025, art. 14
Risk-assess the remote channel before and during use	Assess the channel's ML/TF/PF, impersonation, document, synthetic-identity, account-takeover and wider operational risks before deployment and after material change. Define human-review levels for categories of legal persons and retain all KYB information required by the instruction.	Channel risk assessment, legal-person typology, human-review matrix, change review and control testing	BCEAO Instruction 003-03-2025, arts. 15-16
Match the person to the identity evidence	Ensure the technology compares the customer's physical characteristics with the submitted identity evidence. Where biometrics are used, ensure they can be linked unambiguously to the customer and apply presentation-attack, duplicate and exception controls proportionate to risk.	Face or biometric match result, liveness or equivalent test, duplicate check, thresholds, manual review and QA	BCEAO Instruction 003-03-2025, art. 17
Route ambiguous remote evidence to in-person verification	Where identification evidence is insufficient, ambiguous or uncertain and affects reliability, stop remote completion and route the customer to physical verification. Do not override this rule merely to preserve conversion.	Quality rules, failed cases, in-person referral, completion evidence, override prohibition and monitoring	BCEAO Instruction 003-03-2025, art. 18
Obtain ARTCI authorisation before biometric processing	Treat facial, fingerprint, voice or other biometric identity processing as sensitive and obtain the required prior authorisation from ARTCI before production use. Align the authorised purpose, dataset, retention, processors and transfers with the deployed workflow.	ARTCI authorisation, approved processing description, biometric data map, vendor contract, retention and deletion test	Law 2013-450, art. 7; ARTCI biometric-processing guidance

6. CUSTOMER RISK, PEPS AND ENHANCED DUE DILIGENCE

Customer risk, PEPs and enhanced due diligence

Use documented risk classification to drive approvals, information depth, monitoring and review frequency without indiscriminate exclusion.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply enhanced controls to politically exposed persons	Use systems and current authoritative lists to identify domestic, foreign and international-organisation PEPs, their family members and close associates. Under Article 29 of Ordinance No. 2023-875, obtain executive approval before establishing or continuing the relationship, establish source of wealth and source of funds, apply enhanced ongoing monitoring, and reassess every PEP customer's profile every three years. Apply periodic and event-driven CDD updates as additional controls, including the sector controls required by BCEAO Instructions No. 001-03-2025 and No. 003-03-2025.	PEP and associate screening, list-validation record, executive approval, source-of-wealth and source-of-funds evidence, enhanced-monitoring review, documented three-year profile reassessment under Ordinance Article 29, and additional periodic or event-driven CDD refresh under applicable BCEAO sector controls	Ordinance 2023-875, art. 29; BCEAO Instructions 001-03-2025 and 003-03-2025
Apply enhanced or simplified measures only on evidence	Apply enhanced diligence where risk is higher and preserve written results. Use simplified measures only where a documented lower-risk assessment supports them; stop simplification whenever suspicion or a specific higher-risk condition exists.	Risk decision, EDD or SDD checklist, corroborating records, written outcome, approval and monitoring	Ordinance 2023-875, arts. 84-85
Use FATF status as a risk input, not an automatic exit rule	Record Côte d'Ivoire's increased-monitoring status in country and institutional risk assessments and track FATF updates. Do not interpret grey-list status as a FATF call for blanket EDD, automatic rejection or de-risking; apply proportionate controls based on actual customer and transaction risk.	Country-risk entry, dated FATF source, customer-specific assessment, proportionality rationale and update log	FATF Increased Monitoring statements, 13 February and 19 June 2026; Ordinance 2023-875, arts. 15 and 30
Control correspondent and shell-bank exposure	Before a cross-border correspondent relationship, understand the respondent's business, reputation, supervision and AML controls, obtain prior senior approval, define responsibilities in writing and test any payable-through access. Do not establish or maintain relationships with shell banks or respondents permitting shell-bank use.	Correspondent questionnaire, public checks, control assessment, approval, agreement and shell-bank attestation	Ordinance 2023-875, arts. 31-32; BCEAO Instruction 001-03-2025, art. 13

7. ONGOING MONITORING, UNUSUAL ACTIVITY AND TRANSFERS

Ongoing monitoring, unusual activity and transfers

Keep profiles current, monitor actual activity against expected behaviour and preserve complete payment-chain information.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor the relationship continuously	Scrutinise transactions throughout the relationship to ensure consistency with the customer's identity, business, risk profile, source of funds and expected activity. Keep customer and beneficial-owner information current whenever prior information is no longer accurate or relevant.	Customer profile, monitoring coverage, alert cases, trigger reviews, refreshed CDD and quality testing	Ordinance 2023-875, arts. 16 and 19-20
Investigate complex, unusual and apparently purposeless activity	Specially examine unusually complex, high-value or otherwise atypical operations and cash or bearer-instrument activity meeting the competent threshold. Establish origin and destination of funds, transaction purpose and beneficial owners; prepare a confidential written report and retain it for ten years.	Alert, customer inquiry, corroborating evidence, written analysis, disposition and retention record	Ordinance 2023-875, arts. 21 and 23
Aggregate related cash activity without inventing thresholds	Detect single and linked cash transactions for the reports required by Article 72 and apply enhanced attention to unusual or activity-inconsistent deposits. Configure monetary values and comparison operators only from current competent-authority decisions and preserve the source and effective date in the rules register.	Linked-transaction logic, threshold register, rule tests, cash reports, unusual-deposit cases and filing receipts	Ordinance 2023-875, art. 72; UMOA Decisions 021/21/12/2023 and 003/28/03/2024
Carry complete originator and beneficiary information	For domestic and cross-border wire transfers, collect, verify where required, transmit and retain the prescribed originator and beneficiary information. Apply ordering, intermediary and beneficiary-institution controls for missing or incomplete data and decide whether to execute, reject, suspend, monitor or report.	Payment-message specification, validation rules, role matrix, sample transfers, repair and reject queue and STR decisions	Ordinance 2023-875, arts. 39-47
Control agents, distributors and outsourced monitoring	Apply the programme to operations performed under the institution's responsibility by mandated intermediaries, transfer sub-agents, foreign-exchange sub-delegates and electronic-money distributors. Contract for CDD, screening, records, training, audit and incident rights and monitor effective performance.	Agent and provider register, due diligence, contract, training, monitoring results, issues and termination controls	Ordinance 2023-875, arts. 12-14 and 33; BCEAO Instructions 001-03-2025 and 003-03-2025, art. 3

8. SUSPICIOUS TRANSACTION REPORTING AND CONFIDENTIALITY

Suspicious transaction reporting and confidentiality

Escalate and report suspicion immediately, preserve the pre-transaction rule and prevent tipping off.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report suspicion immediately to CENTIF-CI	Immediately report funds recorded in the books and completed or attempted operations where there is suspicion or reasonable grounds to suspect ML, TF, PF or a predicate offence. Apply the rule regardless of amount and include tax-fraud suspicion where the regulatory criterion is present.	Case chronology, suspicion rationale, report, immediate-submission timestamp and CENTIF receipt	Ordinance 2023-875, art. 60
Report unresolved identity doubt and supplements	Report any operation where the originator, beneficial owner, trust settlor or equivalent asset-arrangement party remains doubtful after diligence. Send without delay any information that negates, reinforces or modifies an earlier report.	CDD investigation, unresolved-doubt decision, initial report, supplemental report and timestamps	Ordinance 2023-875, art. 60
Report before executing where possible	Refrain from executing suspect operations until the report has been made. If an operation was already executed because delay was impossible, would have frustrated an investigation or suspicion arose only afterward, inform CENTIF-CI without delay and preserve the reason execution occurred.	Hold decision, filing timestamp, execution chronology, exception rationale and post-execution notice	Ordinance 2023-875, art. 61
Protect report confidentiality and prevent tipping off	Restrict access to suspicious transaction reports, related analysis and CENTIF follow-up. Do not tell the customer, transaction owner or unauthorised third party that a report exists, what it contains or what action followed; train customer-facing staff on safe communications.	Access controls, need-to-know list, communication scripts, training, audit logs and incident response	Ordinance 2023-875, art. 63
Operationalise CENTIF opposition orders	Capture the declared execution deadline and ensure operations can be stopped when CENTIF-CI issues a written opposition. Maintain the hold for the statutory period of no more than four days and implement only a competent judicial extension or provisional seizure; do not release early without authority.	Opposition order, hold timestamp, four-day calculation, judicial decision, release approval and audit trail	Ordinance 2023-875, arts. 64-65
Keep the authorised declarant function continuously available	Notify CENTIF-CI and the supervisor of the identity and role of authorised declarants and changes without delay. Separate the declarant role from the director-general role, preserve emergency escalation and ensure the function can answer CENTIF requests within required deadlines.	Declarant appointment, regulator notifications, incompatibility check, deputy coverage, request log and response evidence	Ordinance 2023-875, art. 100

9. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Screen current UN and national designations, freeze immediately without notice and report assets, attempted transactions and implementation measures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a without-delay sanctions operating model	Maintain documented organisation and procedures to implement asset freezes and prohibitions on making funds, property or other economic resources available or usable without delay, including across group entities where applicable.	TFS policy, authoritative-list inventory, roles, decision tree, group deployment and simulation results	Ordinance 2023-875, art. 89; Decree 2024-216 as amended by Decree 2024-997
Apply UN and national designations on the correct legal basis	Subscribe to the official CENTIF-CI and competent-authority distribution channels. Treat relevant UN Security Council designations as immediately applicable under the amended decree and implement national administrative-freeze decisions ordered by the Minister responsible for Finance.	Subscription, designation source, receipt timestamp, legal-basis record, list update and screening completion	Ordinance 2023-875, art. 124; Decree 2024-216 as amended by Decree 2024-997
Freeze immediately and without prior notice	Immediately freeze funds, property and other economic resources belonging to designated persons and entities upon official notification, without informing the holder in advance. Include directly or indirectly owned or controlled assets and assets of persons acting on behalf of or at the direction of designated parties as required by the amended framework.	Match analysis, ownership and control map, freeze timestamp, asset inventory, no-notice record and approval	Ordinance 2023-875, art. 89; Decree 2024-216 as amended by Decree 2024-997
Prohibit availability, use and circumvention	Prevent direct or indirect availability or use of frozen assets for designated persons, controlled entities, agents or instructed parties, and prevent transactions designed to evade or circumvent the measure. Continue the freeze until a competent delisting, release or other lawful decision applies.	Payment blocks, connected-party analysis, circumvention scenarios, continuing-freeze review and release authority	Ordinance 2023-875, art. 89; Decree 2024-216 as amended by Decree 2024-997
Report frozen assets, matches and attempted transactions	Immediately notify CENTIF-CI of funds linked to listed TF or PF persons, entities and associated terrorists. Report to the competent authority all frozen assets and measures taken under UN prohibitions, including attempted transactions, and suspend any customer order benefiting a frozen target while informing the authority without delay.	CENTIF notice, competent-authority report, frozen-asset schedule, attempted-transaction report, suspended order and timestamps	Ordinance 2023-875, arts. 90-91; Decree 2024-216 as amended by Decree 2024-997

10. PAYMENT-SERVICE COMPLIANCE

Payment-service compliance

Overlay the national AML framework with the BCEAO's authorisation, governance, safeguarding and operational requirements for UMOA payment services.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Classify every payment service under Article 4	Map account operation, cash placement or withdrawal, payment execution, payment-instrument issuance or acquisition, money remittance, payment initiation and account-information functionality to the service categories in the instruction. Confirm which entity performs each regulated role.	Product-to-service map, funds-flow diagram, role allocation, legal opinion and authorised-scope comparison	BCEAO Instruction 001-01-2024, arts. 2-4
Meet legal-form and establishment requirements	Ensure an applicant payment institution uses a permitted legal form and has its registered office in an UMOA member state. Align governance, shareholding, management, operational programme and controls with the authorisation dossier and notify material changes as required.	Constitutional documents, registered-office proof, ownership file, governance records, application and change log	BCEAO Instruction 001-01-2024, arts. 13-17
Operate payment governance and risk controls	Maintain governance, internal control, risk and security management, personal-data protection, incident handling and customer-complaint arrangements proportionate to the services. Integrate AML ownership, monitoring, sanctions and reporting into those arrangements rather than treating them as a separate paper policy.	Governance framework, control map, risk register, security and privacy assessments, incident log and complaints register	BCEAO Instruction 001-01-2024, art. 16; BCEAO Instruction 001-03-2025, arts. 4-12
Safeguard customer funds	Identify all funds received from payment-service users or through another provider and apply the instruction's separation and safeguarding requirements. Reconcile protected balances, settlement accounts and user liabilities and prevent use for the institution's own account.	Safeguarding structure, designated accounts, daily reconciliation, exception log, insolvency analysis and management review	BCEAO Instruction 001-01-2024, art. 48
Verify counterparties against the current register	Before partnering with a payment institution, verify its name, jurisdiction and authorisation against the latest BCEAO register. As of 28 February 2026, the BCEAO reported nine authorised payment institutions in Côte d'Ivoire; treat the count as dated information and verify the named entity, not only the total.	Dated register extract, entity match, permitted-services check, periodic rescreening and discrepancy escalation	BCEAO list of authorised payment institutions in the UMOA, 28 February 2026

11. RECORDS, PRIVACY AND REGULATORY READINESS

Records, privacy and regulatory readiness

Preserve reconstructable ten-year evidence while meeting ARTCI formalities, purpose, rights, security and transfer controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain AML and transaction evidence for ten years	Keep customer identity, customer knowledge, risk profile, CDD analyses and other relevant information for ten years after account closure or the end of the permanent or occasional relationship. Keep transaction records, account books and business correspondence for ten years after execution and ensure individual transactions can be reconstructed.	Retention schedule, immutable archive, relationship-end triggers, transaction samples, retrieval test and deletion controls	Ordinance 2023-875, arts. 23-24
Complete the correct ARTCI prior formality	Inventory every personal-data processing activity and determine whether it requires declaration, prior authorisation or another ARTCI formality before use. Obtain ARTCI prior authorisation for biometric processing under Article 7 and for other processing where the law requires it, and keep the authorised purpose and design aligned with production.	Processing inventory, formality assessment, declaration or authorisation, change review and ARTCI correspondence	Law 2013-450, art. 7; Decree 2015-79; ARTCI biometric guidance
Process lawfully, fairly and for defined purposes	Define the legal basis and explicit legitimate purposes for KYC, screening, monitoring, fraud and reporting data; collect only adequate and relevant data, maintain accuracy, provide required notices and do not repurpose or retain identifiable data incompatibly with the declared purpose.	Lawful-basis register, privacy notices, purpose map, minimisation review, accuracy controls and retention rationale	Law 2013-450, arts. 15-18
Enable data-subject rights without compromising AML law	Provide operational channels for information, access, rectification, update, opposition and other applicable rights. Document any restriction required to protect suspicious-report confidentiality, sanctions implementation, investigations or another legal obligation rather than disclosing protected compliance activity.	Rights procedure, request log, identity checks, response records, exemption rationale and legal review	Law 2013-450, arts. 28-36; Ordinance 2023-875, art. 63
Secure data and govern processors	Apply technical and organisational measures appropriate to identity, biometric, financial and screening data so records are not altered, damaged or accessed by unauthorised persons. Contractually limit processors, control access, encrypt sensitive data, test recovery and deletion, and document incidents and remediation.	Security risk assessment, access review, encryption evidence, processor agreement, test results, incident log and remediation	Law 2013-450, arts. 39-41
Control interconnection and cross-border transfers	Map every API, shared database, cloud region and overseas support access. Obtain ARTCI authorisation where interconnection or transfer requires it, document destination safeguards and recipients, and ensure transfers remain within the notified or authorised purpose and security design.	Data-flow map, interconnection approval, transfer authorisation, destination assessment, contracts and transfer register	Law 2013-450, arts. 14 and 26-27
Maintain annual privacy accountability evidence	Where the statutory controller and correspondent reporting duties apply, prepare the annual compliance report and submit it to ARTCI. Keep a personal-data protection correspondent with appropriate independence and records of advice, controls and escalations.	Correspondent appointment, annual report, submission receipt, activity log, findings and remediation	Law 2013-450, arts. 41-42

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Stay inspection- and sanction-ready	Maintain a single evidence index connecting each legal duty to policy, owner, system control, sample, issue and remediation. Support on-site and off-site supervision and respond fully to lawful requests. Before applying the 2022 administrative-sanctions regime, check the exclusions for specified financial-sector categories in Article 3; Decree No. 2024-58 designates particular EPNFD (DNFBP), non-profit organisation, manual foreign-exchange and decentralised financial-system supervisors.	Obligations register, Article 3 exclusion analysis, evidence library, inspection protocol, request log, issue register and closure proof	Ordinance 2022-237, art. 3; Decree 2024-58; Ordinance 2023-875, arts. 107 and 113

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. 2023-875 of 23 November 2023 on AML/CFT/CPF
CENTIF-CI · primary
Open official source

Côte d'Ivoire AML/CFT/CPF legislation and regulation portal
CENTIF-CI · primary
Open official source

Ordinance No. 2022-237 on administrative sanctions and supervision
CENTIF-CI · primary
Open official source

Decree No. 2024-58 implementing Ordinance No. 2022-237
CENTIF-CI · primary
Open official source

Decree No. 2024-216 on targeted financial sanctions
CENTIF-CI · primary
Open official source

Decree No. 2024-997 amending Decree No. 2024-216
CENTIF-CI · primary
Open official source

Official targeted-financial-sanctions lists and customer check
CENTIF-CI · primary
Open official source

Law No. 2024-362 establishing the beneficial-ownership register
CENTIF-CI · primary
Open official source

Decree No. 2024-583 on access to beneficial-ownership information
CENTIF-CI · primary
Open official source

UMOA Decision No. 021 of 21 December 2023 on AML/CFT/CPF thresholds
BCEAO · primary
Open official source

UMOA Decision No. 003 of 28 March 2024 on complementary thresholds
BCEAO · primary
Open official source

BCEAO Instruction No. 001-01-2024 on payment services in the UMOA
BCEAO · primary
Open official source

BCEAO Notice No. 004-03-2025 ending the payment-services transition
BCEAO · primary
Open official source

BCEAO Instruction No. 001-03-2025 on AML/CFT/CPF organisation, internal control and compliance
BCEAO · primary
Open official source

BCEAO Instruction No. 003-03-2025 on customer identification, verification and knowledge
BCEAO · primary
Open official source

Authorised payment institutions in the UMOA at 28 February 2026
BCEAO · primary
Open official source

Law No. 2013-450 of 19 June 2013 on personal-data protection
ARTCI · primary
Open official source

ARTCI biometric-processing guidance
ARTCI · primary
Open official source

ARTCI personal-data protection decisions
ARTCI · primary
Open official source

FATF jurisdictions under increased monitoring, 13 February 2026
FATF · primary
Open official source

FATF jurisdictions under increased monitoring, 19 June 2026
FATF · primary
Open official source

KYC and AML Compliance in Ivory Coast 2026
VOVE ID · contextual
Open contextual guide

Document control

Version 1.3 / Published 15 July 2026 / Last reviewed 15 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general compliance information, not legal advice. Ordinance No. 2023-875 is the current AML/CFT/CPF baseline; it displaced contrary provisions of former Law No. 2016-992 and this checklist does not use that superseded law as authority. Confirm sector-specific rules, applicable UMOA threshold decisions, reporting forms, supervisory directions and licence conditions directly with CENTIF-CI, the BCEAO, the UMOA Banking Commission, ARTCI and the competent national authority before implementation.