VOVE ID

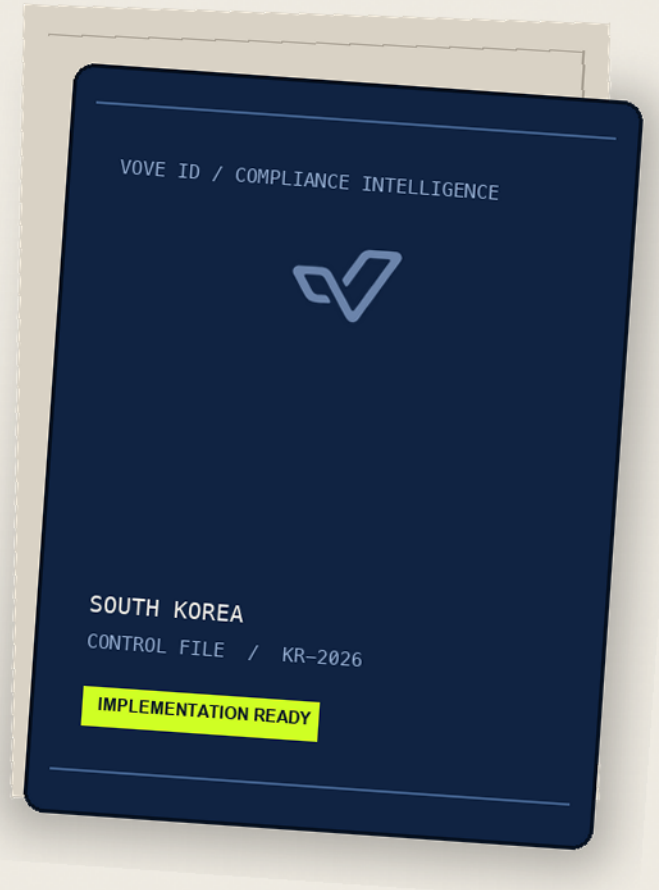
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

SOUTH KOREA

SOUTH KOREA / KR



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

South Korea KYC, KYB & AML Compliance Checklist

An implementation checklist for the Republic of Korea's financial-sector customer due diligence, beneficial ownership, suspicious and cash reporting, targeted financial sanctions, payments, virtual assets and privacy requirements.

FIU	**Korea Financial Intelligence Unit (KoFIU)**
Primary AML law	**Act on Reporting and Using Specified Financial Transaction Information (FTRA), as in force**
STR timing	**Without delay after reasonable grounds for suspicion arise**
Cash threshold report	**KRW 10 million or more paid or received in cash, aggregated separately per trading day and same real name, subject to statutory exclusions**
AML retention	**Five years from termination of the relevant financial-transaction relationship, using the statutory termination event**
AML beneficial owner	**25% voting ownership first, then largest holder or other control, then the representative as fallback**
Privacy authority	**Personal Information Protection Commission (PIPC)**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Act on Reporting and Using Specified Financial Transaction Information (Financial Transaction Reports Act or FTRA), its Enforcement Decree and KoFIU regulations govern covered financial companies, casinos and virtual asset service providers. The Act on Real Name Financial Transactions and Guarantee of Secrecy supports real-name verification. The AML perimeter is sector-specific and should not be treated as a universal obligation on every Korean business or professional.

FATF context

The Republic of Korea was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. FATF's October 2024 follow-up rated Korea compliant on 13 Recommendations, largely compliant on 20 and partially compliant on 7; its next reporting is in the fifth-round mutual evaluation. Absence from a public list is not a low-risk classification.

IMPORTANT

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 25 September 2026. Confirm the entity-specific FTRA perimeter, current KoFIU regulations and forms, sector licence, VASP transition dates, sanctions notices, privacy basis and any Korean-language source text with the competent authority and qualified Korean 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 exact regulated activity and supervisor before applying this financial-sector checklist.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether the entity is a financial company or other reporting entity within the FTRA.	Map each banking, securities, insurance, cooperative, casino, electronic-finance, remittance and virtual-asset activity against the current FTRA and Enforcement Decree; document exclusions and the responsible sector supervisor.	Legal-entity chart, product and funds-flow inventory, perimeter memo, licence register and counsel confirmation.	FTRA Articles 2 and 15; FTRA Enforcement Decree Articles 2 and 15
Do not apply the financial-sector AML perimeter as a universal business rule.	For lawyers, accountants, real-estate businesses, dealers and other professionals, identify any separate sector duty and avoid describing them as FTRA reporting entities without a current legal basis.	Sector-by-sector applicability matrix, statutory sources and approved customer-scope decision.	FTRA Article 2; FATF Korea Follow-Up Report 2024, Recommendations 22, 23 and 28
Obtain each required payments or electronic-finance permission or registration before service.	Classify electronic currency, electronic funds transfer, debit, prepaid and payment-gateway services under the Electronic Financial Transactions Act and complete Financial Services Commission permission or registration unless a documented exemption applies.	Service classification, application, approval or registration, exemption analysis, conditions and change log.	Electronic Financial Transactions Act Articles 2 and 28
Register a covered virtual asset service provider with KoFIU.	File and maintain the FTRA registration, satisfy current information-security, real-name account where applicable, governance, systems, staffing, internal-control and fit-and-proper conditions, and track renewal and modification deadlines.	Perimeter analysis, registration acceptance, ISMS evidence, account evidence, governance pack, renewal calendar and change filings.	FTRA Articles 6-8; FTRA Enforcement Decree Articles 10-11 to 10-20, as amended effective 20 August 2026

2. GOVERNANCE AND ML/TF RISK MANAGEMENT

Governance and ML/TF risk management

Covered entities need accountable reporting, risk-based controls, training and independent evaluation.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Appoint the responsible reporting officer and maintain an internal reporting system.	Document appointment and dismissal, authority, escalation routes and access to KoFIU reporting channels; notify KoFIU where required.	Appointment record, notification, role description, delegation matrix and tested escalation workflow.	FTRA Article 5(1); FTRA Enforcement Decree Article 9
Maintain risk-based AML/CFT procedures and work guidelines.	Assess customer, product, channel, geography, transaction, new-technology and group risks and translate the results into proportionate CDD, monitoring, reporting and sanctions controls.	Risk methodology, current assessment, approved procedures, model inventory, change assessments and residual-risk decisions.	FTRA Article 5(1)-(4); FTRA Enforcement Decree Articles 4 and 9
Provide role-appropriate AML/CFT training and supervision.	Train relevant officers and employees at onboarding and periodically, test understanding, and supervise compliance with work guidelines.	Training content, attendance, assessment results, supervision reports and remediation records.	FTRA Article 5(1)3 and (4)
Independently evaluate the adequacy and effectiveness of the AML program.	Use a function independent from AML operations, set a risk-based scope and frequency, report findings to accountable management and verify closure.	Independence assessment, review plan, workpapers, report, management response and closure testing.	FTRA Article 5(3)2

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Real-name verification and FTRA CDD apply at relationship opening, scoped occasional-transaction thresholds and risk triggers.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Complete CDD when opening a new account or business relationship.	Identify and verify the customer's real name, address and contact information using reliable evidence before or at onboarding, subject only to a documented rule that permits later completion without delay.	Identity attributes, evidence source, verification result, timestamps, exception basis and completion record.	FTRA Article 5-2; FTRA Enforcement Decree Articles 10-2, 10-4 and 10-6; Act on Real Name Financial Transactions and Guarantee of Secrecy
Apply the correct occasional-transaction CDD threshold.	Trigger CDD at KRW 3 million for casino transactions, KRW 1 million equivalent for virtual-asset transactions, KRW 1 million equivalent for wire transfers, USD 10,000 equivalent for foreign-currency transactions, or KRW 10 million for other occasional financial transactions; do not treat one amount as universal.	Transaction classifier, aggregation logic where applicable, exchange-rate source, CDD trigger log and test cases.	FTRA Article 5-2(1)1; FTRA Enforcement Decree Article 10-3
Identify persons acting for a customer and verify their authority.	Collect the representative's identity, verify the mandate or corporate authority and link the person to the customer before accepting instructions.	Representative KYC, power of attorney or board authority, verification result and transaction audit trail.	FTRA Article 5-2; Financial Transaction Reports and Supervisory Regulation Article 38; KoFIU CDD guidance
Reject or terminate where required CDD cannot be completed.	Do not open the account or perform the new transaction when identity cannot be verified; terminate an existing relationship where the statutory condition applies and review whether an STR is required.	Information requests, refusal or termination decision, legal basis, customer communication and STR assessment.	FTRA Article 5-2(4)-(5)

KYB, registries, and beneficial ownership

Verify legal existence, representatives and the natural persons who ultimately own or control the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person or organization identity and existence.	Collect the real name, business type or establishment purpose, head-office and business locations, contact details and representative information; corroborate them with a current court commercial-register extract and other reliable documents.	Commercial-register extract, business registration, constitutional documents, representative verification and discrepancy log.	FTRA Enforcement Decree Article 10-4; Financial Transaction Reports and Supervisory Regulation Article 38; Commercial Act Article 34
Apply the statutory AML beneficial-owner cascade.	Identify the natural person holding at least 25% of issued voting shares or investment; if none can be identified, test the largest holder, appointment of a majority of management and other substantial control; if still none, identify the representative.	Layered ownership chart, voting and investment calculations, control analysis, identity verification and fallback rationale.	FTRA Article 5-2(1)1(b); FTRA Enforcement Decree Article 10-5(2)-(4)
Trace corporate owners to natural persons and resolve nominees or indirect control.	Look through each corporate layer, corroborate ownership and control independently, and escalate opaque or foreign structures rather than accepting the immediate shareholder as the beneficial owner.	Full chain, source extracts, shareholder registers, agreements, nominee analysis and enhanced review.	FTRA Enforcement Decree Article 10-5(3)-(4); KoFIU CDD guidance
Keep commercial-registration evidence separate from the AML beneficial-owner conclusion.	Use court registration and the company's shareholder register as KYB evidence, but perform the FTRA ownership-and-control test independently because basic or legal ownership evidence may not reveal ultimate control.	Registry extract, Commercial Act shareholder register, reconciliation and signed beneficial-owner determination.	Commercial Act Articles 34 and 352; FTRA Enforcement Decree Article 10-5; FATF Korea Mutual Evaluation 2020

PEPs, enhanced due diligence, and remote onboarding

Higher-risk customers require additional information and controls; Korea's PEP framework retains FATF-identified limitations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify foreign PEP exposure and apply the required enhanced measures.	Screen the customer and beneficial owner for foreign PEP, family-member and close-associate status; obtain required senior approval, establish source of wealth and source of funds, and increase monitoring under the current KoFIU regulation.	Screening result, relationship map, approval, source corroboration and monitoring plan.	Financial Transaction Reports and Supervisory Regulation; FATF Korea Follow-Up Report 2024, Recommendation 12
Treat domestic and international-organization PEP coverage as a controlled legal gap.	Apply risk-based screening and enhanced review as an internal control where not expressly required, and confirm sector-specific rules; do not state that Korean law fully implements every FATF PEP category.	Legal-gap memo, approved risk policy, screening scope and exception decisions.	FATF Korea Follow-Up Report 2024, Recommendation 12
Perform enhanced CDD where ML/TF risk is high or actual ownership is doubtful.	Obtain and verify additional information including transaction purpose and source of funds, investigate inconsistencies and impose risk-appropriate approval and monitoring.	Risk trigger, enhanced questionnaire, source evidence, approval and review schedule.	FTRA Article 5-2(1)2; KoFIU CDD guidance
Control non-face-to-face identity and biometric processing.	Layer document, device, liveness and fraud controls. Where biometrics uniquely identify a person, establish a valid PIPA basis, obtain separate consent when relied upon, give required notices and apply enhanced security and deletion controls.	Method assessment, fraud tests, PIPA basis, consent and notice records, security review, retention schedule and vendor diligence.	PIPA Articles 15, 23, 29 and 30; Enforcement Decree of PIPA Article 18; PIPC Biometric Information Protection Guideline

Monitoring and suspicious transaction reporting

Ongoing CDD and transaction monitoring must support prompt, confidential reporting to KoFIU.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing, risk-based CDD and transaction monitoring.	Review transactions against customer activity, business, risk and source-of-funds information; set refresh cycles by risk and reverify when information is inconsistent, doubtful or materially changed.	Scenario inventory, alerts, case decisions, periodic reviews, refreshed CDD and quality testing.	FTRA Article 5; FTRA Enforcement Decree Article 10-6; KoFIU CDD guidance
File an STR with KoFIU without delay when the statutory suspicion test is met.	Record when reasonable grounds arose, state the grounds clearly and submit using the current KoFIU-prescribed form and channel without waiting for proof or a monetary threshold.	Alert chronology, information reviewed, suspicion decision, STR, submission receipt and timeliness test.	FTRA Article 4(1) and (3); FTRA Enforcement Decree Article 7; KoFIU STR guidance
Consider an STR after failed CDD, rejection or termination.	Route every statutory CDD refusal or relationship termination to the reporting officer for a documented suspicion assessment and preserve the decision.	Failed-CDD case, escalation, STR decision, filing receipt if applicable and closure approval.	FTRA Article 5-2(4)-(5); KoFIU CDD guidance
Protect STR information and prevent tipping off.	Restrict knowledge of an intended or filed STR to authorized internal use and any express legal exception; block customer-facing notes or disclosures that reveal the report.	Access controls, disclosure log, communication review, training and incident response.	FTRA Article 4(6)

7. CASH REPORTS, WIRES, AND VIRTUAL-ASSET TRANSFERS

Cash reports, wires, and virtual-asset transfers

Cash aggregation, wire fields and virtual-asset travel rules use different scopes and thresholds.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report covered large cash transactions.	Report to KoFIU within 30 days when KRW 10 million or more in cash is paid or received, aggregating payments and receipts separately over one trading day under the same real name at the same institution and applying only the statutory exclusions.	Cash ledger, same-name aggregation, exclusion logic, CTR, submission receipt and reconciliation.	FTRA Article 4-2; FTRA Enforcement Decree Articles 8-2 to 8-7; KoFIU CTR guidance
Detect structuring intended to avoid cash reporting.	Monitor linked and split transactions, investigate evasion indicators and file the required report or STR when the relevant statutory test is met.	Aggregation scenarios, linked-party logic, alert case, disposition and filing receipt.	FTRA Article 4-2(2); FTRA Enforcement Decree Article 8
Transmit prescribed originator and beneficiary information for covered wires.	For transfers above KRW 1 million domestically or USD 1,000 equivalent cross-border, populate the statutory originator and beneficiary fields, retain them and answer permitted domestic information requests within three business days.	Field mapping, message samples, threshold tests, request log, response timestamp and exception queue.	FTRA Article 5-3; FTRA Enforcement Decree Article 10-8
Apply the current virtual-asset travel rule and track the deferred expansion.	Until the 2026 amendment's later effective date, transmit the prescribed customer names and virtual-asset addresses for domestic VASP-to-VASP transfers of at least KRW 1 million and provide additional originator identifiers within three business days on a valid request. Prepare for all-size domestic coverage and the new overseas-transfer rules that take effect six months after promulgation.	Rule-version register, transfer controls, messages, request responses, transition plan and release testing.	FTRA Article 6(3); FTRA Enforcement Decree Article 10-10; FSC release of 11 August 2026

Targeted financial sanctions and CPF

Korean restricted-person measures require pre-transaction blocking, permission controls and prompt reporting.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen current FSC and incorporated UN restricted-person designations.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding, periodically and on list updates; assess entities owned or controlled under the applicable rules, not only exact names.	List source and timestamp, configuration, ownership-control analysis, match decisions and quality tests.	PFOPIA Article 4(1); PFOPIA Enforcement Decree; KoFIU CFT regime and current designation notices
Do not transact with or dispose of property for a restricted person without prior FSC approval.	Block the transaction or disposal before execution, preserve the property and case evidence, and seek FSC permission only through the statutory process.	Block timestamp, asset record, legal assessment, permission application and decision.	PFOPIA Article 4(4); KoFIU CFT regime
Report known terrorist- or proliferation-financing property without delay.	When an employee knows that transaction assets are TF/PF funds or that the counterparty is conducting a restricted transaction without permission, report without delay to the competent investigative authority and make the related KoFIU report.	Knowledge and escalation chronology, authority report, KoFIU filing, receipts and controlled communications.	PFOPIA Article 5(2); FTRA Article 4(1)3; KoFIU designated-person guidance
Test sanctions controls against Korea's FATF-identified TFS limitations.	Document how UN designations, domestic notices, ownership or control and update timing reach screening and blocking systems; treat known TF/PF TFS gaps as heightened control risk.	Gap assessment, list-update SLA, sample testing, remediation and senior risk acceptance.	FATF Korea Follow-Up Report 2024, Recommendations 6 and 7

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Retain reconstructable AML evidence for the statutory period and make it retrievable.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain AML reporting, CDD and transfer information for five years.	Start the five-year clock from the statutory termination of the financial-transaction relationship, including settlement of all claims and obligations for virtual-asset relationships, and preserve each required data category.	Record inventory, trigger-date logic, retention schedule, legal holds and sampled retrieval.	FTRA Article 5-4(1)-(2); FTRA Enforcement Decree Article 10-9
Preserve STR files separately and securely.	Keep the STR and supporting identification, transaction and suspicion-ground data segregated from ordinary transaction records with tightly limited access and auditable retrieval.	Repository configuration, access log, retention metadata, backup test and destruction approval.	FTRA Article 5-4; FTRA Enforcement Decree Article 10-9(1)-(3)
Support lawful KoFIU and supervisory access.	Maintain records in a form and location that permits timely production, with integrity, lineage, Korean-language context and confidentiality preserved.	Regulator-response procedure, data dictionary, immutable export, translation control and production log.	FTRA Articles 13 and 15; FTRA Enforcement Decree Article 10-9

Privacy, biometrics, breaches, and transfers

KYC data is also regulated personal information; AML retention does not displace PIPA controls outside its legal scope.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Implement the PIPA governance duties effective 11 September 2026.	Designate a personal information protection officer (CPO) unless the controller qualifies for the small-business exemption; where that exemption is used, document that the business owner or representative is deemed to be the CPO under PIPA Article 31(2). Give the CPO independent authority, access to specialist personnel and budget, and reporting access to the business owner or representative and board. If the controller meets the thresholds in Enforcement Decree Article 32(3), obtain board approval for each CPO designation, change or removal and submit the prescribed notice to PIPC within six months after the relevant event. For a qualifying controller whose CPO was already designated when the amended decree commenced, submit the notice within six months after 11 September 2026. A PIPC-approved extension may be available for unavoidable circumstances, within the decree's one-year limit. Track the separate ISMS-P mandate as a 1 July 2027 transition, not a current requirement.	CPO appointment and role charter, exemption or threshold analysis, deemed-CPO record where applicable, board minutes, six-month deadline calculation, PIPC filing and receipt, any extension decision, budget and staffing record, independence safeguards, reporting calendar and 1 July 2027 transition plan.	PIPA Article 31; PIPA Enforcement Decree Article 32 and supplementary provisions, as in force 11 September 2026; PIPC release of 10 September 2026
Establish and document a PIPA basis for each KYC processing purpose.	Map collection, use, sharing, outsourcing and retention to consent, statutory duty, contract necessity or another available basis; provide the required notices and collect only necessary data.	Processing register, legal-basis matrix, privacy notices, consent records, minimization review and retention schedule.	PIPA Articles 15, 17, 18, 21, 26 and 30
Protect resident registration numbers and sensitive biometric information.	Process resident registration numbers only under a specific statutory or other permitted condition, encrypt as required, and use separate consent or another express basis plus enhanced safeguards for biometric identifiers treated as sensitive information.	Authority mapping, separate consent where used, encryption proof, key controls, access review and deletion evidence.	PIPA Articles 23, 24, 24-2 and 29; Enforcement Decree of PIPA Article 18
Control cross-border personal-information transfers.	Use a permitted Article 28-8 route, give or disclose the prescribed transfer details, bind recipients to protective measures and monitor onward transfer and PIPC suspension risk.	Transfer map, Article 28-8 basis, notice or consent, recipient contract, security diligence and onward-transfer register.	PIPA Articles 28-8 and 28-9; Enforcement Decree of PIPA Articles 29-7 to 29-11
Operate separate 72-hour workflows for actual breaches, regulator reports and specified possible breaches.	When actual loss, theft, leakage, forgery, alteration or damage is known, notify affected persons within 72 hours, subject to the limited statutory exceptions, and provide follow-up details as they are confirmed. Report to PIPC or KISA within 72 hours only when the current decree criteria apply, including a breach involving at least 1,000 data subjects, sensitive or unique-identification information, or unlawful external access, subject to the decree's limited exception. Also notify affected persons within 72 hours when either possible-breach scenario in Enforcement Decree Article 39-2 is identified, and follow up if an actual breach is confirmed or ruled out.	Incident chronology, affected-person analysis, Article 39-2 possible-breach assessment, notification copies and timestamps, Article 40 regulator-reporting analysis, PIPC/KISA receipt where required, exception rationale and follow-up notices.	PIPA Article 34; PIPA Enforcement Decree Articles 39, 39-2, 39-3 and 40, as in force 11 September 2026
Scope privacy impact assessment correctly.	For public institutions establishing or changing a covered personal-information file, complete the statutory impact assessment before operation; for private high-risk biometric KYC, use an impact assessment as a documented risk control without mislabeling it universally mandatory.	Applicability decision, assessment, mitigations, approval and residual-risk register.	PIPA Article 33; operational control for non-statutory cases

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Assemble evidence that reconstructs legal scope, customer decisions, reporting and privacy compliance.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a complete onboarding and beneficial-ownership pack.	Link identity and legal-existence evidence, authority, ownership chain, 25% and control analysis, risk rating, PEP and sanctions results and approval.	One sampled file showing source provenance, timestamps, reviewer and unresolved issues.	Operational control supporting FTRA Article 5-2 and Enforcement Decree Articles 10-4 and 10-5
Maintain a reconstructable reporting and sanctions pack.	Link monitoring alert, suspicion or designation analysis, decision time, CTR or STR or authority report, submission receipt, confidentiality and blocked-property actions.	One sampled case with full chronology, filings, access record and management review.	Operational control supporting FTRA Articles 4 and 4-2 and PFOPIA Articles 4 and 5
Maintain a current regulatory-change pack.	Track the Korean controlling text, English translation lag, KoFIU notices, VASP deferred effective dates, FATF statements and PIPA amendments; assign owners and test changes before effective dates.	Source register, legal update log, impact assessment, approved implementation plan and post-change test.	Operational control supporting the FTRA, PFOPIA and PIPA frameworks

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.

Financial Transaction Reports Act - current Korean text
Korea Ministry of Government Legislation · Primary legislation
Open official source

FTRA - English statutory translation
Korea Legislation Research Institute · Authoritative legal translation
Open official source

FTRA Enforcement Decree - current Korean text
Korea Ministry of Government Legislation · Primary subordinate legislation
Open official source

KoFIU AML/CFT statutes and regulations
Korea Financial Intelligence Unit · Official legal index
Open official source

KoFIU AML/CFT regime and CDD guidance
Korea Financial Intelligence Unit · Official FIU guidance
Open official source

KoFIU customer due diligence guidance
Korea Financial Intelligence Unit · Official FIU guidance
Open official source

KoFIU suspicious transaction reporting guidance
Korea Financial Intelligence Unit · Official FIU guidance
Open official source

KoFIU currency transaction reporting guidance
Korea Financial Intelligence Unit · Official FIU guidance
Open official source

Approved 2026 VASP registration and AML rule changes
Financial Services Commission · Official regulatory release
Open official source

PFOPIA - English statutory text
Korea Legislation Research Institute · Authoritative legal translation
Open official source

KoFIU counter-terrorist and proliferation-financing regime
Korea Financial Intelligence Unit · Official sanctions guidance
Open official source

KoFIU designated-person reporting guidance
Korea Financial Intelligence Unit · Official sanctions guidance
Open official source

KoFIU current notices and subordinate rules
Korea Financial Intelligence Unit · Official notice register
Open official source

Electronic Financial Transactions Act
Korea Legislation Research Institute · Authoritative legal translation
Open official source

Commercial Act - registration and shareholder records
Korea Legislation Research Institute · Authoritative legal translation
Open official source

Supreme Court registration services
Supreme Court of Korea · Official registry guidance
Open official source

Personal Information Protection Act - current text and versions
Korea Legislation Research Institute · Authoritative legal translation
Open official source

PIPC laws and regulations
Personal Information Protection Commission · Official privacy law index
Open official source

PIPC biometric information protection guideline
Personal Information Protection Commission · Official privacy guidance
Open official source

PIPC personal-information breach reporting
Personal Information Protection Commission · Official incident guidance
Open official source

PIPA governance and breach amendments effective 11 September 2026
Personal Information Protection Commission · Official amendment guidance
Open official source

FATF Korea follow-up report 2024
FATF · Authoritative current assessment
Open official source

FATF Korea mutual evaluation 2020
FATF · Authoritative mutual evaluation
Open official source

FATF jurisdictions under increased monitoring - 19 June 2026
FATF · Authoritative current public list
Open official source

FATF high-risk jurisdictions subject to a call for action - 19 June 2026
FATF · Authoritative current public list
Open official source

Official Taegeukgi design and construction
Ministry of the Interior and Safety · Official national-symbol guidance
Open official source

Document control

Version 1.2 / Published 25 September 2026 / Last reviewed 25 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 25 September 2026. Confirm the entity-specific FTRA perimeter, current KoFIU regulations and forms, sector licence, VASP transition dates, sanctions notices, privacy basis and any Korean-language source text with the competent authority and qualified Korean counsel before launch.