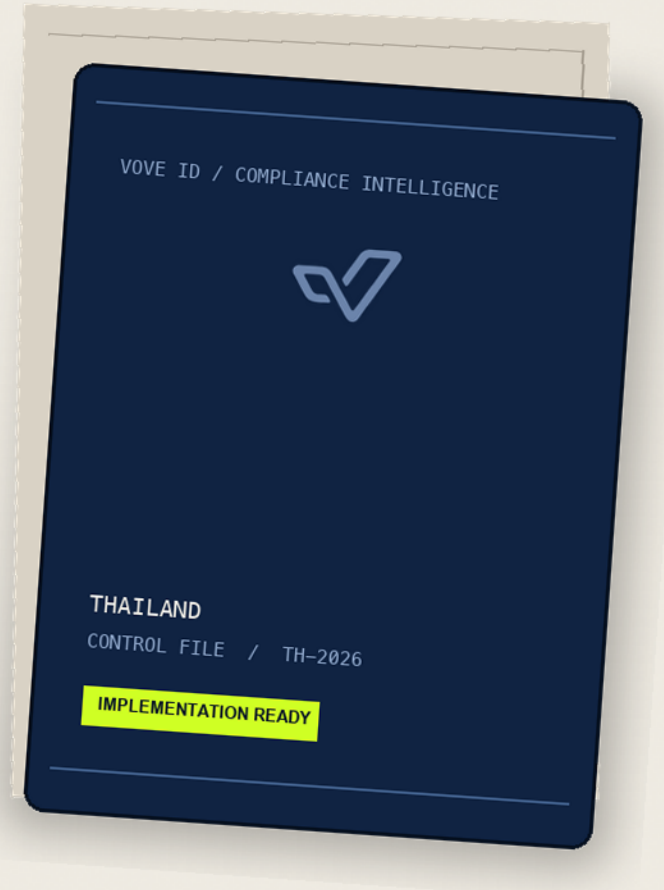
VOVE ID

VOVE COUNTRY CONTROL FILE
KYC / KYB / AML
2026 EDITION

THAILAND

THAILAND / TH



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Thailand KYC, KYB & AML Compliance Checklist

An implementation checklist for customer and business verification, beneficial ownership, transaction reporting, sanctions, payments, digital assets and personal-data protection in Thailand.

FIU	**Anti-Money Laundering Office (AMLO)**
Primary AML rules	**Anti-Money Laundering Act B.E. 2542, as amended, and CDD Regulation B.E. 2563**
STR timing	**File through AMLO within the applicable statutory or prescribed period; do not wait for a monetary threshold**
Threshold reports	**Transaction type and reporting-person specific; use the current AMLO schedules and aggregation rules**
AML records	**CDD and transaction records have distinct statutory periods; preserve longer when AMLO directs or a matter remains active**
Wire information	**Cross-border transfers at THB 50,000 or more are a documented information breakpoint under the assessed framework**
Privacy breach	**Notify the PDPC without delay and, where feasible, within 72 hours when the statutory risk test is met**
FATF public lists	**Not listed at 19 June 2026; APG member**

Scope and legal framework

The Anti-Money Laundering Act B.E. 2542 (1999), as amended, the Ministerial Regulation on Customer Due Diligence B.E. 2563 (2020), the Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559 (2016), and AMLO notifications form the core AML/CFT/CPF framework. Bank of Thailand, Securities and Exchange Commission and other sector rules add activity-specific requirements.

FATF context

Thailand was absent from the FATF jurisdictions under increased monitoring and jurisdictions subject to a call for action statements dated 19 June 2026. Thailand is an Asia/Pacific Group on Money Laundering member and joined the FATF FSRB Guest Initiative in August 2026. 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 26 September 2026. English materials do not replace controlling Thai-language instruments. Confirm the reporting-person perimeter, current AMLO forms and electronic route, sector thresholds, licensing, sanctions directions, registry filings and PDPA transfer rules with the competent authority and qualified Thai counsel before launch.

HOW TO USE THIS GUIDE

Turn each requirement into owned evidence

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

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

Checklist legend

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

Minimum review record

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

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

Scope, authorities, and licensing

Classify the entity, activity and supervisor before applying any control or threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is performed by a reporting person.	Map financial-institution and section 16 professional activities to the current AMLA perimeter, amendments and subordinate instruments; document exclusions and the competent supervisor.	Entity chart, product and funds-flow inventory, perimeter memorandum, source extracts and counsel sign-off.	AMLA sections 3, 13 and 16, as amended
Obtain every sector licence, registration or approval before launch.	Confirm BOT, SEC, Office of Insurance Commission or other authority requirements for the actual payment, e-money, securities, insurance, money-transfer, foreign-exchange or digital-asset service.	Perimeter analysis, application, licence or registration, conditions and renewal calendar.	Payment Systems Act B.E. 2560; Emergency Decree on Digital Asset Businesses B.E. 2561, as amended; applicable sector law
Maintain current AMLO reporting access and accountable contacts.	Enrol authorised users in AMLO's current reporting channel, test access, protect credentials and update appointments and entity details.	Enrolment, user register, access test, appointments and change log.	AMLA sections 13 and 16; AMLO transaction-reporting rules and portal guidance

Governance and ML/TF/PF risk assessment

Controls must be risk-based, approved, resourced and independently tested.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented institutional ML/TF/PF risk assessment.	Assess customers, countries, products, services, transactions, channels, technology, agents and outsourcing; update before material change and when official risk information changes.	Methodology, current assessment, data sources, approval, residual-risk decisions and remediation plan.	CDD Regulation B.E. 2563; AMLO institutional-risk guidance
Maintain approved AML/CFT/CPF policies and accountable governance.	Assign board and senior-management oversight and an empowered compliance function; document CDD, monitoring, reporting, sanctions, records, training and escalation.	Approved programme, appointments, committee minutes, reports, training and issue log.	AMLA and CDD Regulation B.E. 2563; applicable AMLO and sector rules
Independently test design and operating effectiveness.	Use a risk-based audit scope to sample customer files, ownership, reporting clocks, sanctions, data quality, agents and remediation.	Audit plan, independence record, samples, findings, management response and closure tests.	CDD Regulation B.E. 2563; applicable supervisor rules

Natural-person identification

Identity controls apply at relationship, applicable occasional-transaction, suspicion and prior-data-doubt triggers.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify natural-person customers.	Collect prescribed identity attributes and verify them from reliable independent evidence; resolve discrepancies and prohibit anonymous or fictitious-name relationships.	Customer record, identity evidence, verification source, timestamp and discrepancy resolution.	CDD Regulation B.E. 2563, customer identification and verification provisions
Apply the correct CDD trigger and sector threshold.	Configure relationship opening, applicable occasional transactions, suspicion and doubt about prior information. Maintain a versioned sector matrix rather than applying one monetary threshold to every business.	Trigger matrix, linked-transaction logic, tested scenarios, rule version and exceptions.	CDD Regulation B.E. 2563; applicable AMLO and sector notifications
Verify representatives and their authority.	Identify and verify each person acting for a customer and establish the mandate and its limits before accepting instructions or access.	Representative KYC, authority instrument, verification, scope limits and activity log.	CDD Regulation B.E. 2563
Control failed CDD and tipping-off risk.	Where required CDD cannot be completed, do not establish or continue the relationship or transaction as the governing rule requires, assess an STR and avoid alerting the customer.	CDD gap, restriction or exit decision, approvals, suspicion assessment and filing evidence.	CDD Regulation B.E. 2563; AMLA suspicious-reporting and confidentiality provisions

KYB, registries, and beneficial ownership

Verify legal existence, authorised persons and natural-person ownership or control; registry evidence is not conclusive AML proof.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify each legal person or arrangement.	Obtain current Department of Business Development or other competent registry evidence, constitutional documents, purpose, address, directors, partners, trustees and authorised persons.	Certified registry material, constitutional documents, licences, mandates and discrepancy log.	CDD Regulation B.E. 2563; Civil and Commercial Code; applicable registry rules
Identify and verify beneficial owners through ownership and control.	Trace the chain to natural persons, assess control by other means and apply the senior-managing-person fallback only when no natural person is identified under the governing test; record every step.	Ownership chart, calculations, registry evidence, control analysis, verified identities and fallback rationale.	CDD Regulation B.E. 2563; AMLO beneficial-owner identification guidance
Identify parties to trusts and comparable arrangements.	Identify and verify the settlor, trustee or equivalent, protector where relevant, beneficiaries or classes and every natural person exercising ultimate effective control.	Trust instrument, party schedule, control powers, entitlement analysis and verified identities.	CDD Regulation B.E. 2563
Reconcile corporate filings without treating them as dispositive.	Keep DBD registrations and shareholder information current, compare them with the AML ownership analysis and investigate inconsistencies or nominee indicators.	DBD extracts, shareholder records, reconciliation, nominee-risk review and escalation.	Civil and Commercial Code; DBD registration guidance; CDD Regulation B.E. 2563

PEPs, enhanced due diligence, and remote onboarding

Political exposure, higher risk and remote delivery require stronger measures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify politically exposed persons and relevant relationships.	Screen customers and beneficial owners for domestic, foreign and international-organisation PEP status and the relationships covered by the current AMLO notification; refresh risk-sensitively.	Screening result, source, relationship map, rationale and refresh history.	CDD Regulation B.E. 2563; AMLO Notification on Politically Exposed Persons effective 2 February 2026
Apply enhanced due diligence when higher risk requires it.	Obtain required senior approval, corroborate source of wealth and funds, obtain additional purpose information and increase monitoring frequency and depth.	Risk trigger, approval, corroboration, enhanced plan and periodic reviews.	CDD Regulation B.E. 2563
Control non-face-to-face identity and biometric processing.	Validate document authenticity, liveness, impersonation and device risk; document the PDPA lawful basis, necessity, security and retention of biometric or identity data.	Method assessment, fraud tests, privacy assessment, vendor diligence and exception log.	CDD Regulation B.E. 2563; Personal Data Protection Act B.E. 2562 sections 24, 26 and 37

Monitoring and suspicious transaction reporting

Monitor against expected activity and report suspicion to AMLO without waiting for a threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing due diligence and transaction monitoring.	Keep identity, ownership and risk information current and scrutinise activity against purpose, profile, capacity and expected source of funds; investigate deviations promptly.	Monitoring scenarios, alerts, case analysis, refresh history and dispositions.	CDD Regulation B.E. 2563
Detect and assess suspicious transactions and attempts regardless of amount.	Map the statutory suspicion indicators and relevant attempted activity, record the facts and escalate promptly to the authorised decision-maker.	Alert chronology, indicator mapping, analysis, decision and supporting records.	AMLA sections 3 and 13, as amended
File STRs through the current AMLO route within the applicable period.	Record when suspicion arose, apply the current statutory or prescribed clock, submit the correct report and retain acknowledgement and any supplement. Do not invent a portal or deadline from an obsolete form.	Decision timestamp, report, validation result, AMLO acknowledgement and supplement log.	AMLA section 13; current AMLO reporting rules and portal guidance
Protect reporting confidentiality and prevent tipping off.	Restrict STR, suspicion and AMLO-request information to authorised need-to-know access; legally review disclosures and customer communications.	Access matrix, disclosure log, legal review, training and incident record.	AMLA confidentiality and tipping-off provisions

Threshold reports, wires, payments, and digital assets

Amounts, aggregation, report type and licensing are transaction- and sector-specific.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply transaction-reporting thresholds only with their legal scope.	Maintain the current AMLO schedule for cash, property and other prescribed transactions by reporting-person type; preserve aggregation and exception logic and do not confuse reporting amounts with CDD triggers.	Versioned threshold matrix, transaction data, aggregation test, reports and acknowledgements.	AMLA section 13; ministerial regulations prescribing reportable transactions
Carry required originator and beneficiary information in transfers.	For cross-border transfers at THB 50,000 or more, apply the information requirements documented in Thailand's assessed framework; for every transfer apply any stricter current sector rule and repair, reject or restrict incomplete messages.	Field matrix, payment-message samples, validation tests, repair queue and rejection record.	CDD Regulation B.E. 2563 and AMLO electronic-transfer notification; APG Thailand follow-up assessment
Obtain payment-system permission before providing regulated services.	Map the service to designated payment systems and designated payment services and obtain the required Ministry of Finance licence or BOT registration before commencement.	Service map, legal analysis, licence or registration, conditions and agent inventory.	Payment Systems Act B.E. 2560; BOT payment-system oversight guidance
Obtain digital-asset authority and apply the current travel-rule controls.	Classify exchange, broker, dealer, advisory, fund management, custodial-wallet and ICO activities; obtain required approval and implement the SEC travel-rule and KYC/CDD requirements in force for the service.	Activity analysis, licence, SEC correspondence, KYC/CDD configuration, transfer-data tests and exceptions.	Emergency Decree on Digital Asset Businesses B.E. 2561, as amended in 2025; SEC digital-asset rules and September 2026 travel-rule announcement

Targeted financial sanctions

Controls must detect designated persons, ownership and control and support freezing without delay.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen relevant persons and transactions against current designations.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding, during the relationship and when UN or Thai designations change; assess indirect ownership and control.	List inventory, update logs, configuration tests, match analysis and disposition.	Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559
Freeze designated property without delay and report through the verified route.	On an applicable designation, immediately prevent dealing or availability, preserve related property and follow the current AMLO notification, reporting, exemption and release process.	Match and control analysis, freeze timestamp, report, system blocks and authority correspondence.	Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559
Maintain distinct TF and PF sanctions procedures.	Map designation, freezing, reporting, exemption, delisting and unfreezing routes for terrorism and proliferation and test direct and indirect availability scenarios.	Legal map, procedure, list-update record, scenario tests and escalation log.	Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559; applicable AMLO rules

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Records must reconstruct identity, ownership, transactions, reporting and decisions from the correct trigger.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain transaction and CDD records for their distinct legal periods.	Apply the current statutory period and trigger to each record class, preserve records longer for an active case or AMLO direction and do not collapse all records into one retention rule.	Retention schedule, trigger calculations, archive samples, legal holds and deletion approvals.	AMLA sections 22 and 22/1, as amended; CDD record-retention regulations
Preserve evidence in a form that reconstructs each transaction and relationship.	Link identity, ownership, risk, instructions, transaction data, alerts, reports, sanctions actions, approvals and communications under stable identifiers.	Sample case pack, lineage report, retrieval test and access log.	AMLA sections 21-22/1; CDD Regulation B.E. 2563
Provide records securely to authenticated competent authorities.	Maintain a controlled request process that validates authority, preserves confidentiality and records the material produced and delivery route.	Request register, authority validation, production index, approval and receipt.	AMLA; applicable AMLO and sector-supervisor powers

Privacy, biometrics, breaches, and transfers

AML processing remains subject to PDPA purpose, lawful-basis, security and accountability controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document a lawful basis and proportionality for KYC processing.	Map identity, biometric, screening and monitoring fields to legal obligation, consent or another valid basis; provide notice, minimise collection and maintain accuracy.	Data inventory, lawful-basis map, notices, consent where relied upon, field justification and correction process.	Personal Data Protection Act B.E. 2562 sections 19, 23-26 and 37
Implement security and processor accountability.	Use risk-appropriate organisational and technical safeguards, access controls, processor terms, deletion controls and incident cooperation; review sensitive-data vendors.	Security assessment, access review, contracts, subprocessor register, tests and training.	Personal Data Protection Act B.E. 2562 sections 37 and 40
Notify qualifying personal-data breaches on the statutory clock.	Assess likely risk to individuals and notify the PDPC without delay and, where feasible, within 72 hours; notify affected persons without delay when high risk is likely, documenting any exception or delay.	Incident chronology, risk assessment, PDPC notice, data-subject notice and remediation.	Personal Data Protection Act B.E. 2562 section 37(4)
Control cross-border personal-data transfers.	Map destinations and onward transfers, assess adequacy or another lawful transfer mechanism and preserve enforceable safeguards, security and data-subject rights.	Transfer map, mechanism analysis, contracts, recipient assessment and monitoring.	Personal Data Protection Act B.E. 2562 sections 28-29; current PDPC cross-border rules

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

Evidence should reproduce onboarding, reporting, sanctions and launch decisions end to end.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, representative authority, KYB, ownership and control, PEP and sanctions screening, risk, approvals, privacy records and exceptions.	Complete sampled onboarding pack and retrieval result.	Operational control supporting AMLA and CDD Regulation B.E. 2563
Maintain a reconstructable reporting and sanctions pack.	Link transactions, alerts, analysis, decision times, report, acknowledgement, freeze actions, authority communications and access logs.	Complete sampled case pack, timeline and controlled access log.	Operational control supporting AMLA section 13 and the CTPF Act B.E. 2559
Maintain a regulator-scoped launch pack.	Record perimeter, permissions, current sources, reporting readiness, ownership analysis, sanctions, privacy transfers, agents, vendor controls and validation before launch or material change.	Signed launch pack, source register, regulator map, uncertainty log, tests 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.

Anti-Money Laundering Office main portal
AMLO · Official FIU and regulator portal
Open official source

AMLO supervisory laws and ministerial regulations index
AMLO · Official legal index
Open official source

AMLO CDD guidance index
AMLO · Official regulatory guidance
Open official source

AMLO customer-risk and beneficial-owner guidance
AMLO · Official regulatory guidance
Open official source

AMLO 2026 politically exposed persons notification notice
AMLO · Official regulatory notice
Open official source

AMLO reporting and customer-identification guidance
AMLO · Official reporting guidance
Open official source

AMLO designated-person list portal
AMLO · Official sanctions portal
Open official source

Payment Systems Act oversight
Bank of Thailand · Official regulatory guidance
Open official source

Notifications under the Payment Systems Act
Bank of Thailand · Official regulatory index
Open official source

BOT KYC rules for e-money service activation
Bank of Thailand · Official supervisory regulation
Open official source

Digital Asset Businesses
Securities and Exchange Commission Thailand · Official licensing and rules portal
Open official source

Emergency Decree on Digital Asset Businesses, consolidated English text
Securities and Exchange Commission Thailand · Primary legislation
Open official source

SEC 2026 enhanced KYC/CDD guidelines
Securities and Exchange Commission Thailand · Official supervisory guidance
Open official source

SEC 2026 digital-asset travel-rule announcement
Securities and Exchange Commission Thailand · Official supervisory notice
Open official source

Department of Business Development
Department of Business Development · Official company registry portal
Open official source

Personal Data Protection Commission
PDPC Thailand · Official privacy authority portal
Open official source

Thailand 2023 sixth enhanced follow-up report
FATF / APG · Authoritative assessment
Open official source

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

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

FATF FSRB Guest Initiative announcement
FATF · Authoritative current status
Open official source

United Nations Security Council consolidated sanctions list
United Nations · Authoritative sanctions list
Open official source

Document control

Version 1.0 / Published 26 September 2026 / Last reviewed 26 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 26 September 2026. English materials do not replace controlling Thai-language instruments. Confirm the reporting-person perimeter, current AMLO forms and electronic route, sector thresholds, licensing, sanctions directions, registry filings and PDPA transfer rules with the competent authority and qualified Thai counsel before launch.