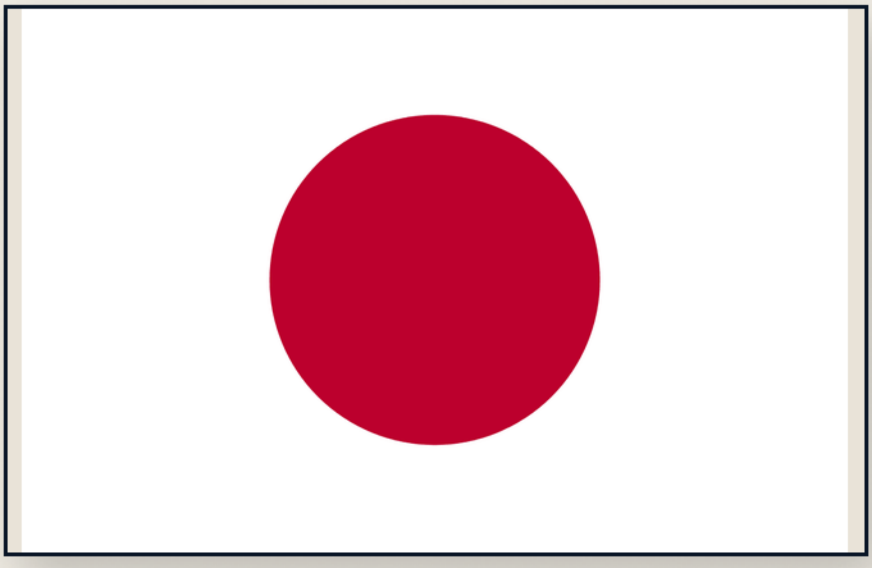
VOVE ID

VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

JAPAN



JAPAN / JP

KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Japan KYC, KYB & AML Compliance Checklist

An implementation checklist for Japan's transaction verification, beneficial ownership, suspicious transaction reporting, transfer information, sanctions, payments, crypto-assets and personal-data controls.

FIU	**Japan Financial Intelligence Center (JAFIC), National Police Agency**
Primary AML rule	**Act on Prevention of Transfer of Criminal Proceeds and its current Order and Ordinance**
STR timing and route	**Promptly to the competent administrative authority through its prescribed route; JAFIC centralizes and analyzes notified information**
Threshold reporting	**No universal cash-threshold report; CDD thresholds and transaction-record exclusions are sector- and transaction-specific**
High-risk source check	**For a high-risk transaction transferring more than JPY 2 million, verify assets and income to the extent required by the APTCP framework**
AML records	**Generally 7 years, with the start event depending on verification or transaction record type**
Privacy authority	**Personal Information Protection Commission (PPC) under the APPI**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Act on Prevention of Transfer of Criminal Proceeds (APTCP), its Enforcement Order and Enforcement Ordinance impose sector- and transaction-specific duties on specified business operators. Financial institutions must also apply the Financial Services Agency's 2026 AML/CFT Guidelines and applicable business laws. Sanctions and asset-freezing controls arise principally under the Foreign Exchange and Foreign Trade Act and the International Terrorist, etc. Asset-Freezing Act.

FATF context

Japan was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. FATF's October 2024 third enhanced follow-up report rated Japan compliant on 4 Recommendations and largely compliant on 35, with none partially compliant; Japan is to report remaining deficiencies in its 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. The legally effective texts are Japanese. Confirm the current specified-business and specified-transaction perimeter, sector rules, filing route, sanctions designation, privacy basis, outsourcing structure and licensing position with the competent authority and qualified Japanese 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

Japan applies the APTCP by specified business, specified activity and specified transaction, with supervision remaining sector-specific.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map each Japanese activity to the specified-business and specified-transaction perimeter.	Classify the legal entity, service, customer, transaction and exemptions under APTCP Article 2, the Enforcement Order and Enforcement Ordinance before onboarding or product launch; do not assume every business or every transaction is covered identically.	Perimeter memo, service and funds-flow map, statutory mapping, exemptions and Japanese counsel sign-off.	APTCP Articles 2 and 4; Enforcement Order Articles 6 and 7; JAFIC APTCP Overview dated 7 August 2026
Identify the competent administrative authority and filing channel for each regulated activity.	Record the sector supervisor, registration or licence, APTCP reporting destination and current e-Gov or authority procedure; distinguish the reporting destination from JAFIC's FIU analysis role.	Authority matrix, licence or registration, filing credentials, test submission and escalation contacts.	APTCP Articles 8 and 13; JAFIC suspicious-transaction reporting destination table
Obtain the required financial-services registration or authorization before operating.	Map banking, funds-transfer, electronic-payment-instrument, crypto-asset, prepaid-payment, financial-instruments and intermediary activities to the current business law and FSA perimeter; obtain approval or registration and observe scope and conditions.	Regulatory-perimeter analysis, application, FSA or Local Finance Bureau decision, conditions and renewal or change log.	Payment Services Act; Banking Act; Financial Instruments and Exchange Act; FSA FinTech Support Desk guidance

Governance and risk assessment

Controls must reflect Japan's national risk assessment, the operator's own risks and sector-supervisory expectations.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain an enterprise-wide ML/TF/PF risk assessment.	Assess customers, beneficial owners, products, services, countries, delivery channels, transactions, technologies, agents and outsourced providers; incorporate the current National Risk Assessment and refresh for material change.	Methodology, current assessment, data sources, inherent and residual risk, approval and remediation plan.	APTCP Article 11; Enforcement Ordinance Article 32; 2025 National Risk Assessment; FSA AML/CFT Guidelines revised 31 March 2026
Maintain risk-based policies, governance and an accountable control function.	Document customer verification, ongoing review, monitoring, STR, transfer information, sanctions, records, training, audit and outsourcing controls; designate an overall manager and give management usable risk reporting.	Approved framework, roles, committee minutes, management information, training, control testing and issue closure.	APTCP Article 11; Enforcement Ordinance Article 32; FSA AML/CFT Guidelines revised 31 March 2026
Test whether the framework operates effectively.	Use independent and risk-based validation to test data, scenarios, customer-risk models, screening, reporting, record retrieval and remediation rather than relying only on policy existence.	Testing plan, samples, model and data validation, findings, owners, deadlines and verified closure.	FSA AML/CFT Guidelines revised 31 March 2026; FSA dialogue paper on validation of effectiveness

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Transaction verification applies at the legally defined trigger and must establish the customer and any person acting for the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Complete transaction verification at each applicable trigger.	Before or when conducting a specified transaction, verify identification particulars, transaction purpose and occupation using a method permitted for the channel; aggregate an apparently split transaction when the Order requires it.	Trigger analysis, identity data, verification source and method, purpose, occupation, timestamp and exception rationale.	APTCP Article 4; Enforcement Order Article 7; Enforcement Ordinance Articles 4 to 10; JAFIC APTCP Overview
Verify the representative and their authority.	Where an individual acts for another customer, verify that individual's identification particulars and establish a valid basis for authority; do not treat an employee card or non-representative officer registration alone as sufficient authority.	Representative KYC, mandate or authority evidence, customer confirmation, scope and transaction log.	APTCP Article 4(4); Enforcement Ordinance Article 12; JAFIC APTCP Overview, representative verification
Use remote verification methods only when every prescribed condition is met.	Select a current Enforcement Ordinance method for non-face-to-face onboarding, test document authenticity and impersonation controls, preserve the required evidence and stop or escalate when verification cannot be completed reliably.	Method legal mapping, images or electronic evidence, liveness and fraud tests, device signals, result and exception review.	APTCP Article 4; Enforcement Ordinance Article 6 as amended; JAFIC materials on transaction-verification methods

KYB, registries, and beneficial ownership

Commercial-registry evidence supports KYB, but beneficial ownership requires a separate natural-person control analysis.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify a legal person's identity, existence, business and representative.	Obtain current commercial or corporation registration, constitutional information, head office, corporate number, officers and business purpose from reliable sources and resolve discrepancies.	Legal Affairs Bureau certificate or registry data, corporate-number check, constitutional documents, officer list and discrepancy log.	APTCP Article 4; Enforcement Ordinance Articles 6 and 7; Commercial Registration Act; Ministry of Justice commercial-registration guidance
Identify the natural persons who ultimately own or control the legal person.	For a capital-majority corporation, identify natural persons with more than 25% direct or indirect voting rights unless a person with more than 50% displaces that tier, then assess control by other means and apply the prescribed senior-manager fallback when no other natural person is identified; use the applicable test for other legal-person types.	Layered ownership chart, voting-right calculations, control evidence, verified identities and fallback rationale.	APTCP Article 4(1)(iv); Enforcement Ordinance Article 11; JAFIC APTCP Overview, beneficial-owner method
Treat the Beneficial Ownership of Legal Persons List as corroboration, not conclusive proof or a universal public register.	Where a stock company supplies a registrar-certified copy, verify its date, attachments and scope, then corroborate ownership and control. Record that the system is request-based, is limited to eligible stock companies and does not prove the submitted description is true.	Certified list copy, attachment inventory, independent corroboration, current ownership check and limitations note.	Ministry of Justice Beneficial Ownership of Legal Persons List System; Enforcement Ordinance Article 11(2)

PEPs, enhanced due diligence, and remote risk

The APTCP defines foreign PEP transactions as high risk; financial-sector expectations require broader risk-sensitive management where relevant.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify foreign PEPs, specified family members and legal persons they beneficially own.	Screen customers and beneficial owners at onboarding and periodically for the foreign-PEP categories in the Enforcement Ordinance, including former office holders and covered family relationships.	Screening source and date, role and relationship analysis, ownership evidence, false-positive disposition and refresh history.	Enforcement Order Article 12; Enforcement Ordinance Article 15; JAFIC APTCP Overview, high-risk transactions
Apply the prescribed enhanced verification to high-risk transactions.	Use the stricter identity and beneficial-owner verification method for impersonation or false-information risk, customers in designated high-risk jurisdictions and foreign PEP transactions. For a high-risk transfer above JPY 2 million, verify assets and income to the extent needed for the STR decision.	Trigger, enhanced sources, dual verification, assets-and-income evidence where scoped, approval and monitoring plan.	APTCP Article 4(2); Enforcement Order Articles 12 and 13; JAFIC APTCP Overview, high-risk verification and JPY 2 million scope
Do not treat domestic PEP screening as an express APTCP foreign-PEP rule.	Where sector guidance or the risk assessment supports screening Japanese public functions, document it as a risk-based control and define approval, source-of-funds, source-of-wealth and monitoring measures without mislabeling it as the statutory foreign-PEP category.	Policy basis, risk assessment, screening result, approval, corroboration and review history.	FSA AML/CFT Guidelines revised 31 March 2026; APTCP foreign-PEP provisions

Ongoing monitoring and suspicious transaction reporting

Suspicion is risk-based, covers attempted or refused activity in relevant cases and must be reported promptly without tipping off.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Keep verified information current and monitor activity against purpose and risk.	Refresh customer, representative and beneficial-owner information; compare activity with expected purpose, occupation or business, known history and the National Risk Assessment; investigate unusual or inconsistent activity.	Refresh schedule, monitoring scenarios, alert chronology, investigation, decision and quality review.	APTCP Articles 8 and 11; Enforcement Ordinance Articles 26 and 32; FSA AML/CFT Guidelines revised 31 March 2026
Report qualifying suspicion promptly to the competent administrative authority.	When property received in specified business is suspected criminal proceeds or the customer is suspected of concealment or receipt conduct, record when suspicion arose and submit promptly through the current sector route. Include attempted or refused activity when the statutory test is met; do not wait for proof.	Suspicion chronology, legal test, decision-maker, report, submission receipt and authority correspondence.	APTCP Article 8; Enforcement Ordinance Articles 25 and 26; JAFIC APTCP Overview and reporting guidance
Apply the professional-sector exceptions and protect report confidentiality.	Confirm whether the operator is excluded or whether professional secrecy limits a report. For a reportable case, prevent disclosure to the customer or related person and restrict report data to authorized personnel.	Sector and privilege analysis, access log, disclosure controls, training and incident record.	APTCP Articles 8 and 12; JAFIC APTCP Overview dated 7 August 2026

Payments, transfers, thresholds, and virtual assets

Amounts in Japan serve different purposes; no single figure is a universal CDD or cash-reporting threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply each sector-specific CDD threshold and anti-structuring rule only to its legal context.	Map account opening, large cash transactions, remittances, payment instruments, crypto-assets, professional services and other specified transactions to the current Order. Aggregate an apparently divided transaction where required and apply special-attention CDD even below a normal threshold.	Threshold matrix, transaction aggregation logic, scenario tests, exceptions and legal citations.	APTCP Article 4; Enforcement Order Article 7; Enforcement Ordinance Articles 4 and 5; JAFIC APTCP Overview
Transmit required originator and beneficiary information for covered transfers.	For foreign-exchange transfers, electronic payment instruments and crypto-assets, populate the prescribed sender and recipient fields, validate completeness, retain the information and apply repair or restriction procedures for missing data.	Field matrix, payment or transfer messages, validation rules, exception queue, disposition and retention evidence.	APTCP Articles 10, 10-3 and 10-5; 2024 fully effective amendments; FSA travel-rule notice effective 3 August 2026
Use the correct Payment Services Act category and registration.	Classify funds-transfer services as Type I, II or III and respect the category conditions; register covered crypto-asset exchange and electronic-payment-instrument services before operation and verify counterparties against current FSA information.	Product and value-flow analysis, category and limit tests, authorization or registration, counterparty checks and change monitoring.	Payment Services Act; FSA FinTech Support Desk; FSA registered crypto-asset exchange provider list

Targeted financial sanctions

Japan's sanctions framework uses transaction restrictions, permission requirements and domestic asset-freezing measures; the applicable list and legal mechanism must be identified.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen against current Japanese designations and restrictions.	Screen customers, beneficial owners, controllers, representatives, counterparties and transactions against the Ministry of Finance and Ministry of Foreign Affairs lists at onboarding, before execution and when lists change; assess ownership and control beyond exact-name matching.	List versions, update logs, configuration tests, match analysis and disposition.	Foreign Exchange and Foreign Trade Act; Ministry of Finance economic-sanctions measures and target lists
Prevent a prohibited or unlicensed payment, capital transaction or asset dealing.	Place an immediate operational hold on a potential match, identify whether FEFTA, the International Terrorist, etc. Asset-Freezing Act or another measure applies, obtain any required permission before activity and follow the competent authority's reporting or consultation route.	Match and ownership-control analysis, hold timestamp, legal-mechanism memo, authority contact, permission and release decision.	FEFTA; International Terrorist, etc. Asset-Freezing Act; Ministry of Finance AML/CFT/CPF regime overview
Keep AML suspicion and sanctions decisions linked but legally distinct.	Assess whether the same facts require an STR, sanctions action, both or neither; do not delay sanctions control while investigating suspicion and do not assume a sanctions false positive resolves AML risk.	Parallel decision log, STR assessment, sanctions disposition, approvals and case closure.	APTCP Article 8; FEFTA; International Terrorist, etc. Asset-Freezing Act

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Seven years is the central APTCP period, but the record category determines when the clock starts.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain verification records for seven years from the applicable end event.	Create the record immediately after verification and retain it for seven years from termination or completion of the contract or transaction specified by the APTCP framework; preserve the method, documents and verified matters.	Verification record, retention classification, start event, deletion hold and retrieval test.	APTCP Article 6; Enforcement Ordinance Articles 19 and 20; JAFIC APTCP Overview
Retain covered transaction records for seven years from the transaction date.	Record the customer or lookup key, date, type, value and transfer origin or destination for covered activity and retain for seven years, subject to the scoped small-transaction exclusions.	Transaction record, source and destination fields, exclusion rationale, retention proof and retrieval test.	APTCP Article 7; Enforcement Ordinance Articles 23 and 24; JAFIC APTCP Overview
Provide accurate and retrievable records to the competent authority.	Maintain Japanese-readable records and controlled export procedures so reports, inspections and correction orders can be answered completely without altering source data or exposing STR information improperly.	Request log, data lineage, production package, approval, delivery receipt and remediation tracking.	APTCP Articles 15 to 18; applicable sector supervisory law

Privacy, biometrics, breaches, and transfers

KYC necessity does not remove the separate APPI duties for purpose, notice, security, third parties, overseas transfers and incidents.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Specify lawful use purposes and minimize KYC personal information.	Identify and communicate the use purpose as specifically as possible, collect only data needed for AML, fraud, sanctions and service purposes, control incompatible use and honor applicable access, correction and cessation rights.	Data inventory, purpose register, notices, necessity assessment, rights workflow and deletion schedule.	APPI Articles 17 to 21 and 32 to 39; PPC APPI legal materials
Protect identity and biometric data with risk-appropriate safeguards.	Classify face images, facial templates and other identity data under the APPI based on their actual form and use; document necessity, accuracy and retention, restrict access, test vendors and avoid treating every biometric as automatically special care-required personal information.	Data classification, privacy assessment, security controls, accuracy and bias tests, vendor review and deletion evidence.	APPI Articles 2 and 23; PPC Guidelines; PPC facial-recognition principles
Control reportable breaches and foreign third-party transfers.	Escalate a qualifying leakage or other incident to the PPC and affected individuals under the Act and Rules, preserving the preliminary and final reporting clocks that apply to the incident. Before providing personal data to a third party abroad, use consent or a valid statutory route, provide required country and safeguard information and maintain continuing-information duties where applicable.	Incident assessment, PPC reports and notices, transfer map, recipient-country information, consent or exception, contract and monitoring.	APPI Articles 26 and 28; Enforcement Rules; PPC General and Foreign Transfer Guidelines

Practical evidence packs

Evidence should reconstruct the Japan-specific legal basis and every material decision from onboarding through reporting and exit.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable customer and KYB pack.	Bundle trigger analysis, identity, representative authority, registry evidence, beneficial ownership, purpose, occupation or business, risk, PEP and sanctions results, privacy records and exceptions under stable identifiers.	Complete sampled onboarding pack, source provenance, approvals and retrieval result.	Operational control supporting APTCP Articles 4 and 6 and APPI security duties
Maintain a reconstructable monitoring, STR and sanctions pack.	Link activity, alerts, information reviewed, suspicion time, promptness decision, submission, confidentiality, sanctions hold, authority contacts and release or exit decision.	Complete sampled case pack, timeline, receipts and controlled-access record.	Operational control supporting APTCP Article 8 and Japanese sanctions laws
Maintain a launch and change-control pack.	Record the service perimeter, licence, competent authority, customer-verification method, transaction thresholds, transfer information, reporting route, sanctions, APPI controls, outsourcing and validation before launch and material change.	Signed launch pack, source register, legal-change log, tests, uncertainty register and approvals.	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.

Act on Prevention of Transfer of Criminal Proceeds - current Japanese text
e-Gov Laws and Regulations · Primary legislation
Open official source

Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds
e-Gov Laws and Regulations · Primary delegated legislation
Open official source

Ordinance for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds
e-Gov Laws and Regulations · Primary delegated legislation
Open official source

APTCP overview current at 7 August 2026
Japan Financial Intelligence Center, National Police Agency · Official current legal guidance
Open official source

JAFIC Annual Report 2025
Japan Financial Intelligence Center, National Police Agency · Official implementation report
Open official source

National Risk Assessment 2025
National Police Agency · Official risk assessment
Open official source

Suspicious transaction reporting and competent authorities
Japan Financial Intelligence Center, National Police Agency · Official reporting guidance
Open official source

AML/CFT Guidelines revised 31 March 2026
Financial Services Agency · Official supervisory guidance
Open official source

Reference cases on suspicious transactions
Financial Services Agency · Official reporting guidance
Open official source

Commercial and corporation registration
Ministry of Justice · Official registry guidance
Open official source

Beneficial Ownership of Legal Persons List System
Ministry of Justice · Official beneficial-ownership guidance
Open official source

FinTech Support Desk regulatory perimeter guidance
Financial Services Agency · Official licensing guidance
Open official source

Finalized 2026 travel-rule jurisdiction amendment
Financial Services Agency · Official transfer-rule notice
Open official source

Registered crypto-asset exchange service providers - 1 April 2026
Financial Services Agency · Official register
Open official source

Japan AML/CFT/CPF legislative regime
Ministry of Finance · Official regime overview
Open official source

Current economic sanctions measures and target lists
Ministry of Finance · Authoritative sanctions lists
Open official source

APPI laws and policies
Personal Information Protection Commission · Primary law and official guidance
Open official source

Guidelines for provision to a third party in a foreign country
Personal Information Protection Commission · Official privacy guidance
Open official source

Japan country profile and 2024 follow-up report
Financial Action Task Force · Authoritative current assessment
Open official source

FATF jurisdictions under increased monitoring - 19 June 2026
Financial Action Task Force · Authoritative current status
Open official source

FATF high-risk jurisdictions subject to a call for action - 19 June 2026
Financial Action Task Force · Authoritative current status
Open official source

Act on National Flag and Anthem
e-Gov Laws and Regulations · Primary national-symbol legislation
Open official source

Document control

Version 1.0 / 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. The legally effective texts are Japanese. Confirm the current specified-business and specified-transaction perimeter, sector rules, filing route, sanctions designation, privacy basis, outsourcing structure and licensing position with the competent authority and qualified Japanese counsel before launch.