VOVE ID

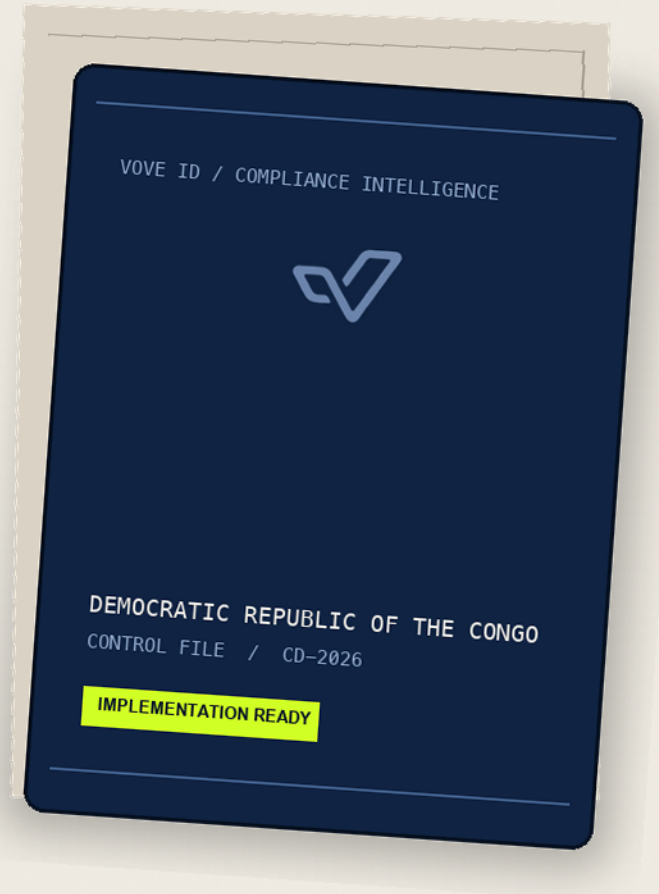
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

DEMOCRATIC REPUBLIC OF THE CONGO

DEMOCRATIC REPUBLIC OF THE CONGO / CD



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Democratic Republic of the Congo KYC, KYB, AML, CFT, CPF and Data Protection Compliance Checklist 2026

A source-backed 2026 implementation dataset for customer and business verification in the Democratic Republic of the Congo. It incorporates Law No. 22/068, BCC Instruction No. 15 modification No. 3, the statutory beneficial-owner regime and its pending central register, CENAREF reporting, CONASAFIC sanctions procedures, payment and transfer controls and the Digital Code's personal-data rules.

Primary AML/CFT/CPF law	**Law No. 22/068 of 27 December 2022**
Financial intelligence unit	**Cellule nationale des renseignements financiers (CENAREF)**
STR timing	**Without delay once knowledge, suspicion or reasonable grounds exist; attempted transactions are included**
STR method	**Written, digital, electronic or telephone submission to CENAREF; telephone reports require prompt written confirmation**
Core AML retention	**10 years from relationship end or transaction execution, by record class; specified intermediary wire data at least 5 years**
Beneficial-owner test	**More than 25% direct or indirect ownership or voting rights, other control, then the statutory management or legal-representative fallback**
Central BO register	**Required by Law No. 22/068 but the implementing Justice Ministry order was still a draft in April 2026**
BCC occasional CDD trigger	**Above USD 15,000 for the transactions and institutions covered by Instruction No. 15 modification No. 3, including linked transactions**
Cash and bearer instruments	**USD 10,000 equivalent statutory restriction, subject to stated exceptions and BCC derogations**
Cross-border cash declaration	**USD 10,000 equivalent or more on entry to or exit from the DRC**
Targeted sanctions	**Use CONASAFIC/Sentinelle and current UN and national lists; freeze without delay and without prior notice**
FATF status	**Substantially completed action plan in June 2026; still under increased monitoring pending on-site assessment**

Scope and legal framework

Law No. 22/068 of 27 December 2022 is the principal cross-sector AML/CFT/CPF statute. BCC Instruction No. 15 modification No. 3 adds operational rules for the financial intermediaries within its scope, while Instruction No. 15 bis modification No. 4 addresses derogations from the statutory USD 10,000 cash and bearer-instrument restriction. Law No. 22/069 and BCC payment instruments govern regulated financial and payment activity. Decrees Nos. 24/24 and 24/25, implementing orders and CONASAFIC procedures govern targeted financial sanctions. Personal data are governed by Ordinance-Law No. 23/010 of 13 March 2023 establishing the Digital Code.

FATF context

As at 16 July 2026, the Democratic Republic of the Congo remained under FATF increased monitoring pending an on-site assessment. On 19 June 2026 FATF made the initial determination that the DRC had substantially completed its action plan, citing the national risk assessment and strategy, risk-based supervision, FIU capacity, investigation and prosecution capacity and effective TF/PF targeted-financial-sanctions implementation. FATF stated that the on-site assessment would depend on the public-health situation. Increased monitoring is a country-risk input; FATF expressly does not call for blanket enhanced due diligence or de-risking solely because a jurisdiction is listed.

IMPORTANT

This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 16 July 2026. Confirm current gazetted law, sector rules, thresholds, filing mechanics and supervisor expectations with Congolese counsel and the competent authority before launch. The statutory beneficial-owner register and the APD's operating procedures were not confirmed as fully operational public filing routes at the review date. VOVE ID can support evidence collection, screening and audit trails, but the reporting entity remains responsible for risk decisions, customer acceptance, reports, freezes and regulatory compliance.

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 regulated activities

Begin with the legal entity, activity and supervisor perimeter. The 2022 statute is broad; BCC instructions and other sector instruments apply only within their stated scopes.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Law No. 22/068 applies broadly and identifies financial institutions and specified non-financial businesses and professions, including casinos, real-estate agents, precious-metals and stones dealers, accountants, lawyers, notaries and bailiffs.	Map every entity, product, profession and customer-facing activity to the statutory reporting-person category and competent supervisor before configuring controls.	Signed perimeter memorandum, entity-product matrix, licence records and supervisor map.	Law No. 22/068, arts. 2-3
CENAREF is the financial-intelligence unit and recipient of suspicious transaction reports. BCC supervises regulated financial intermediaries and issues operational AML/CFT/CPF instructions for its sectors.	Assign authority contacts, reporting ownership, BCC reporting obligations and escalation coverage, with controlled credentials and alternates.	Authority map, appointments, CENAREF procedure, BCC reporting calendar and access register.	Law No. 22/068, arts. 92-113; BCC Instruction No. 15 modification No. 3
Professional funds or value transfer and transport activity requires BCC approval, and payment, e-money, card and connected-service activity is subject to the applicable BCC licensing or authorisation perimeter.	Do not launch regulated transfer, e-money, payment-instrument, aggregation or related infrastructure activity until BCC confirms the classification and grants every required approval.	Legal classification, BCC approval, licensed-service map, agent register and conditions tracker.	Law No. 22/068, arts. 69-70; Law No. 22/069; BCC Instructions Nos. 24 and 42
The statute treats virtual-asset service providers as reporting persons, but statutory AML coverage is not itself evidence of a current VASP licence.	Block any virtual-asset product launch until the competent authority confirms the licensing basis, permitted services and AML, custody, technology and reporting conditions in writing.	Authority correspondence, legal opinion, licence or refusal, product restriction and control assessment.	Law No. 22/068, arts. 2-3 and 92

Governance, risk assessment and control ownership

Controls must follow documented ML, TF and proliferation-financing risk and be owned, resourced, tested and updated.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting persons identify, assess, understand and mitigate their exposure to ML, TF and proliferation-financing risk, proportionate to their nature, size and transaction volume.	Maintain enterprise, customer, product, geographic, transaction and delivery-channel assessments and link the results to acceptance, CDD, monitoring, EDD and sanctions rules.	Risk methodology, assessment, data inputs, mitigation plan and governing-body approval.	Law No. 22/068, arts. 20-22; BCC Instruction No. 15 modification No. 3, arts. 6-8
A reporting person must maintain a risk-appropriate AML/CFT/CPF programme with compliance leadership, centralised information, independent audit, staff integrity checks, training, internal control and suspicious-reporting arrangements.	Appoint accountable management and compliance owners, approve policies, protect independence and resources and test design and operating effectiveness.	Appointments, charter, policies, training logs, monitoring plan, audit reports and remediation tracker.	Law No. 22/068, arts. 44-45; BCC Instruction No. 15 modification No. 3, arts. 75-87
New products, business practices, channels and technologies require risk assessment before launch and proportionate mitigation.	Assess identity fraud, impersonation, cyber, privacy, sanctions and transaction risks before production and gate launch on accepted residual risk.	Pre-launch assessment, threat model, vendor due diligence, tests and release approval.	Law No. 22/068, art. 22
Groups apply equivalent AML/CFT/CPF controls and information-sharing arrangements to branches and subsidiaries, subject to local-law conflicts; reliance on a third party does not transfer final responsibility.	Set group minimums, document local-law gaps, obtain customer evidence immediately from relied-on parties and preserve audit and exit rights.	Group standard, conflict analysis, reliance contract, retrieval test and remediation record.	Law No. 22/068, arts. 27-30; BCC Instruction No. 15 modification No. 3, arts. 26 and 46-47

Natural-person CDD and failed verification

Identity is verified from reliable independent evidence at every applicable trigger, with a controlled outcome when verification cannot be completed.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
CDD applies before a relationship or qualifying occasional transaction, to linked operations, qualifying electronic transfers, whenever suspicion exists and whenever earlier identity information is doubtful. For institutions within BCC Instruction No. 15's scope, the listed occasional-transaction trigger is above USD 15,000.	Configure relationship, aggregation, transfer, suspicion and refresh triggers; keep sector thresholds and exceptions in a governed register.	CDD trigger matrix, threshold register, aggregation tests, workflow configuration and exception report.	Law No. 22/068, arts. 31-32; BCC Instruction No. 15 modification No. 3, art. 10
Identify and verify a natural person using current official photo identification and reliable independent sources; verify address and any representative's authority.	Validate the identity document, authenticity, identity attributes, address and mandate before activation, subject only to a documented lawful low-risk deferral.	Identity copy, authenticity result, source provenance, address evidence, mandate and completion timestamp.	Law No. 22/068, arts. 31 and 33; BCC Instruction No. 15 modification No. 3, arts. 10-16
Understand the purpose and intended nature of the relationship, expected activity, source of funds where appropriate and the customer's risk profile; anonymous, fictitious and pseudonymous accounts are prohibited.	Capture expected products, flows, counterparties, countries and funding and compare later activity to the approved profile.	Purpose statement, expected-activity baseline, source evidence, risk score and account-opening controls.	Law No. 22/068, arts. 26 and 47; BCC Instruction No. 15 modification No. 3, arts. 9 and 27-31
If identity or beneficial ownership cannot be established, do not execute or begin the relationship; for an existing relationship, end it where required and assess an STR. If further CDD would tip off a suspected customer, stop the verification and report without delay.	Route failed, doubtful or overdue CDD to decline, restriction or exit with a confidential CENAREF-reporting decision.	Failure reason, decline or restriction, exit record, STR decision and access log.	Law No. 22/068, arts. 36-38; BCC Instruction No. 15 modification No. 3, arts. 24 and 40

KYB, commercial registry and beneficial ownership

Legal existence, authority and ultimate ownership or control are separate tests. The statutory central register is not a substitute for independent KYB.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
For a legal person or legal arrangement, verify constitution and existence, understand purpose, activity, ownership and control and identify directors and representatives.	Collect a current RCCM or other official registry extract, constitutional documents, tax and licence evidence, registered address, directors and signatory mandates; reconcile material discrepancies.	Registry extract, statutes, tax evidence, licence, management list, mandate and discrepancy log.	Law No. 22/068, art. 34; BCC Instruction No. 15 modification No. 3, arts. 17-22
Identify the natural person who directly or indirectly owns more than 25% of capital or voting rights, then test control by other means and use the applicable statutory management or legal-representative fallback only if no natural person is otherwise identified.	Trace every ownership layer, calculate direct and indirect interests, test factual and legal control and document any fallback.	Ownership chart, percentage calculations, control analysis, source records and verified BO files.	Law No. 22/068, arts. 35 and 39
Specified persons must declare and update beneficial-owner identity through GUCE or the National Cooperatives Service. Reporting persons collect and retain accurate current BO information and transmit information to GUCE under the implementing mechanism.	Maintain an internal BO register and change trigger, prepare the statutory data set and preserve proof of any filing accepted by the competent registry.	Internal BO register, change log, filing package, registry receipt and reconciliation.	Law No. 22/068, arts. 39 and 46

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
The Justice Minister's order must establish the central BO register and its access, protection and retention mechanics. An official ITIE-RDC workshop on 9 April 2026 still described that order as a draft awaiting adoption and operationalisation.	Do not invent a portal, form or deadline. Confirm the current order and GUCE workflow before automating central filing, while continuing statutory collection, verification and update controls.	Dated legal check, authority correspondence, current order, filing procedure and implementation ticket.	Law No. 22/068, arts. 40-43; ITIE-RDC, 9 April 2026
Reporting persons and supervisors report discrepancies in registered BO information to GUCE; if the legal person does not regularise within one month after GUCE's request, GUCE informs CENAREF.	Maintain a discrepancy workflow that separates customer remediation, registry notification and any independent suspicious-reporting decision.	Discrepancy notice, customer evidence, GUCE correspondence, one-month timer and STR assessment.	Law No. 22/068, art. 42

PEPs, enhanced due diligence and remote onboarding

Higher-risk, politically exposed and non-face-to-face relationships require additional evidence, accountable approval and closer monitoring.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether a customer or beneficial owner is a domestic, foreign or international-organisation PEP and cover statutory family members and close associates. The statutory definition looks back 36 months, subject to continuing risk-based enhanced measures.	Screen before activation and continuously, resolve matches using reliable role and relationship evidence and record any decision to cease PEP treatment.	Screening result, match disposition, role evidence, relationship analysis and risk rationale.	Law No. 22/068, art. 3 definition 40 and arts. 53 and 56
A PEP relationship requires appropriate management approval, reasonable measures to establish source of wealth and source of funds and enhanced continuous monitoring.	Collect and corroborate wealth and funds evidence, obtain approval before starting or maintaining the relationship and configure enhanced review.	Source-of-wealth and source-of-funds file, approval, monitoring plan and review history.	Law No. 22/068, art. 56; BCC Instruction No. 15 modification No. 3, arts. 41 and 64
Financial intermediaries within Instruction No. 15's scope inform CENAREF of an identified PEP at onboarding even where no suspicious indicator exists.	Keep this PEP notification separate from an STR, confirm CENAREF's current submission channel and preserve the acknowledgement.	PEP notice, submission record, receipt and separate STR decision where applicable.	BCC Instruction No. 15 modification No. 3, art. 65
Complex, unusually large, unjustified or apparently non-economic activity requires enhanced examination. Instruction No. 15 requires enhanced review of cash or bearer activity at USD 10,000 equivalent or more for its covered institutions.	Document origin and destination of funds, purpose, actors, corroboration and the final reporting decision in a confidential report.	Enhanced-review report, transaction data, source evidence, decision and reviewer sign-off.	Law No. 22/068, arts. 54-55; BCC Instruction No. 15 modification No. 3, arts. 61-63

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Remote onboarding remains subject to full identity, beneficial-owner, sanctions and PEP controls, with adapted safeguards such as document authentication and independent verification.	Use risk-based document integrity, liveness or presence, device, fraud and manual-escalation controls and validate them before production.	Remote-onboarding standard, vendor review, performance tests, fraud cases and exception log.	BCC Instruction No. 15 modification No. 3, arts. 23 and 25

Ongoing monitoring, STRs and prohibited disclosure

Monitoring must detect activity inconsistent with the known profile and route suspicion promptly and confidentially to CENAREF.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing monitoring, keep customer and BO information current and review BCC-sector customer risk profiles at least semi-annually under Instruction No. 15.	Compare activity to purpose, expected behaviour, business and source of funds; trigger refresh after material identity, ownership, activity or risk changes.	Monitoring scenarios, alert decisions, profile review, change log and governance metrics.	Law No. 22/068, arts. 26 and 47; BCC Instruction No. 15 modification No. 3, arts. 27-31
Report without delay to CENAREF where there is knowledge, suspicion or reasonable grounds to suspect criminal proceeds or ML, TF or PF; attempted transactions and later information that changes an STR are included.	Timestamp suspicion formation, submit immediately through the confirmed CENAREF route and send supplements without delay.	Suspicion timestamp, STR, submission proof, case reference and supplemental reports.	Law No. 22/068, art. 92; BCC Instruction No. 15 modification No. 3, arts. 88-90
Unresolved uncertainty about an originator, beneficial owner, trust settlor or similar arrangement is independently reportable. A separate threshold report for qualifying cash or e-money funds transmissions depends on an implementing Finance Minister order.	File on unresolved identity uncertainty and keep any automatic threshold report disabled until the current ministerial amount and procedure are verified.	Identity-escalation decision, STR, controlled threshold register and authority confirmation.	Law No. 22/068, art. 92
An STR may be sent in writing, digitally, electronically or by telephone; a telephone report is confirmed in writing promptly. No authoritative public CENAREF self-service filing portal was verified at the review date.	Confirm the current secure operational channel directly with CENAREF, maintain tested primary and contingency routes and preserve acknowledgements without delaying urgent reporting.	CENAREF confirmation, channel test, controlled contact list, submission and receipt.	Law No. 22/068, art. 94; BCC Instruction No. 15 modification No. 3, arts. 93-94

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Do not disclose an STR, its content or its outcome to the customer or unauthorised third parties. CENAREF may oppose execution for up to seven days; the public prosecutor may extend or seize for up to eight additional days.	Restrict case access, use approved customer communications and implement holds, extensions, releases and seizures exactly as instructed.	Access log, confidentiality script, hold timeline, CENAREF notice, judicial order and release record.	Law No. 22/068, arts. 93 and 96

Cash, payments, wires and agents

Cash restrictions, cross-border declarations, payment licensing and wire information are distinct controls and should not be collapsed into one threshold rule.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Transactions at USD 10,000 equivalent or more generally may not be settled in cash or bearer instruments, subject to statutory exceptions and BCC derogations. This is a payment restriction, not a universal automatic STR threshold.	Enforce the cashless rule, document any lawful exception or Instruction No. 15 bis derogation and separately assess unusual or suspicious activity.	Payment control, exception basis, BCC derogation, enhanced review and STR decision.	Law No. 22/068, art. 23; BCC Instruction No. 15 bis modification No. 4
A person entering or leaving the DRC declares cash or bearer negotiable instruments at USD 10,000 equivalent or more at the point of entry or exit.	For relevant customer journeys and own-cash movements, provide the declaration requirement and retain customs evidence; do not treat the border rule as an account-monitoring report.	Procedure, declaration copy, customs receipt and exception or seizure record.	Law No. 22/068, art. 25
Wire messages carry required originator and beneficiary data. Missing or inaccurate information must be obtained and verified; if it remains unavailable, do not execute and inform CENAREF where applicable.	Validate required fields before release, preserve unique references and route incomplete transfers to repair, rejection and suspicious-reporting assessment.	Field matrix, message sample, repair queue, rejection test and STR decision.	Law No. 22/068, arts. 57-61; BCC Instruction No. 15 modification No. 3, arts. 45 and 66-69
Instruction No. 15 article 67 provides narrowly framed online-payment verification relief only where no suspicion exists, funds move between qualifying named accounts and the transaction and rolling limits remain below USD 2,500 and USD 30,000 respectively.	Apply the relief only after confirming the drafting and sector scope with BCC; configure both unit and rolling limits and full CDD on any exception or suspicion.	BCC confirmation, eligibility rules, threshold tests, named-account evidence and exception log.	BCC Instruction No. 15 modification No. 3, art. 67

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Funds or value transfer providers using agents must notify the competent authority of agents, include them in the AML programme, monitor them and retain relevant operational information for CENAREF.	Maintain an approved agent register, due diligence, training, transaction oversight, audit rights and termination controls.	Agent list, approval, contract, training, monitoring report and issue closure.	Law No. 22/068, arts. 69-70

Sanctions, freezing and proliferation financing

Targeted financial sanctions are implemented through current CONASAFIC, UN and national-list procedures and are operationally separate from suspicious reporting.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen current UN and national designations disseminated by CONASAFIC, including names, aliases, identifiers and ownership or control; subscribe a monitored address to CONASAFIC alerts and use the Sentinelle platform.	Automate list updates where reliable, test ingestion and matching, monitor alert delivery and preserve list-version evidence for every decision.	List inventory, Sentinelle access, alert subscription, update log, test results and match file.	Decrees Nos. 24/24 and 24/25; CONASAFIC list-diffusion procedure
Freeze designated funds, other assets and economic resources without delay and without prior notice, prevent any direct or indirect availability or service and prohibit circumvention.	Execute the freeze immediately, secure all affected products and benefits and do not wait for an STR decision or customer contact.	Freeze timestamp, asset inventory, system blocks, decision record and no-notice control.	Law No. 22/068, arts. 152-163; Decree No. 24/24
Notify CENAREF and CONASAFIC without delay and report the measures and attempted transactions under the current procedure; follow authority instructions for false positives, exemptions, delisting and release.	Use a controlled notification and case-management matrix and release property only on a valid authority instruction.	Notification, receipt, authority correspondence, false-positive analysis and release instruction.	Law No. 22/068, arts. 162-163; CONASAFIC guidelines and Sentinelle
A sanctions match, freeze and STR are separate decisions that may arise from the same facts.	Link but do not merge the cases; record legal basis, decision owner, timing, confidentiality and communications for each track.	Linked case records, freeze action, separate STR assessment, access controls and audit trail.	Law No. 22/068, arts. 92 and 152-163

Records, retention and authority access

Records must support full reconstruction and prompt authorised access while protecting confidential reporting and personal data.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep customer and beneficial-owner identity, account books, business correspondence and analysis for 10 years from account closure or relationship end, and transaction and e nhanced-examination records for 10 years after execution.	Map every AML record class to the correct event, preserve legal holds and prevent premature deletion.	Retention schedule, lifecycle configuration, legal-hold procedure and deletion test.	Law No. 22/068, art. 48; BCC Instruction No. 15 modification No. 3, art. 48
An intermediary institution keeps received wire data for at least five years where technical constraints prevent it remaining attached to the corresponding domestic transfer.	Preserve detached message data with a reliable link to the transaction and test retrieval and reconstruction.	Wire archive, linkage key, retention configuration and reconstruction test.	Law No. 22/068, art. 48; BCC Instruction No. 15 modification No. 3, art. 49
Provide required CDD and transaction records without delay to authorised judicial, investigative, supervisory and CENAREF authorities; professional secrecy cannot defeat a lawful request.	Authenticate each request, apply least-privilege disclosure, log the response and maintain rapid searchable retrieval.	Authority-request register, authentication, response package, access log and retrieval test.	Law No. 22/068, arts. 49 and 97
STR and sanctions files require restricted access and tamper-evident auditability throughout retention.	Separate confidential-case roles from ordinary customer service, preserve immutable event history and test unauthorised-access prevention.	Access matrix, immutable log, access review, incident record and audit result.	Law No. 22/068, arts. 93-105

Privacy, biometrics and international transfers

AML necessity does not displace the Digital Code. Identity and biometric processing require purpose, authority formalities, security, data-subject rights and transfer controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Personal-data processing is generally subject to prior APD declaration; biometric, national-identifier, criminal, medical and foreign-transfer processing requires prior authorisation unless a specific exemption applies.	Map every identity, biometric, screening, transaction and investigation purpose and determine the declaration, authorisation or documented exemption before production.	Processing inventory, legal-basis register, APD filing or decision, exemption analysis and privacy notice.	Ordinance-Law No. 23/010, arts. 183-191
Process data lawfully, fairly, transparently and for specified purposes; minimise it, keep it accurate, limit storage to necessity and apply appropriate technical and organisational security.	Publish clear notices, define purpose and retention, restrict collection and access and implement backup, recovery, encryption and monitoring proportionate to risk.	Notice, data map, minimisation review, retention rules, security design and test results.	Ordinance-Law No. 23/010, arts. 192-195 and 220-224
Appoint an independent DPO and maintain processing records where required. The SME and startup exception does not apply to risky, non-occasional, special-category or criminal-data processing.	Document whether the exception is available; for KYC and biometric operations, appoint the DPO, publish contact details and maintain controller and processor registers.	Applicability analysis, DPO appointment, contact notice, registers and management reporting.	Ordinance-Law No. 23/010, arts. 222 and 225-231
Notify the APD and affected person without delay of a personal-data breach, subject to the statutory exceptions for individual communication; processors alert controllers without delay.	Maintain a tested incident plan, assess every security event promptly and document authority and individual notifications or the legal reason not to notify an individual.	Incident log, risk assessment, APD notice, individual communication and processor alert.	Ordinance-Law No. 23/010, art. 244

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
High-risk processing, including large-scale biometric identification and significant automated profiling, requires a data-protection impact assessment and may require prior APD consultation.	Complete a DPIA before launch, involve the DPO and consult the APD if residual high risk remains.	DPIA, DPO advice, mitigation tests, APD consultation and launch decision.	Ordinance-Law No. 23/010, arts. 245-246
A foreign transfer requires prior APD authorisation and adequate protection or a documented statutory derogation. The APD was created by statute, but a fully operational public filing route was not verified at the review date.	Map hosting and support locations, document the transfer basis and safeguards and obtain written current filing instructions before transferring KYC data abroad.	Transfer map, adequacy or derogation analysis, APD authorisation or correspondence, contract and access controls.	Ordinance-Law No. 23/010, arts. 187 and 201-202 and 262-263

11. IMPLEMENTATION AND AUDIT EVIDENCE PACK

Implementation and audit evidence pack

A defensible programme links every rule to configuration, ownership, testing, dated source evidence and a controlled residual-risk decision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Run a documented pre-launch regulatory gate covering perimeter, licensing, CDD, BO, PEP, sanctions, monitoring, CENAREF reporting, records, privacy and payments.	Block production until accountable owners approve control design and every material gap has a closed remediation or explicit lawful launch condition.	Launch checklist, approvals, test pack, gap register and release decision.	Law No. 22/068; applicable BCC, CONASAFIC and Digital Code instruments
Third-party verification, agents, cloud providers and outsourcing do not transfer the reporting entity's legal responsibility.	Assess each provider, contract immediate evidence access and audit rights, test retrieval, monitor performance and maintain an exit plan.	Due-diligence file, contract, access test, monitoring report, issues and exit plan.	Law No. 22/068, arts. 29-30; BCC Instruction No. 15 modification No. 3, art. 26; Digital Code, arts. 224 and 229
Track official changes from the Gazette, CENAREF, BCC, GUCE, CONASAFIC, the Digital Ministry or APD, FATF and GABAC, especially the BO-register order, APD operating decree and threshold or filing orders.	Assign source owners, review official updates on a controlled schedule and assess each change against policies, products and existing customers.	Legal inventory, dated monitoring log, impact assessment, implementation ticket and approval.	Official DRC authority and FATF publications
Independently test onboarding, BO, PEP, sanctions, payments, monitoring, STR, privacy and retention controls and preserve why each rule is configured as it is.	Run risk-based monitoring and independent assurance, report material findings to governance and verify remediation to closure.	Control-to-law map, monitoring plan, audit report, issue register, closure evidence and release history.	Law No. 22/068, arts. 44-45; BCC Instruction No. 15 modification No. 3

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. 22/068 of 27 December 2022 on AML/CFT/CPF
Republic of the DRC / ANAPI · Primary legislation
Open official source

Official company-creation and legal-document portal
ANAPI · Official government portal
Open official source

Banking regulatory register including Instruction No. 15 modification No. 3
Banque Centrale du Congo · Official sector register
Open official source

Instruction No. 15 modification No. 3 on AML/CFT/CPF standards
Banque Centrale du Congo · Primary sector instruction
Open official source

Instruction No. 15 annexes on BCC reporting
Banque Centrale du Congo · Primary sector reporting annex
Open official source

Instruction No. 15 bis modification No. 4 on cash and bearer derogations
Banque Centrale du Congo · Primary sector instruction
Open official source

Instruction No. 15 bis modification No. 4 PDF
Banque Centrale du Congo · Primary sector instruction
Open official source

Payment-systems regulatory register
Banque Centrale du Congo · Official sector register
Open official source

Instruction No. 24 on e-money issuance and e-money institutions
Banque Centrale du Congo · Primary sector instruction
Open official source

Instruction No. 42 on card and electronic payment rules
Banque Centrale du Congo · Primary sector instruction
Open official source

BCC-authorised connected payment-service providers
Banque Centrale du Congo · Official provider register
Open official source

Services attached to the Ministry of Finance, including CENAREF
Ministry of Finance · Official authority directory
Open official source

CENAREF strategic activity report 2021-2023
CENAREF · Official FIU report
Open official source

CONASAFIC official portal
CONASAFIC / Ministry of Finance · Official sanctions portal
Open official source

CONASAFIC legal and procedure documents
CONASAFIC / Ministry of Finance · Official sanctions register
Open official source

Procedure for disseminating targeted-financial-sanctions lists
CONASAFIC · Official sanctions procedure
Open official source

Sentinelle sanctions search, alert and compliance platform
CONASAFIC · Official sanctions platform
Open official source

UN Security Council consolidated sanctions list
United Nations · Official sanctions list
Open official source

Ordinance-Law No. 23/010 establishing the Digital Code
Autorite de Regulation du secteur de l'Electricite / Presidency of the DRC · Primary legislation
Open official source

Digital Code personal-data authority provisions
Droit-Numerique.cd · Legislation access and article index
Open official source

April 2026 workshop on the draft beneficial-owner-register order
ITIE-RDC · Official implementation-status notice
Open official source

Jurisdictions under increased monitoring, 19 June 2026
FATF · Official international status statement
Open official source

DRC mutual evaluation report
GABAC / FATF · Official historical assessment context
Open official source

Law No. 22/069 and current sanctions-framework documents
CONASAFIC · Official legislation and implementation register
Open official source

BCC regulatory publications and current contacts
Banque Centrale du Congo · Official regulator portal
Open official source

Document control

Version 1.0 / Published 2026 / Last reviewed 16 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice or a licence determination. It reflects sources reviewed on 16 July 2026. Confirm current gazetted law, sector rules, thresholds, filing mechanics and supervisor expectations with Congolese counsel and the competent authority before launch. The statutory beneficial-owner register and the APD's operating procedures were not confirmed as fully operational public filing routes at the review date. VOVE ID can support evidence collection, screening and audit trails, but the reporting entity remains responsible for risk decisions, customer acceptance, reports, freezes and regulatory compliance.