VOVE ID

VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

TOGO

TOGO / TG

KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Togo KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for financial institutions, fintechs and designated non-financial businesses operating in Togo under the 2026 AML/CFT/CPF law, UMOA rules, beneficial-ownership framework and personal-data law.

Primary AML/CFT/CPF law	**Law No. 2026-001 of 2 March 2026**
Financial intelligence unit	**CENTIF Togo**
STR timing	**Immediately after suspicion or reasonable grounds arise**
Cash transaction report	**XOF 15 million or more, including apparently linked operations**
Core AML retention	**10 years under record-class-specific clocks**
Beneficial ownership	**Controlling ownership, other control, then senior-manager fallback**
Payments authority	**BCEAO within the UMOA framework**
Privacy authority	**IPDCP Togo**
VASP perimeter	**Prior competent-authority approval or authorisation required**
FATF public lists	**Not named in the June 2026 statements**

Scope and legal framework

Law No. 2026-001 of 2 March 2026 is Togo's principal AML/CFT/CPF law and implements the 2023 UMOA uniform framework. UMOA Council Decision No. 021 of 21 December 2023 supplies key operational thresholds. BCEAO instructions apply additional controls to regulated financial institutions and payment services. Law No. 2019-014 of 29 October 2019 governs personal-data processing under IPDCP oversight.

FATF context

As at 24 July 2026, Togo was not named in FATF's June 2026 statements on jurisdictions under increased monitoring or jurisdictions subject to a call for action. Togo remains in GIABA enhanced follow-up; that peer-review status is distinct from FATF public-list status.

IMPORTANT

This checklist is general regulatory information, not legal advice or a licence determination. It reflects primary and authoritative materials reviewed on 24 July 2026. Confirm the live CENTIF reporting route and forms, activity-specific licences, sanctions instructions, beneficial-owner filing workflow, IPDCP formalities and all sector overlays with the competent authority and qualified Togolese counsel before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

For every row, assign an owner, confirm whether the control applies, link the evidence, record gaps, and set a remediation date. A checked box is not evidence by itself.

01 / SCOPE	02 / DESIGN	03 / EVIDENCE	04 / REVIEW
Confirm institution, supervisor, product, customer and risk scope.	Map each obligation to a policy, system control or human review.	Retain the document, decision, timestamp, owner and rationale.	Test the control and update it when rules or risks change.

Checklist legend

CONTROL tells you what outcome to cover. IMPLEMENTATION ACTION translates that outcome into operational work. EVIDENCE suggests what an auditor or reviewer should be able to inspect. SOURCE points back to the primary rule or regulator guidance.

Minimum review record

Keep a compact decision record for each checklist row so a later reviewer can reconstruct what applied, who decided, and what evidence was inspected.

APPLICABILITY	OWNERSHIP	TRACEABILITY
Applicable, not applicable, or pending legal confirmation, with a short rationale.	Named control owner, reviewer, approval date and next review date.	Evidence link, source version, test result, gap status and remediation ticket.

Scope, authorities and regulated activities

Resolve entity, activity and supervisor scope before onboarding or launch.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Financial institutions and listed designated non-financial businesses and professions are reporting persons.	Map each entity, product, profession, branch, distributor, agent and outsourced function to Law No. 2026-001 and document the responsible supervisor.	Perimeter memorandum, entity-product map, licences and supervisor correspondence.	Law No. 2026-001, arts. 2-4 and 107
CENTIF receives and analyses suspicious transaction reports and may request information.	Appoint an authorised correspondent and obtain the current CENTIF access, form and acknowledgement instructions before production reporting.	Appointment, access record, reporting procedure and test evidence.	Law No. 2026-001, arts. 60, 64 and 95-103
In-scope virtual-asset services require prior approval or authorisation from the competent authority.	Obtain a written perimeter assessment and the required approval before exchange, transfer, custody or other in-scope virtual-asset activity.	Classification, application, approval, conditions and service map.	Law No. 2026-001, arts. 58-59
Regulated payment services require the applicable BCEAO authorisation.	Map each payment, e-money, acquiring, transfer, remittance, initiation and agent function to the current UMOA payment-services framework.	Licence or exemption analysis, BCEAO register check and partner file.	BCEAO Instruction No. 001-01-2024 and current authorised-institution register

Governance, risk assessment and control ownership

Build documented, risk-based controls with accountable governance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting persons must maintain internal organisation, controls and risk management proportionate to their activities.	Approve policies for CDD, BO, PEPs, sanctions, monitoring, reporting, recordkeeping, training, screening and independent testing.	Policy suite, approvals, control library, training and audit reports.	Law No. 2026-001, arts. 12-14
Money-laundering, terrorist-financing and proliferation-financing risks must be identified, assessed, documented and kept current.	Assess customers, geographies, products, services, transactions, channels, new products and technologies before launch and on material change.	Risk assessment, methodology, source data, change log and approvals.	Law No. 2026-001, art. 15
Institutions must be able to justify that customer controls are proportionate to risk.	Define risk-rating logic, control variants, approval levels and review cycles, then test their operation.	Risk model, decision records, samples and assurance results.	Law No. 2026-001, arts. 19-21 and 84-85

Natural-person identification and CDD

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Before a relationship or assisted transaction, collect and verify identity from reliable, independent sources and understand purpose and intended nature.	Capture identity attributes, verify evidence provenance, identify the beneficial owner and establish the expected activity profile.	CDD file, source provenance, verification result, purpose and risk decision.	Law No. 2026-001, arts. 16-17
CDD also applies to transfers, suspicion, identity doubt and applicable occasional or linked transactions.	Configure relationship, transfer, cash aggregation, suspicion and identity-quality triggers; do not treat a threshold as a safe harbour.	Trigger matrix, aggregation results, alerts and CDD timestamps.	Law No. 2026-001, arts. 17 and 49; UMOA Decision No. 021
Limited delayed verification must finish as soon as possible and before the first transaction, with effective risk controls.	Block transaction capability until verification is complete and document why each statutory condition is satisfied.	Deferral approval, restrictions, completion timestamp and exception testing.	Law No. 2026-001, art. 18
Remote relationships require particular and sufficient preventive measures.	Use risk-calibrated document, device, liveness, biometric or equivalent safeguards and manual escalation without assuming one technology is legally sufficient.	Remote-onboarding standard, vendor review, model tests and exceptions.	Law No. 2026-001, art. 22

KYB, authority and beneficial ownership

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Legal-person and legal-arrangement CDD covers legal name, form, constitutive documents, powers, management and addresses.	Obtain current registry and constitutional evidence and verify every representative's identity and authority.	Registry extract, statutes, managers, addresses, mandate and discrepancy log.	Law No. 2026-001, arts. 17 and 26
The BO cascade tests controlling ownership, then control by other means, then the relevant senior managing official.	Trace every ownership layer and control right; document why each stage did or did not identify a natural person before using the fallback.	Ownership chart, control analysis, fallback rationale and verified BO files.	Law No. 2026-001, art. 26
Trusts and comparable arrangements use role-based BO tests.	Identify and verify the settlor, trustee, protector, beneficiaries or class and every other natural person exercising ultimate control.	Instrument, role register, identity files and control analysis.	Law No. 2026-001, art. 26
Companies must keep accurate, current shareholder, member and BO information; the national BO register is established by law.	Maintain event-driven updates, reconcile registry data and complete filings under the current competent-authority implementation procedure.	Registers, update log, filing receipts, supporting documents and discrepancies.	Law No. 2026-001, arts. 76-79 and 122; current competent-authority implementation instruments

5. PEPS, ENHANCED DUE DILIGENCE AND RELIANCE

PEPs, enhanced due diligence and reliance

Apply stronger approval, evidence and monitoring where risk is higher.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
PEP relationships require risk systems, senior-management approval, source-of-wealth and source-of-funds measures, and enhanced monitoring.	Screen customers and BOs for domestic, foreign and international-organisation PEP exposure and connected-person risk.	Screening, match rationale, source file, approval and monitoring plan.	Law No. 2026-001, art. 29
Institutions reassess identified PEP customer profiles every three years and retain risk-based treatment where warranted.	Schedule the statutory reassessment and document any change to status or controls.	Review diary, reassessment, decision and approval.	Law No. 2026-001, art. 29
Higher-risk relationships require enhanced measures; simplified treatment needs a demonstrated lower-risk basis and cannot override suspicion.	Document control changes, corroboration, approvals and monitoring intensity for each risk treatment.	EDD or SDD rationale, evidence, approval and review.	Law No. 2026-001, arts. 30 and 84-85
Reliance on a third party does not remove the institution's responsibility for CDD.	Assess eligibility, obtain required information immediately, contract for document access and test retrieval.	Due diligence, agreement, retrieval test and exceptions.	Law No. 2026-001, arts. 35-38

Failed CDD, monitoring and suspicious reporting

Block unsafe activity, monitor continuously and report suspicion immediately and confidentially.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
If required CDD cannot be completed, do not open or execute, or terminate the relationship, and submit an STR.	Operate a controlled block or exit and preserve the confidential STR decision.	Failure reason, block, closure, STR and acknowledgement.	Law No. 2026-001, art. 25
Relationships and transactions require ongoing scrutiny, current CDD and written examination of complex, unusual or apparently purposeless activity.	Investigate source, destination, purpose and BO, refresh CDD and retain the confidential written analysis.	Alerts, cases, report, refreshed CDD and review.	Law No. 2026-001, arts. 19-21
Reporting persons must immediately report suspected sums, transactions and attempted transactions to CENTIF.	Timestamp when suspicion or reasonable grounds arose and file using the current prescribed route and model; send changes or supplements without delay.	Internal report, analysis, STR, CENTIF receipt and timeline.	Law No. 2026-001, art. 60
Suspicious activity is withheld before reporting unless the statutory post-execution conditions apply; tipping off is prohibited.	Govern holds, lawful release, post-execution reporting and restricted communications.	Hold decision, exception rationale, access logs and communications record.	Law No. 2026-001, arts. 61 and 63

Wires, cash thresholds, payments and agents

Keep CDD triggers, special examination and threshold reports distinct.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Cash transactions of XOF 15 million or more, including apparently linked operations, are reported to CENTIF.	Aggregate linked activity, configure the exact in-scope entity and transaction logic, and obtain current CENTIF reporting instructions.	Threshold configuration, tests, reports, receipts and exception record.	Law No. 2026-001, art. 72; UMOA Decision No. 021, art. 8
Multiple cash transactions exceeding XOF 9 million in one day or at unusual frequency trigger identification and verification for financial institutions.	Aggregate by person and account across channels and apply CDD regardless of amount where suspicion exists.	Aggregation logic, customer match, CDD file and testing.	Law No. 2026-001, art. 17(i); UMOA Decision No. 021, art. 3
Payment in cash or bearer title at XOF 50 million or more, and unusual or unjustified operations at XOF 10 million or more, require special examination.	Investigate origin, destination, purpose and BO and retain a confidential report.	Scenario, investigation, source evidence, report and approval.	Law No. 2026-001, art. 21; UMOA Decision No. 021, art. 4
Wire transfers must carry required originator and beneficiary information and deficient transfers require governed handling.	Validate required data throughout the chain and define reject, suspend, execute, investigate and follow-up rules.	Field matrix, validation, repair queue, samples and decisions.	Law No. 2026-001, arts. 39-47

8. TARGETED FINANCIAL SANCTIONS AND CPF

Targeted financial sanctions and CPF

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Reporting persons must implement internal procedures for targeted financial sanctions.	Screen customers, BOs, controllers, representatives and transactions at onboarding, list updates and before relevant activity.	List inventory, update logs, screening results and match files.	Law No. 2026-001, arts. 89 and 124
Property of a designated person or entity is frozen immediately after notification, without prior notice, and must not be made available.	Maintain a 24/7 freeze and escalation path covering direct, indirect, owned and controlled exposure.	Procedure, system test, match decision, freeze and audit trail.	Law No. 2026-001, art. 89
CENTIF and the competent authority are informed immediately of relevant funds, frozen assets, measures and attempted operations.	Use the current competent-authority route and obtain written direction before release or dealing.	Notifications, receipts, directions and release decision.	Law No. 2026-001, arts. 90-91

9. RECORDS, ACCESS AND ASSURANCE

Records, access and assurance

Retain reconstructable records under the correct statutory clock.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Customer identity, profile and analysis records are kept for 10 years after account closure or relationship cessation.	Map every customer record class to the relationship-based clock and apply legal holds.	Retention schedule, configuration, sample and deletion test.	Law No. 2026-001, art. 23
Transaction, accounting and business-correspondence records are kept for 10 years after execution.	Use transaction-based clocks and retain enough information to reconstruct individual operations.	Archive configuration, reconstruction test and retrieval log.	Law No. 2026-001, art. 23
Corporate and BO information is retained for at least 10 years after dissolution or the end of the relevant professional relationship.	Assign an archive owner and preserve current and historic ownership evidence.	Dissolution checklist, archive, access controls and retrieval test.	Law No. 2026-001, art. 79
Required records must be available to CENTIF, supervisors, judicial authorities and authorised investigators.	Index linked identity, transaction, investigation and reporting evidence and test controlled export.	Request register, retrieval tests, access log and response package.	Law No. 2026-001, arts. 24 and 103

10. PRIVACY, BIOMETRICS AND TRANSFERS

Privacy, biometrics and transfers

Apply Law No. 2019-014 alongside AML collection, retention and disclosure duties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Personal-data processing requires a defined purpose, lawful treatment, proportionality, security and rights controls.	Inventory identity, BO, screening, monitoring and reporting data; document purpose, access, recipients, location and retention.	Processing register, basis assessment, notices, access matrix and retention map.	Law No. 2019-014 of 29 October 2019
Applicable processing must complete the required IPDCP declaration, register or prior-authorisation formality before implementation.	Classify ordinary, sensitive, biometric, interconnected and cross-border processing with IPDCP or counsel before production use.	Formality matrix, filing, receipt or authorisation and change log.	Law No. 2019-014, arts. 5-9; IPDCP guidance
Biometric and other sensitive identity data require a specific lawful basis, necessity and stronger safeguards.	Document the applicable condition, minimise templates and raw images, test vendors and restrict access.	Legal assessment, necessity record, security design, tests and access logs.	Law No. 2019-014; controlled IPDCP implementation dependency
International transfers and security incidents require analysis under Law No. 2019-014 and current IPDCP procedures.	Document destinations and safeguards and maintain an incident escalation route; confirm current notification forms and deadlines rather than importing foreign rules.	Transfer assessment, contracts, incident log and IPDCP correspondence.	Law No. 2019-014; IPDCP official procedures

11. PRACTICAL EVIDENCE PACKS AND CHANGE CONTROL

Practical evidence packs and change control

Make every acceptance, escalation and regulatory decision reconstructable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
A complete customer file links identity, KYB, BO, screening, risk, approval, monitoring and reporting decisions.	Block activation where mandatory evidence or approval is missing and preserve the release decision.	Control checklist, linked file, approvals and release log.	Law No. 2026-001, arts. 12-26
Time-sensitive thresholds, lists, reporting routes, registers and licences require governed change monitoring.	Assign owners to review Journal Officiel, CENTIF-Togo, BCEAO, UMOA, CFE, IPDCP, FATF and GIABA sources on a documented schedule.	Legal inventory, source log, change assessment and implementation tickets.	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.

Official confirmation of Law No. 2026-001 of 2 March 2026 on AML/CFT/CPF
Ministry of Finance and Budget, Republic of Togo · Official promulgation confirmation
Open official source

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

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

UMOA Decision No. 003 of 28 March 2024 setting complementary thresholds
BCEAO · Primary regional decision
Open official source

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

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

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

CENTIF-Togo reporting information and official guidance
CENTIF-Togo · Official FIU portal
Open official source

Official company-creation and CFE registry procedure
Service public de l'administration togolaise · Official registry procedure
Open official source

Law No. 2019-014 of 29 October 2019 on personal-data protection
Journal Officiel de la Republique Togolaise · Primary legislation
Open official source

Personal-data compliance documentation and forms
IPDCP · Official data-protection authority guidance
Open official source

Togo country assessment and follow-up
FATF · Authoritative assessment index
Open official source

Togo 2025 third enhanced follow-up report
GIABA · Authoritative regional peer review
Open official source

Jurisdictions under Increased Monitoring - 19 June 2026
FATF · Authoritative public statement
Open official source

High-Risk Jurisdictions subject to a Call for Action - 19 June 2026
FATF · Authoritative public statement
Open official source

Document control

Version 1.0 / Published 24 July 2026 / Last reviewed 24 July 2026 / Owner: VOVE ID Compliance Research

This checklist is general regulatory information, not legal advice or a licence determination. It reflects primary and authoritative materials reviewed on 24 July 2026. Confirm the live CENTIF reporting route and forms, activity-specific licences, sanctions instructions, beneficial-owner filing workflow, IPDCP formalities and all sector overlays with the competent authority and qualified Togolese counsel before launch.