VOVE ID

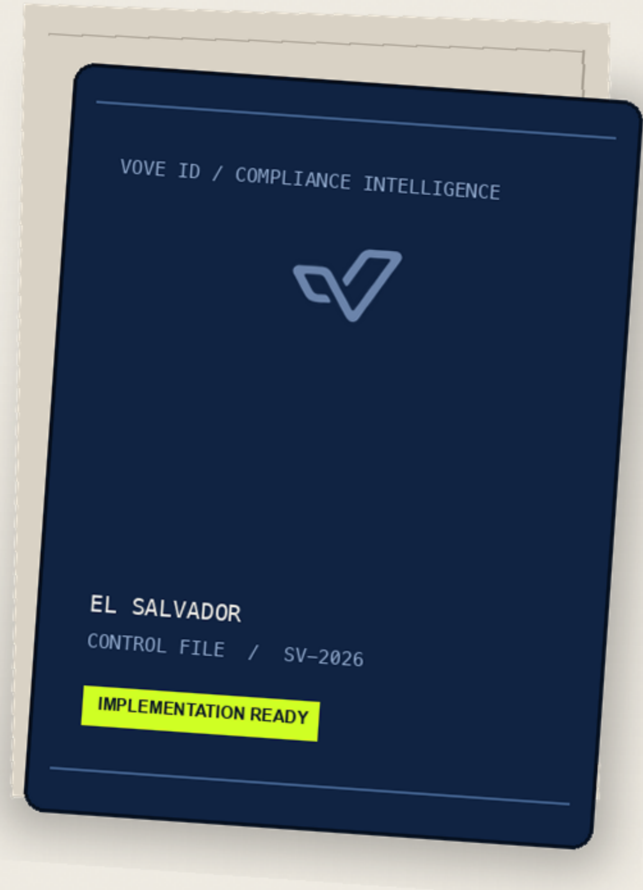
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

EL SALVADOR

EL SALVADOR / SV



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

El Salvador KYC, KYB & AML Compliance Checklist

An implementation-focused checklist for El Salvador's AML/CFT/CPF framework under the special law effective 24 October 2025, including UIF reporting, sector supervision, beneficial ownership, targeted financial sanctions, personal-data protection and digital-asset services.

National FIU	**Unidad de Investigación Financiera (UIF), an autonomous specialist office attached to the Fiscalía General de la República**
Primary AML rule	**Decree 426 special AML/CFT/CPF law, effective 24 October 2025**
Suspicion reporting	**Analyze within up to 15 business days; report to UIF within 24 hours after a suspicious determination**
Regulated reports	**Report covered linked transactions within 5 business days; transitional thresholds require current-instrument confirmation**
Beneficial owner	**Natural person with at least 25% ownership or voting rights, or control by other means**
Retention	**At least 15 years: transaction completion or relationship/account termination, depending on the record**
Privacy authority	**Agencia de Ciberseguridad del Estado (ACE)**
FATF status	**GAFILAT member; absent from FATF June 2026 public lists as reviewed 6 August 2026**

Scope and legal framework

The Special Law for the Prevention, Control and Sanction of Money Laundering, Terrorist Financing and Proliferation Financing (Decree 426) has applied since 24 October 2025 and repealed the 1998 AML law. Its article 61 preserves the former regulation and UIF instruction only until replacement instruments are issued. Sector laws, the Special Law Against Acts of Terrorism, the Digital Assets Issuance Law and the Personal Data Protection Law provide additional layers.

FATF context

El Salvador is a GAFILAT member. Its 2024 mutual evaluation was adopted in August 2024. As reviewed on 6 August 2026, El Salvador was not named in FATF's June 2026 statements on high-risk jurisdictions subject to a call for action or jurisdictions under increased monitoring. This status is time-sensitive and does not replace customer, product, transaction or geographic risk assessment.

IMPORTANT	General regulatory information, not legal advice, a licence determination or a substitute for the operative Spanish texts and current supervisor instructions. Reviewed 6 August 2026. Confirm whether replacement regulations or UIF instructions have been issued, the applicable sector reporting parameters, registry access, sanctions escalation route, privacy guidance and licensing perimeter with the UIF, relevant supervisor and qualified Salvadoran counsel before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

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

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

Checklist legend

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

Minimum review record

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

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

1. SCOPE, AUTHORITIES, AND LICENSING

Scope, authorities, and licensing

Map the business to Decree 426's closed subject categories and the applicable sector supervisor before onboarding.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether the entity is a subject obliged under the new special law.	Map each product and legal entity to article 7, including financial institutions, specified lenders, DNFBPs, money/value transport, digital-asset or bitcoin providers and political parties; document any out-of-scope conclusion.	Perimeter memorandum, product map, legal-entity chart and counsel confirmation.	Decree 426 arts. 1, 7-9
Identify the competent supervisor and complete required registrations or authorisations.	Confirm SSF, Superintendencia de Obligaciones Mercantiles, CNAD or other article 11-12 supervision; separately test financial, payments, bitcoin and digital-asset licensing before launch.	Supervisor mapping, licence analysis, registrations, approvals and correspondence.	Decree 426 arts. 11-13; Digital Assets Issuance Law arts. 18-20
Treat the regulation and UIF instruction as a controlled transition.	At launch and each rules refresh, verify whether the preserved 2000 regulation and current UIF instruction have been replaced under the 2025 law; apply only provisions that do not conflict with Decree 426.	Dated legal-update check, downloaded instruments and conflict analysis.	Decree 426 arts. 55-62; UIF current-law FAQ

Governance and risk assessment

Controls must be proportionate to identified AML/CFT/CPF risk and avoid unsupported blanket exclusion.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Operate a documented risk-based AML/CFT/CPF system.	Assess customer, product, channel, transaction and geographic risks; set simplified, standard or enhanced controls and obtain governance approval.	Enterprise risk assessment, methodology, risk appetite, control matrix and approval minutes.	Decree 426 arts. 9, 13, 15-17
Appoint the required compliance function and deputies.	For SSF-, CNAD- and article 7(2)-supervised entities establish a compliance office with principal and alternate; other supervised entities must appoint a principal and alternate unless a statutory exception applies.	Board resolutions, role profiles, independence record, UIF/supervisor filings and training evidence.	Decree 426 arts. 20-22
Create the prevention committee when a compliance office is mandatory.	Maintain a committee of at least three members, including one member of the highest governing body and the compliance officer, with recorded decisions.	Committee charter, appointments, meeting book and action log.	Decree 426 art. 23

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Identification and verification must be risk-based, reconstructable and completed for the relationship and relevant occasional activity.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify the customer and any representative.	Collect authoritative identity data, verify the document and person, validate authority for representatives, screen, risk-rate and record purpose before activation.	Identity evidence, liveness or equivalent checks, authority document, screening log and onboarding decision.	Decree 426 art. 15
Apply CDD at statutory trigger points.	Perform CDD when establishing a relationship, for occasional transactions above the applicable cash-report threshold, on suspicion, or when prior identity data is doubtful; obtain current sector thresholds before deployment.	Trigger matrix, transaction evidence, refresh record and escalation log.	Decree 426 art. 15
Do not maintain anonymous or coded relationships.	Require nominative customer records and block product activation where required identity evidence is not provided; consider a suspicious-attempt report after analysis.	Account configuration, rejection record and documented reporting decision.	Decree 426 art. 15

KYB, registries, and beneficial ownership

Company verification must combine registry evidence with independent ownership-and-control analysis.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal existence, representatives, activity and powers.	Obtain a current CNR Registro de Comercio certification or equivalent source, constitutive documents, tax details, business address and authority chain; independently verify material facts.	Registry certification, formation documents, tax evidence, address check and authority map.	Decree 426 art. 15; Commercial Code; CNR Registro de Comercio
Identify natural persons meeting the statutory beneficial-owner test.	Trace direct and indirect ownership and voting rights to every natural person at or above 25%, and identify any natural person exercising control by other means.	Ownership chart, cap table, registry documents, shareholder evidence and control analysis.	Decree 426 art. 15
Apply the listed-company exception narrowly.	Use the exception only where the client or owner has at least 25% in a listed commercial company subject to market disclosure requirements; document the market and disclosure basis.	Listing evidence, disclosure-rule analysis and approval.	Decree 426 art. 15
Do not treat registry access as proof of a comprehensive public BO register.	Use CNR company records as one input and obtain ownership/control evidence directly; confirm current beneficial-ownership filing and access arrangements with CNR and the supervisor.	CNR search, certified extracts, customer declaration, corroboration and uncertainty log.	CNR Registro de Comercio services; controlled uncertainty

5. PEPS, EDD, AND REMOTE ONBOARDING

PEPs, EDD, and remote onboarding

High-risk relationships require verified source information and a documented, individualized decision.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify domestic, foreign and internatio nal-organisation PEPs.	Screen customers, beneficial owners, representatives and connected parties; continue PEP treatment for five years after the last appointment and apply enhanced diligence to specified family and close associates.	Screening results, position verification, relationship mapping and five-year control.	Decree 426 art. 19
Verify source of wealth and source of funds for high-risk customers.	Collect and corroborate wealth and funds evidence proportionate to risk and obtain the required senior approval before activation or continuation.	Source dossier, corroboration, risk rationale, approval and monitoring plan.	Decree 426 arts. 15, 19; current UIF instruction
Make remote onboarding equivalent and auditable.	Use authoritative document validation, impersonation and liveness controls, device and channel signals, sanctions/PEP screening, step-up checks and manual exception review.	Vendor testing, model thresholds, session record, fraud results and exception approvals.	Decree 426 arts. 15-17; risk-based implementation control

Monitoring and suspicious reporting

Unusual activity must be analyzed promptly and reports sent confidentially through UIF-authorized channels.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor relationships and investigate unusual activity.	Calibrate scenarios to the risk assessment, preserve alert inputs, investigate context and document whether sufficient grounds for suspicion exist.	Scenario inventory, alert file, analyst workpaper, disposition and quality review.	Decree 426 arts. 9, 15, 24
Complete unusual-operation analysis within the statutory window.	Finish analysis within 15 business days of detection; request the single permitted equal extension from UIF through the compliance officer when justified.	Detection timestamp, case chronology, extension request and UIF response.	Decree 426 art. 24
Report suspicious, attempted and suspicious-activity cases to UIF.	After determining suspicion, submit the authorized report promptly and no later than 24 hours, regardless of amount, using the current UIF channel and format.	Decision timestamp, submitted report, receipt, supporting file and access log.	Decree 426 arts. 3-4, 24
Protect report confidentiality and prevent tipping off.	Restrict report and UIF-request access; do not disclose reports or related requests to customers, users, third parties, auditors or supervisors except as lawfully directed.	Restricted permissions, disclosure protocol, staff attestations and incident log.	Decree 426 arts. 24, 28

Payments, wires, thresholds, and digital assets

Threshold reporting and regulated financial or digital-asset activity require current parameter and licence checks.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report regulated transactions within five business days.	Aggregate transactions in one event or over a month where they appear linked, and report covered cash, other-means, local/international electronic-transfer and digital-asset transactions to UIF within five business days.	Aggregation logic, threshold table, report files, receipts and timeliness metrics.	Decree 426 art. 25
Confirm transitional thresholds before configuring production.	Reconcile Decree 426, any new regulation and the preserved UIF instruction. UIF's current FAQ states instruction thresholds above USD 10,000 cash, USD 25,000 other means and USD 1,000 electronic transfers; do not generalize them without sector confirmation.	Dated instrument set, supervisor confirmation, configuration approval and change log.	Decree 426 arts. 25, 61; UIF current-law FAQ
Preserve complete originator and beneficiary information for transfers.	Collect, validate, transmit and retain the fields required by the applicable BCR/SSF/UIF or CNAD instrument; pause or escalate incomplete transfers under the current sector rule.	Message fields, validation logs, exception queue and current-rule mapping.	Decree 426 arts. 15, 25-26; current sector instruments
Register digital-asset services with CNAD where the territorial and service tests apply.	Before offering article 19 digital-asset services from El Salvador or actively marketing them into the country, complete CNAD registration and confirm UIF obligations; separately analyze bitcoin services supervised by SSF.	Territorial analysis, CNAD registration, public-register check, UIF record and SSF analysis.	Digital Assets Issuance Law arts. 18-20; Decree 426 arts. 7, 12

Targeted financial sanctions

Screening must cover binding designations and produce an immediate, traceable escalation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen UN and applicable national designations continuously.	Screen customers, beneficial owners, representatives and transactions at onboarding, list change and before value movement using UIF-published access points.	List sources, update logs, screening results, match records and test evidence.	Special Law Against Acts of Terrorism art. 37; Decree 426 arts. 10, 32; UIF international-lists portal
Prevent dealing and freeze on a confirmed designation match without delay.	Stop transactions immediately, preserve assets and notify through the current UIF/FGR process; do not release funds without competent authority direction.	Match chronology, freeze record, report receipt, communications and release authority.	Special Law Against Acts of Terrorism art. 37; Decree 426 arts. 10, 32
Control false positives, delisting and exceptions.	Use a documented escalation that protects confidentiality and obtains UIF/FGR or judicial direction for unfreezing, delisting or permitted access; confirm live procedure before launch.	Escalation file, identity comparison, authority response and audit trail.	UIF sanctions guidance and exercises; controlled uncertainty

Records and regulator access

The 2025 law materially extends AML records to at least 15 years.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain reconstructable transaction records for at least 15 years.	Preserve domestic and international transaction records for at least 15 years from completion, sufficient to reconstruct each transaction and answer authority requests immediately.	Retention schedule, transaction archive, retrieval tests and deletion holds.	Decree 426 art. 26
Retain customer identification and account files for at least 15 years after exit.	Start the period at relationship termination or account closure; preserve legal holds and secure electronic accessibility.	Closure date, customer file archive, legal-hold record and retrieval test.	Decree 426 art. 26
Respond securely to UIF, supervisor, FGR and court requests.	Authenticate requests, preserve scope and chain of custody, meet the stated deadline and keep a restricted disclosure log.	Request register, authentication, production manifest and transmission receipt.	Decree 426 arts. 4, 26, 28, 52-53

Privacy, biometrics, and transfers

AML processing must also satisfy the Personal Data Protection Law and ACE policy, subject to lawful AML retention and disclosure duties.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document a lawful, transparent and minimized KYC processing design.	Map each data element and purpose, provide required notices, identify the lawful basis, minimize collection and reconcile deletion rights with the 15-year AML retention duty.	Processing register, privacy notice, purpose/basis matrix, retention reconciliation and rights procedure.	Personal Data Protection Law arts. 5 and 24; Decree 426 art. 26
Apply enhanced safeguards to sensitive and biometric data.	Complete an impact assessment, restrict access, encrypt data, test biometric vendors and document necessity, proportionality and fallback paths.	Impact assessment, security design, vendor diligence, test results and access logs.	Personal Data Protection Law; ACE Policies 001-0309025-DPDP arts. 3-6
Prepare breach notification and response workflows.	Detect, contain and assess incidents and maintain a workflow capable of notifying ACE, FGR and affected individuals within 72 hours where the ACE policy requires it.	Incident plan, severity assessment, decision log, notifications and post-incident review.	ACE Policies 001-0309025-DPDP art. 4
Control processors and international transfers.	Contract for confidentiality, security, auditability and deletion; assess equivalent protection for international transfers and preserve a current data-flow map.	Processor contracts, transfer assessment, country map, encryption evidence and approval.	Personal Data Protection Law; ACE Policies 001-0309025-DPDP art. 4

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Evidence should enable independent reconstruction of onboarding, monitoring, reporting and governance decisions.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain one indexed file per customer or legal entity.	Link identity, KYB, beneficial ownership, screening, risk, approvals, monitoring, refreshes, source evidence and exit decisions under immutable identifiers.	Evidence index, version history, access history and sample reconstruction test.	Decree 426 arts. 15, 19, 26
Test data, screening, reporting and retention controls.	Run periodic samples and scenario tests covering identity, 25% and control BO logic, PEP duration, threshold aggregation, ROS clocks, sanctions and 15-year retention.	Test plan, samples, defects, remediation owners and closure proof.	Decree 426 arts. 13, 15, 19, 24-26
Operate a dated legal-change control.	Before launch and periodically thereafter check UIF, SSF, BCR, CNAD, CNR, ACE, FATF and GAFILAT sources; route changes into policy, rules, training and customer remediation.	Source register, legal-change log, impact assessment and deployment record.	Decree 426 arts. 55-61; risk-based implementation control

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.

Special AML/CFT/CPF Law - Decree 426
Unidad de Investigación Financiera · Primary legislation
Open official source

Current-law frequently asked questions
Unidad de Investigación Financiera · Official current guidance
Open official source

UIF instructions and guides
Unidad de Investigación Financiera · Official guidance portal
Open official source

International sanctions lists portal
Unidad de Investigación Financiera · Official sanctions guidance
Open official source

El Salvador 2024 mutual evaluation
FATF / GAFILAT · Authoritative mutual evaluation
Open official source

FATF high-risk jurisdictions - June 2026
Financial Action Task Force · Authoritative current-status statement
Open official source

FATF jurisdictions under increased monitoring - June 2026
Financial Action Task Force · Authoritative current-status statement
Open official source

Registro de Comercio services
Centro Nacional de Registros · Official company registry portal
Open official source

Personal Data Protection Law - Decree 144
Asamblea Legislativa · Primary legislation
Open official source

ACE personal-data handling policies
Agencia de Ciberseguridad del Estado · Official privacy guidance
Open official source

Digital Assets Issuance Law with reforms
Comisión Nacional de Activos Digitales · Primary legislation
Open official source

Digital-asset service-provider registration
Comisión Nacional de Activos Digitales · Official licensing guidance
Open official source

Document control

Version 1.0 / Published 6 August 2026 / Last reviewed 6 August 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice, a licence determination or a substitute for the operative Spanish texts and current supervisor instructions. Reviewed 6 August 2026. Confirm whether replacement regulations or UIF instructions have been issued, the applicable sector reporting parameters, registry access, sanctions escalation route, privacy guidance and licensing perimeter with the UIF, relevant supervisor and qualified Salvadoran counsel before launch.