VOVE ID

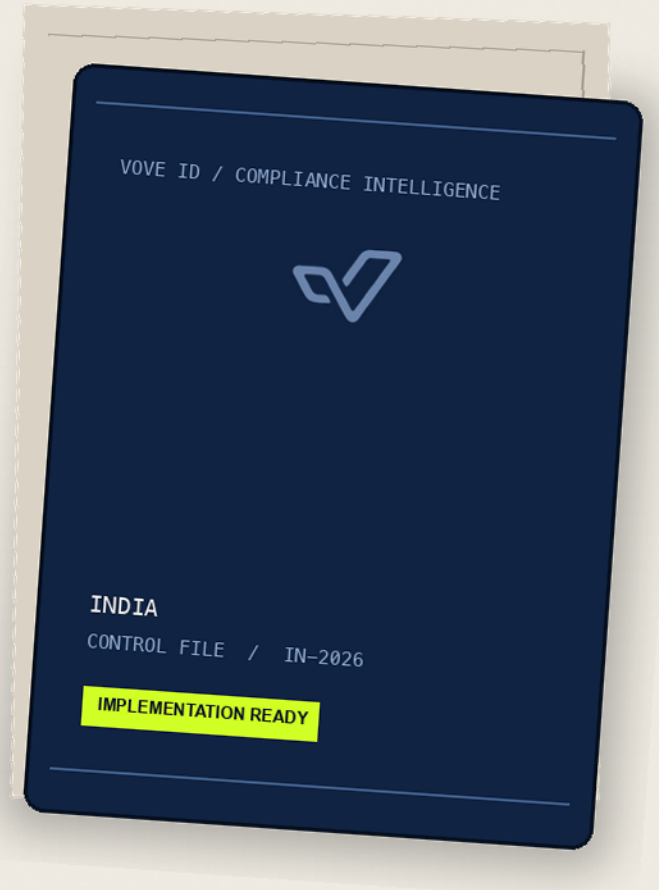
VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

INDIA

INDIA / IN



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

India KYC, KYB & AML Compliance Checklist

An implementation checklist for customer identity, business verification, beneficial ownership, suspicious reporting, sanctions, payments, virtual digital assets and personal-data protection in India.

FIU	**Financial Intelligence Unit - India (FIU-IND)**
Primary AML rules	**PMLA 2002 and PML (Maintenance of Records) Rules 2005, as amended**
STR timing	**Promptly and no later than seven working days after satisfaction that a transaction is suspicious**
Monthly reports	**Applicable prescribed reports by the 15th day of the succeeding month**
AML retention	**Five years from transaction or relationship-end trigger, according to record type**
RBI BO tests	**More than 10% for companies and trusts; more than 15% for unincorporated associations, plus control/fallback rules**
Privacy transition	**DPDP Act and Rules 2025 commence in phases; map each operative provision before relying on it**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Prevention of Money-laundering Act 2002 and the Prevention of Money-laundering (Maintenance of Records) Rules 2005 establish the core reporting-entity framework. RBI, SEBI and other supervisors add sector directions. The Companies Act 2013 and Significant Beneficial Owners Rules govern company disclosure, while the Digital Personal Data Protection Act 2023 and Rules 2025 have phased commencement dates.

FATF context

India was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. The 2024 FATF/APG/EAG mutual evaluation placed India in regular follow-up. 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 22 September 2026. Confirm later Gazette amendments, the reporting entity's sector directions, FIU-IND filing specifications, sanctions implementation orders, phased DPDP commencement and state-specific requirements with the competent authority and qualified Indian 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

Classify the entity, activity and supervisor before relying on any sector control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is within the PMLA reporting-entity perimeter.	Map banking, financial, securities, gaming, property, precious-metals, professional, trust-and-company-service and virtual-digital-asset activities to the current statutory definition and notification.	Entity chart, activity inventory, statutory analysis, notification register and counsel sign-off.	PMLA, sections 2(1)(sa), 2(1)(wa), 11A and 12; applicable Central Government notifications
Identify the competent supervisor and permission for every regulated service.	Confirm whether RBI, SEBI, IRDAI, FIU-IND or another authority licenses, registers or supervises the activity before launch or material change.	Perimeter memorandum, licence or registration, conditions, regulator correspondence and renewal calendar.	PML Rules, rule 9(14); applicable sector law and supervisory direction
Register with FIU-IND where the reporting regime requires it.	Complete the current FINnet/FINGate registration, appoint the required Designated Director and Principal Officer, and keep contact and entity information current.	Registration acknowledgement, appointments, portal access record and change log.	PML Rules, rules 7 and 9; FIU-IND registration materials
Treat notified VDA services as reporting-entity activity.	For exchange, transfer, custody or issuer-related VDA services carried on for another person in the course of business, assess the 7 March 2023 notification and current FIU-IND registration and AML/CFT guidance, including offshore service into India.	Service and geography map, VDA analysis, registration, control gap assessment and ongoing compliance record.	Ministry of Finance notification dated 7 March 2023; FIU-IND VDA guidelines updated 8 January 2026

2. GOVERNANCE AND RISK ASSESSMENT

Governance and risk assessment

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented ML, TF and PF risk assessment.	Assess customer, geography, product, service, transaction, delivery-channel and technology risks and update the assessment after material change.	Methodology, current assessment, data sources, approvals, residual-risk decisions and remediation plan.	PML Rules, rule 9; RBI KYC Direction, sections 4 and 5; FATF India MER 2024, Recommendations 1 and 15
Assign accountable AML leadership.	Appoint a Designated Director and Principal Officer with documented authority, resources, independence and escalation to senior management or the board.	Appointments, notifications, role descriptions, reporting lines and committee minutes.	PML Rules, rules 2(1)(ba), 2(1)(f) and 7
Approve and independently test the AML programme.	Maintain policies for CDD, monitoring, reporting, sanctions, records, employee screening, training, group controls and quality assurance; independently test design and operation.	Policy suite, approval, training, audit plan, samples, findings and verified closure.	PML Rules, rule 9; RBI KYC Direction, Chapters II and X

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

CDD applies at relationship, occasional-transaction, suspicion and doubt triggers under the governing sector rule.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Configure CDD triggers from the applicable sector instrument.	Map account or relationship opening, occasional transactions, international money transfer, suspicion and doubt about previous identification; aggregate linked transactions where the rule requires it.	Trigger matrix, sector-rule version, aggregation tests, timestamps and exception log.	PML Rules, rule 9; RBI KYC Direction, sections 14 and 23
Identify and verify each natural-person customer.	Obtain prescribed identity and address information and verify it through permitted official documents, digital KYC, CKYCR records, Aadhaar routes or other reliable independent means applicable to the entity.	Customer record, verification source, authentication or retrieval result, timestamp and discrepancy resolution.	PMLA, section 11A; PML Rules, rule 9; RBI KYC Direction, sections 16 and 18
Verify representatives and authority.	Identify the person acting for a customer, verify identity and confirm documentary authority before allowing instructions or access.	Representative KYC, mandate, verification result, scope limits and activity log.	PML Rules, rule 9; RBI KYC Direction, section 14
Stop onboarding or restrict activity when required CDD cannot be completed.	Do not open or continue an account or execute the transaction where the applicable rule prohibits it; assess an STR without tipping off the customer.	CDD gap, restriction or exit, approval, suspicion assessment and filing receipt where applicable.	PML Rules, rule 9; RBI KYC Direction, sections 39 and 41

KYB, registries, and beneficial ownership

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person existence, purpose and authority.	Obtain current incorporation, registered-office, tax, constitutional, director or partner and authorisation information from reliable sources such as the MCA registry and applicable regulator.	Registry extract, constitutional documents, PAN, licence, officer list, mandates and discrepancy log.	PML Rules, rule 9; RBI KYC Direction, sections 27-30
Identify the natural-person AML beneficial owner using the applicable cascade.	For RBI-regulated entities apply the current ownership thresholds, then control by other means, and the senior-managing-official fallback only where no natural person is identified; apply sector-specific exemptions carefully.	Layered ownership chart, percentage calculations, control analysis, verified identities, exemption and fallback rationale.	PML Rules, rule 9(3); RBI KYC Direction, section 33
Apply trust and legal-arrangement party identification.	Identify the author or settlor, trustees, beneficiaries meeting the applicable threshold and any other natural person exercising ultimate effective control.	Trust deed, party schedule, ownership or entitlement calculations, authority records and verified identities.	PML Rules, rule 9(3); RBI KYC Direction, section 33
Maintain company significant-beneficial-owner compliance separately.	Assess Companies Act section 90 and the current Significant Beneficial Owners Rules, obtain BEN-1 declarations, maintain BEN-3 and file BEN-2 within the applicable time; do not substitute this registry test for AML CDD.	SBO analysis, notices, declarations, register, filings and change log.	Companies Act 2013, section 90; Companies (Significant Beneficial Owners) Rules 2018, as amended

PEPs, enhanced due diligence, and remote onboarding

Higher-risk and non-face-to-face relationships require stronger measures under the applicable sector rule.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Identify politically exposed customers and beneficial owners.	Use declarations and reliable sources to identify covered foreign PEPs and related family or close-associate relationships; assess domestic prominent public functions under the entity's risk framework and sector rules.	Screening result, declaration, relationship map, source, rationale and refresh history.	RBI KYC Direction, section 35; FATF India MER 2024, Recommendation 12
Apply enhanced measures to higher-risk relationships.	Obtain required senior approval, establish source of funds and source of wealth where applicable, corroborate purpose and increase the degree and frequency of monitoring.	Risk decision, approval, source corroboration, enhanced monitoring plan and reviews.	PML Rules, rule 9; RBI KYC Direction, sections 34-37
Use permitted remote-onboarding methods and control impersonation risk.	Select a permitted V-CIP, digital KYC or equivalent route; verify liveness, location, audit trail, consent and document authenticity and retain the prescribed record.	Method decision, session record, liveness and location results, document checks, consent and QA review.	RBI KYC Direction, sections 18 and Annex I

Monitoring and suspicious reporting

Monitor against expected activity and report suspicion to FIU-IND within the statutory clock.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Monitor transactions and keep customer information current.	Scrutinise transactions for consistency with customer profile, business, risk and source of funds and refresh records at the risk-based frequency required by the supervisor.	Monitoring scenarios, alerts, case analysis, refresh schedule and dispositions.	PMLA, section 12; PML Rules, rule 9; RBI KYC Direction, sections 38 and 39
Report suspicious transactions promptly.	Once the Principal Officer is satisfied that a transaction or attempted transaction is suspicious, file the STR with FIU-IND promptly and no later than seven working days; do not wait for proof or a threshold.	Suspicion chronology, decision, STR, FINGate acknowledgement and supplemental responses.	PML Rules, rules 3(1)(D), 7 and 8; FIU-IND FAQs
Preserve confidentiality and prevent tipping off.	Restrict knowledge of an STR, FIU request or related analysis and do not disclose information that would prejudice reporting or investigation, except where lawfully authorised.	Need-to-know matrix, access logs, communication controls, training and incident register.	PMLA, sections 12 and 14; PML Rules, rule 7
Respond to FIU-IND and competent-authority requests through controlled channels.	Authenticate the request, preserve relevant records, produce complete information promptly and log disclosure while maintaining report confidentiality.	Request register, validation, production index, secure delivery and acknowledgement.	PMLA, sections 12 and 13; PML Rules, rule 7

7. THRESHOLD REPORTS, PAYMENTS, AND TRANSFERS

Threshold reports, payments, and transfers

Threshold reporting and transfer controls are report- and sector-specific.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
File applicable monthly transaction reports by the statutory deadline.	Determine whether CTR, connected cash, NPO receipt, counterfeit-currency or cross-border wire reporting applies and submit the prescribed report by the 15th day of the succeeding month.	Report-scope matrix, aggregation tests, source data, validation output, submission and acknowledgement.	PML Rules, rules 3 and 8; FIU-IND FAQs and Reporting Format Guide
Do not generalise one monetary threshold across all controls.	Apply each amount, currency, aggregation period, product scope and exemption only to the specific report or sector rule that creates it.	Threshold inventory, legal source, rule version, test cases and exception approvals.	PML Rules, rule 3; applicable sector direction
Carry required originator and beneficiary information through transfers.	Collect, validate, retain and transmit prescribed payer and payee data; repair, reject or restrict transfers with missing information as required by the applicable payment rule.	Field matrix, message samples, validation rules, repair queue and rejection record.	RBI KYC Direction, wire-transfer provisions; FATF India MER 2024, Recommendation 16

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Use current UN and Indian designation mechanisms and verified sector procedures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen relevant parties and transactions against current designations.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding, during the relationship and whenever applicable UN or Indian lists change.	List inventory, update logs, screening configuration, tests, match analysis and dispositions.	UAPA, section 51A; Government procedure order dated 2 February 2021 as corrected; RBI KYC Direction, section 52
Freeze covered assets without delay on a confirmed designation.	Follow the current section 51A procedure to prevent dealing in covered funds or assets, report through the competent route and release only under verified authority.	Match analysis, freeze timestamp, ownership-control analysis, report, system blocks and authority correspondence.	UAPA, section 51A; Government procedure order dated 2 February 2021 as corrected
Document proliferation-financing sanctions coverage.	Map applicable UN proliferation designations, domestic implementation orders and sector instructions and test ownership, control and indirect-availability scenarios.	Legal map, list update record, screening tests, escalation procedure and training.	Weapons of Mass Destruction and their Delivery Systems Act 2005, section 12A; FATF India MER 2024, Recommendation 7

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Records must reconstruct transactions and remain available for the correct five-year period.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain transaction records for five years from the transaction date.	Preserve information sufficient to reconstruct individual transactions, including parties, nature, amount, currency, date and channel, subject to any longer lawful hold.	Retention schedule, archive sample, reconstruction test, legal holds and deletion approvals.	PMLA, section 12(1)(a) and 12(3); PML Rules, rule 10
Retain identity and relationship records for five years after the relationship ends or account closes.	Start the retention clock from the correct relationship-end trigger and keep CDD, beneficial ownership, correspondence and analysis retrievable.	Trigger calculations, customer archive, retrieval test, holds and deletion log.	PMLA, section 12(1)(e) and 12(3); PML Rules, rule 10
Maintain records in a form promptly producible to authorities.	Use stable identifiers and controlled access so identity, ownership, risk, transactions, alerts, reports and approvals can be reconstructed and securely produced.	Sample case pack, access review, request register, production index and delivery receipt.	PMLA, sections 12 and 13

Privacy, biometrics, and cyber incidents

Apply currently commenced privacy provisions and track the DPDP transition precisely.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Map commencement before applying the DPDP Act or Rules.	For each processing obligation, identify whether the relevant Act section and Rule is in force on the processing date; do not present future-phase duties as already operative.	Commencement matrix, Gazette copies, legal analysis, owner and transition plan.	Digital Personal Data Protection Rules 2025, rule 1; commencement notifications dated 13 November 2025
Document lawful, necessary and secure handling of KYC data.	Map purpose, notice or statutory basis, fields, access, accuracy, security, retention and deletion for identity, biometric, screening and monitoring data under operative law and sector directions.	Data inventory, lawful-basis map, notices, access reviews, security tests and retention configuration.	DPDP Act 2023 and Rules 2025 as commenced; Information Technology Act 2000; applicable sector directions
Report specified cyber incidents to CERT-In within six hours.	Classify incidents against Annexure I and notify CERT-In within six hours of noticing or being informed of a covered incident while preserving required logs and continuing other applicable notifications.	Incident classification, notice time, submission, logs, containment record and follow-up.	CERT-In Directions under IT Act section 70B(6), 28 April 2022, direction (ii)
Control processors, vendors and cross-border access.	Contract for confidentiality, security, audit, incident cooperation, deletion and subprocessing; assess localisation or transfer constraints under the applicable sector and currently operative privacy rule.	Vendor assessment, contract, subprocessor register, data-flow map, transfer analysis and monitoring.	DPDP Act 2023 and Rules 2025 as commenced; RBI outsourcing and KYC directions where applicable

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, representative authority, KYB, beneficial ownership, PEP and sanctions screening, risk, approvals, privacy records and exceptions under stable identifiers.	Complete sampled onboarding pack and retrieval result.	Operational control supporting PMLA sections 11A-12 and PML Rules rule 9
Maintain a reconstructable reporting and sanctions pack.	Link transactions, alerts, analysis, statutory timing, report, acknowledgement, supplements, freeze actions, authority communications and access logs.	Complete sampled case pack, timeline and controlled access log.	Operational control supporting PML Rules rules 3, 7 and 8; UAPA section 51A
Maintain a regulator-scoped launch pack.	Record activity classification, permissions, current sources, filing readiness, ownership duties, sanctions procedure, privacy transition, 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.

Prevention of Money-laundering Act 2002
India Code · Primary legislation
Open official source

FIU-IND frequently asked questions
Financial Intelligence Unit - India · Official FIU guidance
Open official source

FIU-IND Reporting Format Guide version 2.2
Financial Intelligence Unit - India · Official reporting specification
Open official source

FIU-IND downloads and current sector guidance
Financial Intelligence Unit - India · Official guidance index
Open official source

VDA service-provider registration circular
Financial Intelligence Unit - India · Official registration circular
Open official source

RBI KYC Amendment Directions 2025
Reserve Bank of India · Official supervisory direction
Open official source

RBI KYC Direction 2016 consolidated to November 2024
Reserve Bank of India · Official supervisory direction
Open official source

Companies Act 2013
Ministry of Corporate Affairs · Primary legislation
Open official source

Digital Personal Data Protection Rules 2025
Ministry of Electronics and Information Technology · Official Gazette rules
Open official source

MeitY acts and policies index
Ministry of Electronics and Information Technology · Official legal index
Open official source

CERT-In cyber-security directions dated 28 April 2022
CERT-In · Binding official direction
Open official source

UAPA section 51A sanctions procedure reference
Reserve Bank of India · Official supervisory notification
Open official source

FATF India country profile and 2024 mutual evaluation
FATF · Authoritative current 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

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

National Flag, Emblem and Anthem materials
Ministry of Home Affairs · Official national-symbol guidance
Open official source

Document control

Version 1.0 / Published 22 September 2026 / Last reviewed 22 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 22 September 2026. Confirm later Gazette amendments, the reporting entity's sector directions, FIU-IND filing specifications, sanctions implementation orders, phased DPDP commencement and state-specific requirements with the competent authority and qualified Indian counsel before launch.