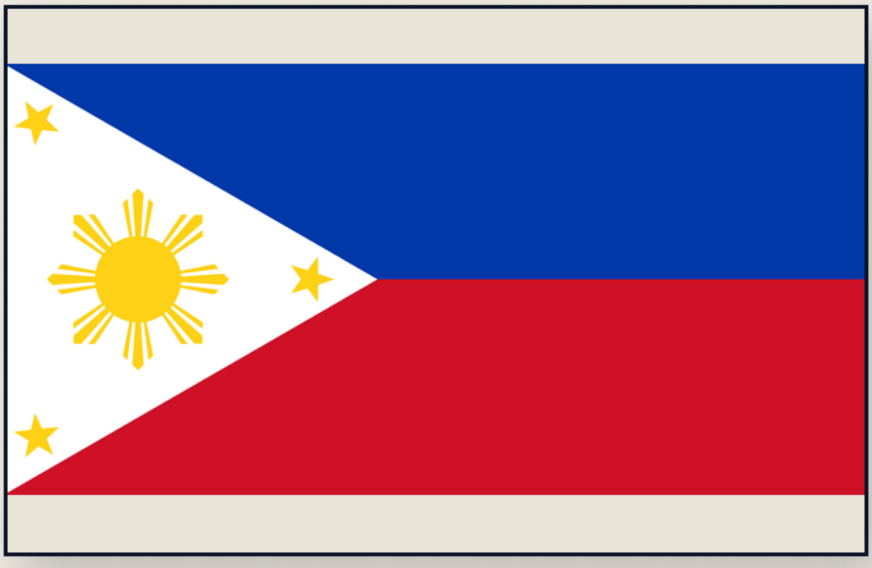
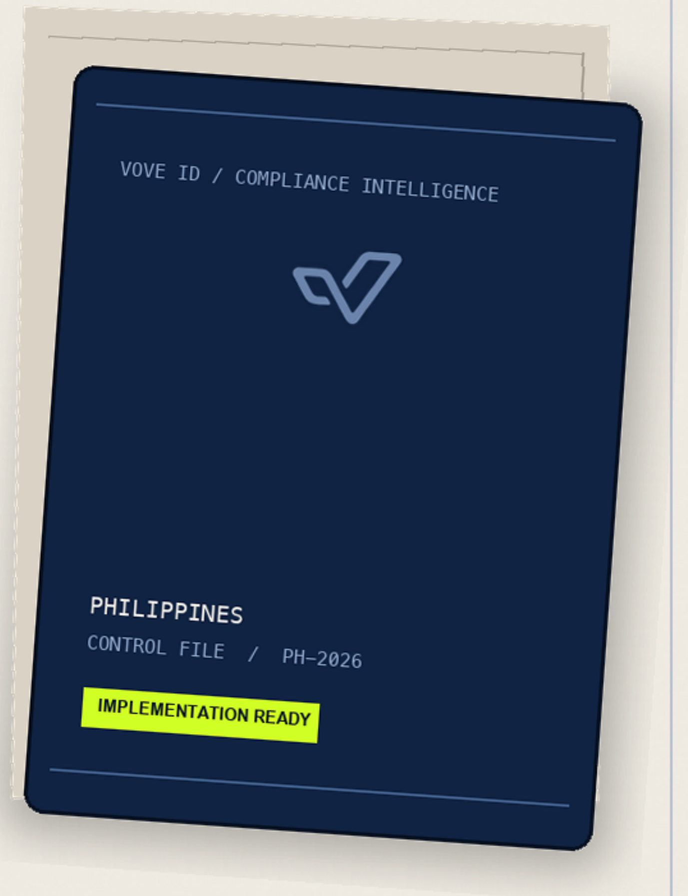
VOVE ID

VOVE COUNTRY CONTROL FILE
KYC / KYB / AML
2026 EDITION

PHILIPPINES



PHILIPPINES / PH



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Philippines KYC, KYB & AML Compliance Checklist

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

FIU	**Anti-Money Laundering Council (AMLC)**
Primary AML rules	**AMLA, as amended, implementing rules and sector-supervisor regulations**
CTR / STR timing	**Generally within 5 working days from occurrence; AMLC may prescribe a different period not exceeding 15 working days**
General covered transaction	**Cash or equivalent monetary instrument exceeding PHP 500,000 within 1 banking day; separate sector thresholds apply**
AML retention	**Generally 5 years, with transaction, account-closure or relationship-end triggers depending on record type**
Banking BO test	**20% is an ownership indicator, followed by control-by-other-means and senior-managing-official fallback**
Privacy breach	**Notify the NPC and affected data subjects within 72 hours when the mandatory-notification test is met**
FATF public lists	**Not listed at 19 June 2026; exited increased monitoring on 21 February 2025**

Scope and legal framework

Republic Act No. 9160, the Anti-Money Laundering Act of 2001 (AMLA), as amended most recently for this framework by Republic Act No. 11521, and its implementing rules establish the core covered-person regime. Republic Act No. 10168 and Republic Act No. 11479 address terrorism financing and terrorism-related freezes; sector supervisors add binding rules. Republic Act No. 12312 has prohibited offshore gaming operations since 2025 and must not be read as a licensing route merely because older AMLA text refers to offshore gaming operators.

FATF context

The Philippines exited FATF increased monitoring on 21 February 2025 and was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. FATF asked the Philippines to sustain its improvements with APG. 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 covered-person perimeter, current AMLC reporting specifications and portal notices, sector-supervisor rules, sanctions orders, licensing availability, SEC HARBOR filing requirements and privacy registration scope with the competent authority and qualified Philippine 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 competent supervisor before relying on a control or launching a service.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is performed by a covered person.	Map financial institutions, securities and insurance businesses, casinos, designated non-financial businesses and professions, real-estate developers and brokers, and other in-scope activities to the current AMLA and implementing rules; document exclusions and the supervising authority.	Entity chart, activity and funds-flow inventory, statutory mapping, supervisor analysis and counsel sign-off.	AMLA, section 3(a), as amended; 2018 IRR, Rule 4, as amended
Register with the AMLC where the covered-person rules require it.	Complete current covered-person registration, appoint authorised users and compliance personnel, maintain AMLC portal access and keep registration particulars current before filing reports.	Certificate or provisional certificate of registration, appointments, portal enrolment, user-access review and change log.	AMLA, sections 7 and 9; AMLC covered-person registration requirements
Obtain each sector licence or registration before regulated activity.	Confirm BSP, SEC, Insurance Commission, PAGCOR or other applicable authority requirements for the actual service, including payment-system operation, merchant acquisition, money service, casino and financial-product activity.	Perimeter memorandum, application, licence or registration, conditions, regulator correspondence and renewal calendar.	Applicable sector law and supervisor issuance; National Payment Systems Act and current BSP payment rules where applicable
Do not treat offshore gaming as a licensable AMLA activity.	Block any business model involving prohibited offshore gaming, POGO content, services, hubs or facilitation; treat detected activity as a legal and suspicious-transaction escalation, not as a registration opportunity.	Product prohibition, customer and merchant screening, escalation record, exit decision and STR assessment.	Republic Act No. 12312, sections 4, 5 and 8

Governance and ML/TF/PF risk assessment

The programme must be risk-based, approved, resourced and tested for the entity's actual exposure.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented institutional ML, TF and PF risk assessment.	Assess customers, countries, products, services, transactions, delivery channels, technology and outsourcing and update the assessment before material change and when official risk information changes.	Methodology, current assessment, data sources, approval, residual-risk decisions and remediation plan.	2018 IRR, Rules 15 and 16, as amended; applicable sector-supervisor AML rules
Maintain an approved prevention programme and accountable compliance function.	Assign board and senior-management oversight and a sufficiently independent compliance officer; document controls for CDD, monitoring, reporting, sanctions, records, training and regulatory response.	Approved programme, appointments, committee minutes, reporting packs, training and issue log.	AMLA, section 9; 2018 IRR, Rule 16, as amended
Independently test programme design and operation.	Use a risk-based audit scope and competent reviewers to test customer files, beneficial ownership, reporting clocks, sanctions, data quality and remediation to verified closure.	Audit plan, independence assessment, sample record, findings, management response and closure tests.	2018 IRR, Rule 16, as amended; applicable BSP, SEC, IC or PAGCOR rules

Natural-person identification

CDD applies at relationship, relevant occasional-transaction, suspicion and prior-data-doubt triggers.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify and verify every natural-person customer using reliable sources.	Collect the prescribed identity attributes, verify official identity evidence or other reliable independent data, resolve inconsistencies and prohibit anonymous or fictitious-name accounts.	Customer record, identity evidence, source provenance, verification result, timestamp and discrepancy resolution.	AMLA, section 9(a); 2018 IRR, Rules 17 and 18; BSP MORB section 921 for BSP-supervised institutions
Apply the correct CDD trigger and threshold.	Configure relationship opening, relevant occasional transactions, suspicion and doubt about prior identification; for BSP-supervised institutions apply the current relevant-business-transaction thresholds and linked-transaction aggregation without generalising them to other sectors.	Sector trigger matrix, aggregation logic, tested scenarios, rule version and exceptions.	2018 IRR, Rule 18; BSP MORB section 921(b)-(d)
Verify representatives and authority.	Identify and verify each person acting for a customer and establish the mandate and its limits before accepting instructions or granting access.	Representative KYC, authority document, verification result, scope limits and activity log.	AMLA, section 9(a); 2018 IRR, Rule 18
Control failed CDD and tipping-off risk.	Where required CDD cannot be completed, do not open or perform the transaction, or terminate the relationship as the applicable rule requires, and consider an STR. If continuing CDD would tip off the customer, stop that inquiry and follow the authorised STR and monitoring procedure.	CDD gap, restriction or exit record, decision approval, suspicion assessment and filing receipt where applicable.	2018 IRR, Rule 18; BSP MORB section 921(a)

KYB, registries, and beneficial ownership

Verify legal existence, authorised persons, ownership and control; keep AML tests separate from corporate disclosure.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person or arrangement identity and existence.	Obtain current registration, constitutional, address, business-purpose, officer, partner, trustee and authority information from the SEC, another competent registry and reliable independent sources.	Registry extract, constitutional documents, licences, officer list, mandates and discrepancy log.	AMLA, section 9(a); 2018 IRR, Rule 18
Identify the natural persons who ultimately own or control the customer.	Trace the ownership chain and control by other means. For BSP-supervised institutions, treat at least 20% ownership as an ownership indicator, then apply control-by-other-means and senior-managing-official fallback rules; do not export that sector formulation without checking the governing rule.	Layered ownership chart, percentage calculations, registry evidence, control analysis, verified identities and fallback rationale.	BSP MORB definition of beneficial owner and section 921(a); 2018 IRR, Rule 18
Identify relevant legal-arrangement parties.	For trusts and comparable arrangements, identify and verify the trustee or equivalent, settlor, beneficiaries or classes, protectors and every other natural person exercising ultimate effective control as the applicable rule requires.	Trust deed, party schedule, control powers, entitlement analysis and verified identities.	2018 IRR, Rule 18; applicable sector-supervisor CDD rules
Maintain current SEC beneficial-ownership disclosures separately.	Apply SEC Memorandum Circular No. 15, series of 2025, and the current HARBOR Beneficial Ownership Declaration process; reconcile filings to the customer file but do not treat a filing as conclusive AML ownership evidence.	BO analysis, declarations, HARBOR receipt, annual filing, change log and discrepancy escalation.	SEC Memorandum Circular No. 15, series of 2025; SEC 2026 reportorial requirements

PEPs, enhanced due diligence, and remote onboarding

Political exposure, higher risk and non-face-to-face delivery require stronger, documented measures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify relevant politically exposed persons and relationships.	Screen customers and beneficial owners for domestic, foreign and international-organisation PEP status and applicable immediate-family and close-associate relationships; refresh results risk-sensitively.	Screening result, source, relationship map, rationale and refresh history.	2018 IRR, Rule 18; BSP MORB section 923 for BSP-supervised institutions
Apply enhanced due diligence when risk or the applicable rule requires it.	Obtain required senior approval, corroborate source of wealth and source of funds, obtain additional purpose information and increase monitoring frequency and depth.	Trigger, approval, source corroboration, enhanced monitoring plan and periodic reviews.	2018 IRR, Rule 18; BSP MORB section 923
Control remote identity and biometric risk.	Validate document authenticity, liveness, impersonation and device risk; assess the legal basis, necessity, proportionality and security of biometric processing before use.	Method assessment, fraud tests, consent or other lawful basis, privacy impact assessment, vendor diligence and exceptions.	Data Privacy Act, sections 12, 13 and 20; NPC Circular No. 2023-06; applicable sector e-KYC rules

Monitoring and suspicious transaction reporting

Monitor against expected activity and report suspicion to the AMLC without waiting for a monetary threshold.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing due diligence and transaction monitoring.	Keep identity, ownership and risk information current and scrutinise activity against the customer's profile, purpose, capacity and expected source of funds; investigate deviations promptly.	Monitoring scenarios, alerts, case analysis, refresh record and dispositions.	2018 IRR, Rule 18; BSP MORB section 921(a)
Identify suspicious transactions and attempts regardless of amount.	Assess the statutory indicators, including no lawful purpose, failed identification, inconsistency with capacity or profile, structuring and connection to unlawful activity; include unsuccessful attempts where the rule applies.	Alert chronology, facts reviewed, indicator mapping, decision-maker and outcome.	AMLA, section 3(b-1); applicable implementing and sector rules
File CTRs and STRs within the applicable reporting clock.	Submit through the current AMLC electronic route generally within five working days from occurrence, subject to any current AMLC-prescribed alternative not exceeding fifteen working days. For an STR, record when suspicious nature was determined and apply the sector rule governing that determination period.	Occurrence and decision timestamps, report, validation output, AMLC acknowledgement and any supplemental submission.	AMLA, section 9(c); BSP MORB section 922; current AMLC portal and reporting notices
Protect report confidentiality and prevent tipping off.	Restrict CTR, STR, suspicion and AMLC-request information to authorised need-to-know access and review every disclosure against the statutory safe harbour and prohibition.	Access matrix, disclosure log, legal review, training and incident record.	AMLA, section 9(c)

Threshold reports, wires, payments, and virtual assets

Amounts, aggregation, report type and licensing are activity-specific.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply the general covered-transaction threshold only to its statutory scope.	Report cash or equivalent monetary-instrument transactions exceeding PHP 500,000 within one banking day when the general rule applies; aggregate as required and keep the amount distinct from CDD or sector thresholds.	Transaction data, aggregation result, scope analysis, CTR and AMLC acknowledgement.	AMLA, section 3(b), as amended
Apply casino and real-estate thresholds only to those covered persons.	For casinos assess a single casino cash transaction exceeding PHP 5 million; for real-estate developers and brokers assess a single cash transaction exceeding PHP 7.5 million. Do not apply either amount outside its statutory sector and transaction type.	Sector classification, cash evidence, threshold calculation, report and exception analysis.	AMLA, section 3(b), as amended by Republic Act No. 11521; Republic Act No. 10927 for casinos
Carry required originator and beneficiary information through wire transfers.	For BSP-supervised institutions, collect, validate and transmit the fields required for transfers below and at or above PHP 50,000, preserve traceability and repair, reject or restrict incomplete transfers according to the governing rule.	Field matrix, payment-message samples, validation tests, repair queue and rejection record.	BSP MORB section 923, fund/wire transfer provisions
Obtain current payment and virtual-asset authority before launch.	Register as an operator of payment systems and obtain a merchant-acquisition licence where applicable. For VASP activity, assess BSP Circular No. 1108, current MORNBFI rules and the continuing new-licence moratorium before making any availability claim.	Service and funds-flow map, OPS registration, merchant-acquisition licence, VASP legal analysis, authority and conditions.	National Payment Systems Act; BSP Circular Nos. 1049, 1108 and 1198; BSP Memorandum No. M-2025-031

Targeted financial sanctions

Sanctions controls must detect designated persons, ownership and control and support immediate preservation.

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, AMLC or Anti-Terrorism Council designations change; assess indirect ownership and control.	List inventory, update logs, configuration tests, match analysis and disposition.	Republic Act No. 10168; Republic Act No. 11479; AMLA section 10(b) as amended
Freeze and preserve covered property without delay.	On an applicable designation or freeze order, immediately block dealing and availability, preserve the specified and related property, follow the current AMLC return and notification route and release only under verified authority.	Match and ownership-control analysis, freeze timestamp, return or report, system blocks and authority correspondence.	Republic Act No. 10168, sections 11 and 16; Republic Act No. 11479, section 36; AMLA section 10(b)
Maintain distinct terrorism- and proliferation-financing procedures.	Map the applicable designation, freeze, exemption, delisting and unfreezing route for terrorism and UN proliferation sanctions and test both direct and indirect availability scenarios.	Legal map, procedure, list-update record, scenario tests, training and escalation log.	Republic Act No. 10168; AMLA sections 3(o)-(p), 7(15) and 10(b), as amended by Republic Act No. 11521

Records and regulator access

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain transaction records for at least five years from the transaction date.	Preserve sufficient data and documents to reconstruct each transaction, subject to any longer legal hold, sector requirement or AMLC direction.	Retention schedule, archive sample, reconstruction test, holds and deletion approvals.	AMLA, section 9(b); BSP MORB section 924
Retain customer records from the correct relationship trigger.	Keep customer identification and transaction documents while the account exists and for at least five years after account closure, relationship termination or the occasional transaction, as applicable; preserve longer when a case remains unresolved.	Trigger calculations, customer archive, case hold, retrieval test and deletion log.	AMLA, section 9(b); BSP MORB section 924
Make records securely and promptly available to competent authorities.	Use stable identifiers and access controls so CDD, beneficial ownership, monitoring, reports, approvals and correspondence can be reconstructed and produced without delay through an authenticated route.	Sample case pack, access review, request register, production index and delivery receipt.	AMLA, sections 7 and 9; applicable sector-supervisor access rules

Privacy, biometrics, breaches, and transfers

KYC data remains subject to purpose, proportionality, security and accountability controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Document the lawful basis and proportionality of KYC processing.	Map each identity, biometric, screening and monitoring field to consent, legal obligation or another valid basis; provide the required notice, minimise collection and keep data accurate.	Data inventory, lawful-basis map, notices, consent where used, field justification and correction process.	Data Privacy Act, sections 11-13 and 16; DPA IRR
Conduct privacy impact assessment and implement current security measures.	Assess each personal-data processing system, designate accountable privacy personnel, maintain the required privacy management and incident programmes, and implement risk-appropriate organisational, physical and technical controls.	PIA, DPO and system registration analysis, privacy programme, access reviews, tests and training.	Data Privacy Act, section 20; NPC Circular Nos. 2022-04 and 2023-06
Notify qualifying personal-data breaches within 72 hours.	Assess the mandatory-notification test and notify the NPC and affected data subjects within 72 hours upon knowledge or reasonable belief that a notifiable breach occurred, using available information and documenting any authorised delay.	Incident chronology, risk assessment, NPC submission, data-subject notice, delay rationale and remediation.	DPA IRR, section 38; NPC Circular No. 16-03
Control processors and cross-border transfers.	Use contracts and due diligence to preserve confidentiality, security, incident cooperation, deletion and audit; remain accountable for transferred personal data and document the applicable recipient protections.	Vendor assessment, contract, subprocessor register, transfer map, safeguards and monitoring.	Data Privacy Act, sections 14 and 21; DPA IRR, sections 43-45

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 under stable identifiers.	Complete sampled onboarding pack and retrieval result.	Operational control supporting AMLA section 9 and 2018 IRR Rule 18
Maintain a reconstructable reporting and sanctions pack.	Link transactions, alerts, analysis, occurrence and decision times, report, acknowledgement, supplements, freeze actions, authority communications and access logs.	Complete sampled case pack, timeline and controlled access log.	Operational control supporting AMLA sections 9(c) and 10 and Republic Act No. 10168
Maintain a regulator-scoped launch pack.	Record covered-person analysis, permissions, current sources, reporting readiness, BO filing, sanctions procedure, privacy registration scope, vendor controls, prohibited POGO screening 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 Act of 2001
Bangko Sentral ng Pilipinas · Primary legislation
Open official source

Republic Act No. 11521 - AMLA amendments
Lawphil · Primary legislation
Open official source

BSP regulations and current manuals index
Bangko Sentral ng Pilipinas · Official regulatory index
Open official source

BSP AML/CFT Regulations - MORB Part IX
Bangko Sentral ng Pilipinas · Official supervisory regulation
Open official source

AMLC portal for registration and reporting
Anti-Money Laundering Council · Official filing portal
Open official source

AMLC covered persons - other covered persons
Anti-Money Laundering Council · Official perimeter and registration guidance
Open official source

Terrorism Financing Prevention and Suppression Act
Lawphil · Primary legislation
Open official source

Anti-Terrorism Act of 2020
Lawphil · Primary legislation
Open official source

Anti-POGO Act of 2025
Lawphil · Primary legislation
Open official source

BSP Circular No. 1108 - VASP guidelines
Bangko Sentral ng Pilipinas · Official supervisory regulation
Open official source

BSP Memorandum No. M-2025-031 - continued VASP licence moratorium
Bangko Sentral ng Pilipinas · Official supervisory issuance
Open official source

BSP payments and settlements regulatory framework
Bangko Sentral ng Pilipinas · Official regulatory guidance
Open official source

SEC Memorandum Circular No. 15, series of 2025
Securities and Exchange Commission · Official beneficial-ownership rules
Open official source

SEC reportorial requirements for corporations
Securities and Exchange Commission · Official registry guidance
Open official source

Data Privacy Act of 2012
National Privacy Commission · Primary legislation
Open official source

Implementing Rules and Regulations of the Data Privacy Act
National Privacy Commission · Official regulation
Open official source

NPC advisories and circulars
National Privacy Commission · Official regulatory index
Open official source

FATF Philippines country profile
FATF · Authoritative current assessment
Open official source

FATF Philippines exit from increased monitoring - 21 February 2025
FATF · Authoritative status statement
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

United Nations Security Council consolidated sanctions list
United Nations · Authoritative sanctions list
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. Confirm the covered-person perimeter, current AMLC reporting specifications and portal notices, sector-supervisor rules, sanctions orders, licensing availability, SEC HARBOR filing requirements and privacy registration scope with the competent authority and qualified Philippine counsel before launch.