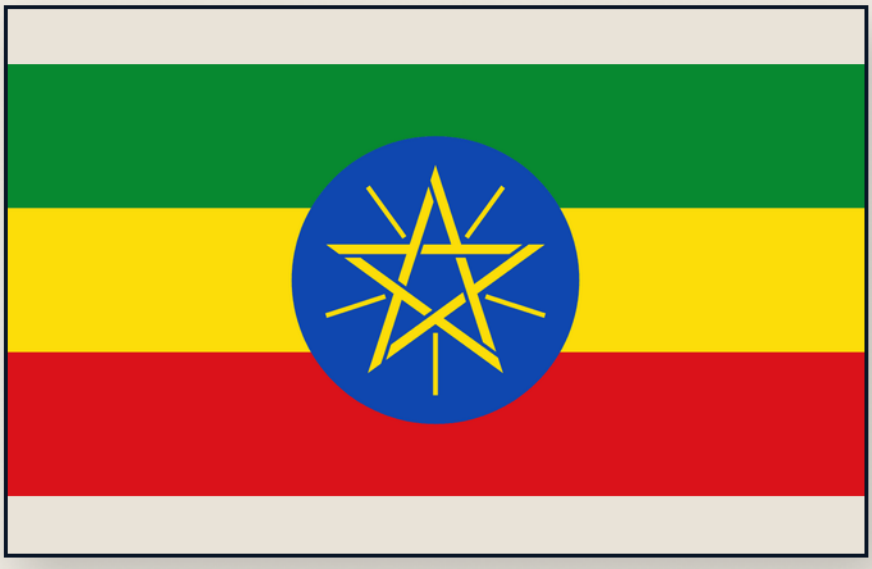
VOVE ID

VOVE COUNTRY CONTROL FILE

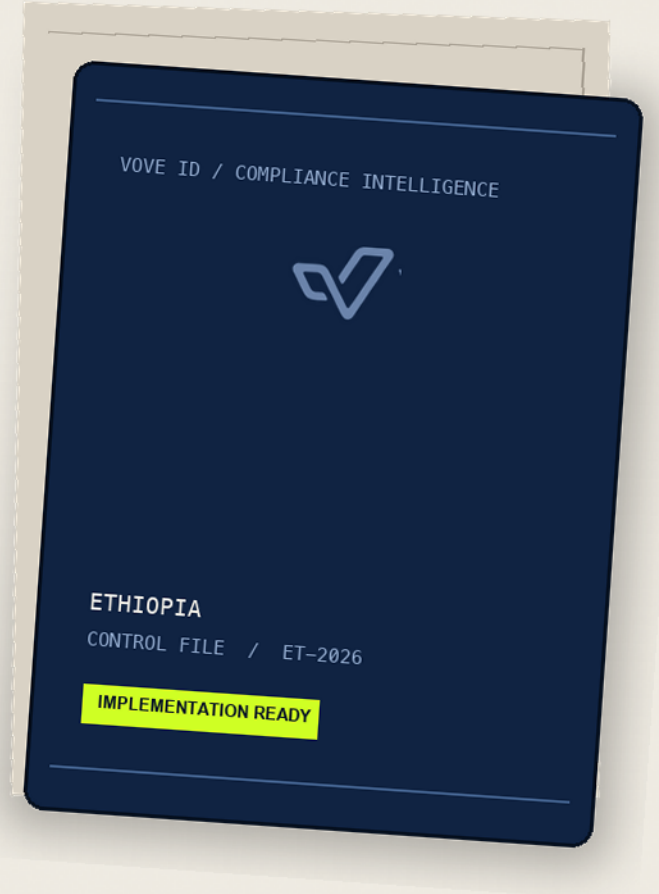
KYC / KYB / AML

2026 EDITION

ETHIOPIA



ETHIOPIA / ET



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Ethiopia KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for banks, microfinance institutions, payment instrument issuers, payment system operators, remittance providers and other reporting persons operating in Ethiopia. It translates Ethiopia's AML/CFT/CPF, banking, payment, foreign-exchange, company-registration, digital-ID and personal-data rules into controls, actions and audit evidence.

Primary AML law	**Proclamation No. 780/2013**
FIU	**Financial Intelligence Service (FIS)**
Financial supervisor	**National Bank of Ethiopia (NBE)**
Privacy authority	**Ethiopian Communications Authority (ECA)**
Financial-institution STR deadline	**No later than 24 hours**
AML record retention	**Minimum 10 years**
FATF status	**Not under increased monitoring**

Scope and legal framework

Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780/2013 and FIS AML/CFT CDD Directive No. 01/2014; Prevention and Suppression of Financing the Proliferation of Weapons of Mass Destruction Proclamation No. 1132/2019; Banking Business Proclamation No. 1360/2025; National Payment System Proclamation No. 718/2011, as amended by Proclamation No. 1282/2023, and NBE payment-system directives; Foreign Exchange Directive No. FXD/01/2024, as amended by FXD/3/2025, FXD/04/2026 and FXD/05/2026; Commercial Registration and Business Licensing Proclamation No. 980/2016, as amended by Proclamation No. 1150/2019; Commercial Code Proclamation No. 1243/2021; Personal Data Protection Proclamation No. 1321/2024; and Ethiopian Digital ID Proclamation No. 1284/2023.

FATF context

Ethiopia is not listed in FATF's 19 June 2026 statements on jurisdictions under increased monitoring or high-risk jurisdictions subject to a call for action. Ethiopia entered increased monitoring again in 2017 and FATF removed it from the monitoring process on 18 October 2019 after completion of its action plan. This status does not remove Ethiopian AML/CFT/CPF, targeted-financial-sanctions or risk-based enhanced-due-diligence duties.

IMPORTANT

This checklist is general information, not legal advice. It reflects official materials available on 15 July 2026. The stated financial-institution thresholds, 24-hour STR deadline and ten-year minimum retention period are drawn from Proclamation No. 780/2013 and FIS AML/CFT CDD Directive No. 01/2014. Confirm whether additional sector rules, later amendments, reporting formats or licence conditions apply to the entity and product with FIS, NBE, the Ethiopian Communications Authority and qualified Ethiopian 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.

1. CONFIRM SCOPE, REGULATOR AND LICENCE PERIMETER

Confirm scope, regulator and licence perimeter

Classify every entity, product and channel before launch. AML/CFT reporting-person status, NBE permission and ECA data-protection duties are separate questions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine reporting-person and supervisory status.	Map each Ethiopia-facing legal entity, branch, product, agent, merchant and outsourced function against Proclamation No. 780/2013 and the relevant FIS and NBE rules. Assign accountable owners for FIS reporting, prudential or payment supervision, foreign exchange and data protection.	Regulatory-perimeter memo; entity-product matrix; reporting-person classification; RACI.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014; NBE directive indexes
Apply Banking Business Proclamation No. 1360/2025 to banking activity.	Do not conduct banking business or present a fintech product as a bank without the licence and approvals required by the current Banking Business Proclamation. Map ownership, governance, management, outsourcing and product conditions to the NBE approval file.	NBE banking licence or legal perimeter analysis; approval correspondence; governance file; product-permission matrix.	Banking Business Proclamation No. 1360/2025
Distinguish payment-system operation from payment-instrument issuance.	Classify switching, clearing, settlement and other system-operation functions under PSO Directive ONPS/02/2020. Classify wallets, electronic money and other payment instruments under PII Directive ONPS/06/2022, as amended by ONPS/09/2023 and ONPS/10/2025. Obtain the permission applicable to each function before launch.	PSO/PII classification; NBE licence or authorisation; application file; current register check.	National Payment System Proclamation No. 718/2011, as amended; ONPS/02/2020; ONPS/06/2022; ONPS/09/2023; ONPS/10/2025; NBE payment-system directive index
Use authorised remittance and money-transfer arrangements.	Verify the current NBE status of every money-transfer operator, Ethiopian representative, settlement bank and corridor partner. Obtain NBE approval where required and do not treat a technology or agency agreement as a substitute for regulatory permission.	NBE MTA-list check; approval; partner due diligence; remittance agreement; funds-flow map.	NBE licensed money-transfer agents list; Foreign Exchange Directive No. FXD/01/2024, as amended

2. ESTABLISH RISK-BASED AML/CFT/CPF GOVERNANCE

Establish risk-based AML/CFT/CPF governance

The compliance programme should cover money laundering, terrorist financing and proliferation financing across customers, products, channels, agents, countries and technologies.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented enterprise risk assessment.	Assess customer, ownership, cash, remittance, agent, geography, product, channel, technology, sanctions and proliferation-financing exposure. Define inherent and residual risk, risk appetite, refresh cycles and event triggers.	Board-approved risk assessment; methodology; risk appetite; source inventory; change log.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014; Proclamation No. 1132/2019
Maintain written controls and an empowered compliance function.	Cover CDD, KYB, beneficial ownership, PEPs, sanctions, transaction monitoring, STR and cash reporting, wire transfers, records, agents, outsourcing, privacy, training and independent testing. Give compliance staff access, authority and a direct escalation route to senior management or the board.	Policy suite; appointments; committee terms; control library; board minutes.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Train personnel and relevant agents by role.	Provide initial and periodic training to directors, management, onboarding, operations, investigators, product, engineering, fraud, privacy and agent personnel. Test understanding of the 24-hour STR clock, confidentiality and no-tipping-off requirements.	Training curriculum; attendance; assessments; agent records; remediation log.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Assess new products and material changes before release.	Require AML/CFT/CPF, sanctions, fraud, privacy and operational-risk approval before deploying new wallet tiers, remote onboarding, APIs, biometric flows, agent models, payment corridors or material rules changes.	Pre-launch assessment; approvals; control acceptance; implementation plan.	FIS AML/CFT CDD Directive No. 01/2014; applicable NBE payment directives; Proclamation No. 1321/2024

3. IDENTIFY AND VERIFY INDIVIDUAL CUSTOMERS

Identify and verify individual customers

Financial institutions must apply CDD at relationship and specified occasional-transaction triggers, as well as whenever suspicion arises or prior identity data are doubtful.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and independently verify each customer and representative.	Collect the prescribed identity, address or contact and identity-document information; verify it using reliable and independent documents, data or information; and verify the authority of anyone acting for the customer.	CDD record; verification response; source document; representative mandate; timestamp and reviewer.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Apply financial-institution CDD to occasional cash transactions exceeding ETB 300,000 or USD 15,000.	Block completion of a single or linked occasional cash transaction above the applicable ETB 300,000 or USD 15,000 threshold until required CDD is complete. Aggregate linked transactions and apply CDD irrespective of value where suspicion or identity-data doubt exists.	Threshold configuration; linked-transaction logic; CDD record; blocked-case log; legal-source register.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Apply the ETB 20,000 or USD 1,000 wire-transfer threshold.	Configure originator and beneficiary information, verification and record controls for wire transfers at or above ETB 20,000 or USD 1,000, while applying any broader relationship, suspicion and payment-system requirements that operate regardless of value.	Wire-rule configuration; message fields; verification record; exception and rejection logs.	FIS AML/CFT CDD Directive No. 01/2014
Understand purpose, expected activity and source-of-funds context.	Record the relationship purpose, expected transaction size and frequency, counterparties, channels, geographies and source of funds. Establish a documented risk rating and monitoring baseline and keep it current.	Customer profile; expected-activity baseline; source-of-funds information; risk score; approval.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Do not proceed when required CDD cannot be completed.	Do not open the relationship or perform the transaction; for an existing relationship, terminate it in accordance with law and controlled exit procedures. Consider whether the failed or evasive CDD gives rise to an STR and preserve the no-tipping-off boundary.	CDD-failure case; blocked or closure record; STR consideration; approval and communication controls.	FIS AML/CFT CDD Directive No. 01/2014

4. VERIFY BUSINESSES, BENEFICIAL OWNERSHIP AND CONTROL

Verify businesses, beneficial ownership and control

KYB should establish legal existence, authority, ownership and the natural persons who ultimately own or control a customer. Registry evidence does not replace a complete beneficial-owner inquiry.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal identity, registration, licence and authority.	Obtain current commercial-registration and business-licence information, constitutional documents, tax or sector identifiers, registered and operating addresses, directors and signing powers from reliable sources.	Registry extract; business licence; constitutional documents; tax record; board authority; independent checks.	Commercial Registration and Business Licensing Proclamation No. 980/2016, as amended by No. 1150/2019; Commercial Code Proclamation No. 1243/2021; FIS AML/CFT CDD Directive No. 01/2014
Identify and verify every relevant natural-person beneficial owner.	Build the ownership and control chain through all legal entities and arrangements. Resolve natural persons with controlling ownership or control by other means and use any permitted senior-manager fallback only after documenting why no natural person could be identified through the preceding tests.	Ownership chart; shareholder and control records; verified BO files; control analysis; fallback rationale.	Proclamation No. 780/2013, art. 5; FIS AML/CFT CDD Directive No. 01/2014
Obtain and maintain current legal-person beneficial-owner information.	Require the customer to provide accurate and current legal-person and beneficial-owner data, reconcile it with available official and independent information, and resolve material discrepancies before onboarding or continuation.	BO declaration; registry reconciliation; discrepancy case; customer clarification; decision record.	Proclamation No. 780/2013, art. 5; FIS AML/CFT CDD Directive No. 01/2014; Proclamation No. 980/2016 as amended; Commercial Code No. 1243/2021
Refresh KYB and beneficial ownership on risk and event triggers.	Re-verify after ownership, control, director, licence, legal-form, address, activity, sanctions or adverse-information changes and at risk-based intervals. Contractually require prompt notice of material changes.	Refresh schedule; customer terms; change alerts; re-verification file; overdue report.	Proclamation No. 780/2013, art. 5; FIS AML/CFT CDD Directive No. 01/2014

5. APPLY PEP AND ENHANCED DUE DILIGENCE CONTROLS

Apply PEP and enhanced due diligence controls

Every identified PEP relationship requires the prescribed enhanced measures; the controls are not optional merely because an internal score is otherwise low.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify PEPs, relevant family members and close associates.	Screen customers, beneficial owners, controllers and relevant representatives at onboarding and throughout the relationship for domestic, foreign and international-organisation PEP exposure. Investigate and document potential matches.	PEP-screening configuration; match disposition; relationship analysis; rescreening log.	FIS AML/CFT CDD Directive No. 01/2014
Obtain senior-management approval for every identified PEP relationship.	Do not establish or continue an identified PEP relationship without recorded approval from the required level of senior management. Re-escalate material changes and newly identified PEP status.	EDD case; senior approval; decision rationale; event-driven reapproval.	FIS AML/CFT CDD Directive No. 01/2014
Establish source of wealth and source of funds for every identified PEP relationship.	Obtain and corroborate information explaining the PEP's accumulated wealth and the funds used in the relationship or transaction. Resolve unexplained inconsistencies before proceeding.	Source-of-wealth analysis; source-of-funds evidence; corroboration; exception decision.	FIS AML/CFT CDD Directive No. 01/2014
Apply enhanced ongoing monitoring to every identified PEP relationship.	Set increased review frequency, lower escalation tolerance and focused transaction monitoring proportionate to the relationship, while retaining all mandatory PEP measures.	Enhanced monitoring plan; scenario assignment; periodic review; investigation outcomes.	FIS AML/CFT CDD Directive No. 01/2014

6. MONITOR TRANSACTIONS AND MAKE FIS REPORTS

Monitor transactions and make FIS reports

Financial institutions should compare activity with the customer profile, investigate unusual activity and file required reports through the FIS-prescribed channel within the legal deadline.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor customers and transactions continuously.	Use risk-based scenarios for unusual size, frequency, velocity, cash, linked transactions, counterparties, geography, rapid movement, agent behaviour and activity inconsistent with the expected profile.	Scenario inventory; tuning rationale; alerts; investigations; quality-assurance results.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
File an STR no later than 24 hours after suspicion is formed.	Start the controlled reporting clock when facts meet the applicable suspicion standard, obtain required internal review without delaying the legal deadline, and submit through the FIS-prescribed channel no later than 24 hours. Protect confidentiality and prohibit tipping off.	Restricted STR case; suspicion timestamp; approval trail; FIS receipt; access log.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Report cash transactions above ETB 300,000 or USD 15,000.	Aggregate linked cash activity, generate the prescribed cash transaction report for amounts above ETB 300,000 or USD 15,000, submit it through the current FIS process and reconcile accepted reports to source transactions. Cash reporting does not replace STR analysis.	Cash-threshold configuration; aggregation logic; report file; receipt; reconciliation; exception log.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Document unusual-activity analysis and reporting decisions.	Examine origin, destination, purpose, parties, beneficial ownership and source of funds. Record the facts, analysis, decision maker, report rationale and any enhanced monitoring or exit action whether or not an STR is filed.	Investigation narrative; supporting data; decision; reviewer sign-off; monitoring plan.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014

7. IMPLEMENT TARGETED FINANCIAL SANCTIONS AND CPF CONTROLS

Implement targeted financial sanctions and CPF controls

Sanctions controls should address terrorism and proliferation financing and be capable of identifying, freezing and reporting relevant assets without making them available to designated persons.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen customers, beneficial owners and transactions against applicable designations.	Screen at onboarding, on list updates and before relevant transactions. Include aliases, identifiers, ownership and control, representatives, counterparties and payment data.	List inventory; screening configuration; update logs; test results; match files.	Proclamation No. 780/2013; Proclamation No. 1132/2019; FIS freezing procedures
Apply WMD proliferation-financing freezing requirements.	Implement Proclamation No. 1132/2019 and the applicable freezing order in sanctions governance and transaction interdiction. Prevent release or availability of property subject to a proliferation-financing freeze and follow the prescribed reporting and competent-authority process.	CPF procedure; current designation sources; freeze and reject workflow; notification records; legal escalation.	Prevention and Suppression of Financing the Proliferation of Weapons of Mass Destruction Proclamation No. 1132/2019 and applicable freezing order
Investigate ownership and control before clearing a potential match.	Do not clear a match solely because the named customer differs from the designated person. Assess direct and indirect ownership, control, agents, counterparties and available identifiers and obtain legal escalation where required.	Match investigation; ownership analysis; disposition approval; audit trail.	Proclamation No. 1132/2019; FIS freezing procedures
Test sanctions and CPF controls independently.	Test list ingestion, fuzzy matching, ownership scenarios, payment interdiction, freeze and report workflows, access restrictions and release controls. Track defects to closure.	Test scripts; results; issue register; remediation and retest evidence.	Proclamation No. 1132/2019; Proclamation No. 780/2013

8. CONTROL PAYMENTS, WALLETS, AGENTS AND REMITTANCES

Control payments, wallets, agents and remittances

Payment businesses require both AML/CFT controls and the NBE permission, safeguarding, operational, security and consumer-protection framework applicable to their role.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Operate payment systems within ONPS/02/2020 permission.	For switching, clearing, settlement or other payment-system operation, map the operating model, governance, security, business continuity, outsourcing and reporting controls to the PSO licence and current conditions.	PSO licence; approved service map; operating manual; continuity tests; NBE correspondence.	PSO Directive ONPS/02/2020; National Payment System Proclamation No. 718/2011, as amended
Issue payment instruments within ONPS/06/2022, as amended by ONPS/09/2023 and ONPS/10/2025.	For wallets, electronic money and other payment instruments, implement current customer tiers, limits, safeguarding, governance, agent, security and reporting controls. Do not use the older joint PSO/PII framework as the current permission matrix.	PII licence; current directive matrix; product configuration; safeguarding reconciliation; NBE filings.	PII Directive ONPS/06/2022; Amendment Directives ONPS/09/2023 and ONPS/10/2025; NBE payment-system directive index
Apply KYC, KYB and monitoring to customers, merchants, agents and walk-in users.	Verify each party under the applicable FIS and NBE rules, enforce current product limits, aggregate linked activity, monitor agent and merchant behaviour and investigate structuring or misuse.	CDD/KYB files; current limit register; agent and merchant monitoring; investigations.	FIS AML/CFT CDD Directive No. 01/2014; ONPS/02/2020; ONPS/06/2022; ONPS/09/2023; ONPS/10/2025
Use current NBE-listed money-transfer partners.	Check the NBE MTA list before onboarding and periodically thereafter, verify each partner's permitted role and corridors, and suspend flows if authorisation lapses or no longer covers the service.	Dated MTA-list check; partner file; corridor matrix; periodic recertification; suspension procedure.	NBE licensed money-transfer agents list; FXD/01/2024 as amended

9. APPLY THE COMPLETE FOREIGN-EXCHANGE AMENDMENT CHAIN

Apply the complete foreign-exchange amendment chain

Foreign-exchange controls must be based on FXD/01/2024 together with all subsequent amendments, not on a single amendment or an outdated bank practice.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Use FXD/01/2024 as the consolidated baseline.	Map foreign-currency accounts, authorised dealers and bureaus, remittances, imports, exports, service payments, capital transactions and documentary requirements to the July 2024 market-based FX framework.	FX perimeter memo; product and transaction matrix; authorised-counterparty checks; baseline legal register.	Foreign Exchange Directive No. FXD/01/2024
Implement FXD/3/2025's operational relaxations and pricing changes.	Update travel and cash-purchase allowances, foreign-currency debit-card utilisation and applicable bank FX fee controls introduced in May 2025. Preserve evidence for customer eligibility, purpose, amount, pricing and the authorised-bank process.	FXD/3/2025 change assessment; customer rules; fee configuration; transaction sample; staff communication.	Foreign Exchange Directive No. FXD/3/2025; NBE Foreign Exchange Market Measures, May 2025
Implement FXD/04/2026's broader account, payment and market relaxations.	Update controls for service-export retention, foreign-currency accounts and cards, documented family service payments, outbound investment approvals, inbound currency treatment, private external-loan guarantees, dividend repatriation, forex-bureau operations and other amended permissions. Retain documentary checks and NBE approval where the amendment still requires it.	FXD/04/2026 change assessment; account and payment rules; approval matrix; forex-bureau controls; implementation evidence.	Foreign Exchange Directive No. FXD/04/2026
Implement FXD/05/2026 trade-payment changes without removing document verification.	Allow authorised banks to approve letters of credit and cash against documents on acceptance for qualifying foreign-currency and retention-account holders without prior NBE approval. Permit shipment initiation before bank approval where allowed, but process payment only after submission and verification of required documents.	FXD/05/2026 change assessment; LC/CAD workflow; account eligibility; document checklist; bank approval and payment trail.	Foreign Exchange Directive No. FXD/05/2026, sections 3.1-3.4
Monitor FX and remittance flows for AML/CFT and sanctions risk.	Detect transaction splitting, unsupported source of funds, unusual beneficiaries, cash conversion, agent concentration, trade-document inconsistency and activity outside the stated purpose. Escalate suspicion to the FIS reporting process within the applicable deadline.	FX scenarios; reconciliation; alerts; investigation; STR decision and timing record.	FXD/01/2024 as amended; Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014

10. RETAIN RECORDS AND SUPPORT AUDIT AND AUTHORITY ACCESS

Retain records and support audit and authority access

Financial institutions must preserve CDD, transaction and correspondence records for at least ten years in a form that supports reconstruction, supervision and investigation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain CDD and customer-account records for at least 10 years.	Preserve identity and verification data, customer profiles, KYB and beneficial-owner records, authority records and risk assessments for the minimum ten-year period measured from the applicable relationship or account trigger under the controlling rule.	Retention matrix; lifecycle configuration; sampled files; deletion controls; legal-hold process.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Retain transaction records and business correspondence for at least 10 years.	Store transaction identifiers, parties, amounts, currencies, dates, channels, wire data, source documents and relevant correspondence for at least ten years and in enough detail to reconstruct individual transactions.	Data dictionary; archived records; reconstruction test; retrieval log; destruction record.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014
Preserve investigation, STR, cash-reporting and sanctions evidence securely.	Keep alert analysis, decisions, reports, submission receipts, freeze actions and access logs in restricted systems. Apply legal holds and longer sector retention where required.	Restricted case archive; receipts; access review; legal-hold register; retrieval test.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014; Proclamation No. 1132/2019
Test control operation and remediate findings.	Perform compliance monitoring and independent audit over onboarding, PEPs, sanctions, transaction reporting, payment partners, FX, retention and privacy. Report significant issues to senior management or the board and verify closure.	Monitoring plan; audit reports; issue register; remediation; board dashboard.	Proclamation No. 780/2013; FIS AML/CFT CDD Directive No. 01/2014; applicable NBE directives

11. PROTECT PERSONAL AND BIOMETRIC DATA

Protect personal and biometric data

The Ethiopian Communications Authority administers the 2024 personal-data framework. KYC, monitoring and biometric workflows should satisfy registration, governance, security, localisation, transfer and breach duties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Register controllers and processors with the Ethiopian Communications Authority.	Determine the registration status required for each entity and processing role, submit the prescribed information and maintain current registration details as processing, contact or organisational information changes.	ECA registration; renewal or update record; controller-processor inventory; responsibility matrix.	Personal Data Protection Proclamation No. 1321/2024
Appoint a data protection officer when the statutory conditions apply.	Assess the nature, scale, monitoring and sensitive-data criteria that trigger a DPO. Where required, appoint an independent and adequately resourced DPO with access to senior management and publish or communicate the prescribed contact details.	DPO applicability assessment; appointment; mandate; conflict check; contact publication.	Personal Data Protection Proclamation No. 1321/2024
Maintain processing records and perform DPIAs for high-risk processing.	Inventory purposes, lawful bases, data categories, recipients, retention, security and transfers. Complete and approve a DPIA before high-risk biometric, large-scale monitoring, profiling, remote-onboarding or other processing identified by the proclamation or ECA.	Record of processing; lawful-basis analysis; DPIA; risk treatment; approval and review log.	Personal Data Protection Proclamation No. 1321/2024
Store personal data in Ethiopia as required and control transfers.	Map hosting, backups, support access and onward transfers. Use Ethiopian storage in accordance with the proclamation and obtain prior ECA approval before transferring sensitive personal data outside Ethiopia; document all other transfer conditions and safeguards.	Hosting architecture; data-location inventory; transfer assessment; ECA approval; vendor terms.	Personal Data Protection Proclamation No. 1321/2024
Notify qualifying breaches within 72 hours.	Detect, contain and assess incidents promptly. Notify the Ethiopian Communications Authority and affected data subjects within 72 hours where the proclamation requires notification, documenting content, timing, risk, delay reasons and remediation.	Incident plan; breach register; 72-hour timeline; ECA notice; data-subject communication; post-incident review.	Personal Data Protection Proclamation No. 1321/2024
Apply heightened controls to sensitive and biometric data.	Minimise collection, establish a valid legal condition, encrypt and segregate data, restrict access, test vendors and preserve an accessible alternative where appropriate. Fayda identity proofing does not remove financial-sector CDD or privacy duties.	Sensitive-data assessment; biometric policy; access logs; encryption design; vendor review; fallback process.	Personal Data Protection Proclamation No. 1321/2024; Ethiopian Digital ID Proclamation No. 1284/2023

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.

Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780/2013
National Bank of Ethiopia · Primary legislation
Open official source

AML/CFT CDD Directive No. 01/2014
Financial Intelligence Service · Primary directive
Open official source

Financial Intelligence Service resource library
Financial Intelligence Service · Official AML/CFT resources
Open official source

Banking Business Proclamation No. 1360/2025
National Bank of Ethiopia · Primary legislation
Open official source

National Payment System directives
National Bank of Ethiopia · Official directives index
Open official source

Payment System Operator Directive ONPS/02/2020
National Bank of Ethiopia · Primary regulation
Open official source

Payment Instrument Issuer Directive ONPS/06/2022
National Bank of Ethiopia · Primary regulation
Open official source

Payment Instrument Issuer Amendment Directives ONPS/09/2023 and ONPS/10/2025
National Bank of Ethiopia · Primary regulations
Open official source

Licensed money-transfer agents
National Bank of Ethiopia · Official register
Open official source

Commercial Registration and Business Licensing Proclamation No. 980/2016 as amended by No. 1150/2019, and Commercial Code No. 1243/2021
Ethiopian Ministry of Justice · Primary legislation collection
Open official source

Foreign Exchange Directive No. FXD/01/2024
National Bank of Ethiopia · Primary regulation
Open official source

Foreign Exchange Directive No. FXD/3/2025
National Bank of Ethiopia · Primary regulation
Open official source

Foreign Exchange Directive No. FXD/04/2026 - Amendment to Foreign Exchange Directive No. FXD/01/2024
National Bank of Ethiopia · Primary regulation
Open official source

Foreign Exchange Directive No. FXD/05/2026
National Bank of Ethiopia · Primary regulation
Open official source

Foreign Exchange Management directive index
National Bank of Ethiopia · Official directives index
Open official source

Personal Data Protection Proclamation No. 1321/2024
Ethiopian Communications Authority · Primary legislation
Open official source

Ethiopian Digital ID Proclamation No. 1284/2023 and Fayda information
National ID Program · Primary framework and official programme information
Open official source

Prevention and Suppression of Financing the Proliferation of Weapons of Mass Destruction Proclamation No. 1132/2019
Federal Justice and Law Institute · Primary legislation
Open official source

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

FATF high-risk jurisdictions subject to a call for action, 19 June 2026
FATF · Official FATF statement
Open official source

FATF statement removing Ethiopia from increased monitoring, 18 October 2019
FATF · Official FATF statement
Open official source

Document control

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

This checklist is general information, not legal advice. It reflects official materials available on 15 July 2026. The stated financial-institution thresholds, 24-hour STR deadline and ten-year minimum retention period are drawn from Proclamation No. 780/2013 and FIS AML/CFT CDD Directive No. 01/2014. Confirm whether additional sector rules, later amendments, reporting formats or licence conditions apply to the entity and product with FIS, NBE, the Ethiopian Communications Authority and qualified Ethiopian counsel before launch.