VOVE ID

VOVE COUNTRY CONTROL FILE

KYC / KYB / AML

2026 EDITION

AUSTRALIA

AUSTRALIA / AU

KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

Australia KYC, KYB & AML Compliance Checklist

An implementation checklist for Australia's reformed customer due diligence, beneficial ownership, transaction reporting, sanctions, virtual assets, professional services and privacy requirements.

FIU and AML/CTF regulator	**Australian Transaction Reports and Analysis Centre (AUSTRAC)**
Primary AML rules	**AML/CTF Act 2006 and AML/CTF Rules 2025, as in force**
SMR timing	**24 hours for terrorism-financing suspicion; otherwise 3 business days after the day suspicion is formed; limited LPP claims may have 5 business days**
Cash threshold report	**A$10,000 or more in physical currency, including foreign-currency equivalent; generally within 10 business days**
AML retention	**Generally 7 years, with the statutory start event depending on record type**
Reform transition	**New regime in force; eligible legacy ACIP transition may continue by customer class until no later than 31 March 2029**
Privacy	**Privacy Act 1988 and Australian Privacy Principles where coverage applies; biometrics used for automated identification or verification are sensitive information**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006, as reformed, and the Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 govern reporting entities. Updated obligations began for existing reporting entities on 31 March 2026 and for newly regulated professional-services, real-estate and precious-metals-and-stones sectors on 1 July 2026, subject to transitional rules.

FATF context

Australia was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. Its latest published technical follow-up is the March 2024 FATF/APG report. Australia's fifth-round mutual evaluation is underway across 2026-2027. 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 23 September 2026. Confirm the designated-service perimeter, transitional position, current Rules, AUSTRAC forms and guidance, sector licensing, sanctions measures, state or territory professional rules and privacy coverage with the competent authority and qualified Australian 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 REGISTRATION

Scope, authorities, and registration

Classify every service, geographic link and transition before relying on a control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity is a designated service with an Australian geographic link.	Map financial, remittance, gambling, bullion, virtual-asset, real-estate, precious-metals-and-stones and professional services to the current Act tables and exclusions before launch or material change.	Entity and service map, customer and funds flows, geographic-link analysis, statutory citations and counsel sign-off.	AML/CTF Act 2006, sections 6, 6A and 6B and current designated-service tables
Enrol with AUSTRAC and register where the Act requires a register entry.	Apply for enrolment within 28 days after commencing a designated service unless a specific earlier transitional deadline applies. Obtain approved remittance or VASP registration before service, subject to the limited 2026 transitional application rule for new VASP services; keep details current.	AUSTRAC Online submission, enrolment confirmation, registration decision, conditions, renewal and change log.	AML/CTF Act 2006, Parts 6 and 6A; AUSTRAC enrolment and registration guidance
Apply the tranche-2 perimeter from 1 July 2026.	For lawyers, conveyancers, accountants, trust and company service providers, real-estate businesses and dealers in precious metals or stones, identify whether the actual service is designated rather than treating an occupation as automatically covered.	Matter-type inventory, designated-service assessment, exclusions, enrolment and scoped procedures.	AML/CTF Act 2006, section 6 and Tables 5-8; AUSTRAC new-regime guidance
Document each transitional rule relied upon.	For eligible pre-31 March 2026 entities, record customer classes, legacy ACIP end dates and the implementation plan; do not combine the legacy and new initial-CDD approaches for one class.	Transition eligibility memo, approved policies, class schedule, end dates, implementation milestones and monitoring.	Anti-Money Laundering and Counter-Terrorism Financing Transitional Rules 2026, Parts 3-4

2. GOVERNANCE AND ML/TF RISK ASSESSMENT

Governance and ML/TF risk assessment

The program must be risk-based, governed by accountable senior management and independently evaluated.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented ML/TF/PF risk assessment.	Assess customers, countries, products, services, transactions, delivery channels, technology and outsourcing; update before material change and when AUSTRAC information changes the risk picture.	Methodology, current assessment, data sources, approval, residual-risk decisions and remediation plan.	AML/CTF Act 2006, Part 1A; AML/CTF Rules 2025, Part 4
Maintain an effective AML/CTF program appropriate to the business.	Translate identified risks into policies for CDD, monitoring, reporting, transfers, sanctions escalation, records, personnel, training, third parties and regulatory response.	Approved program, control mapping, procedures, training records, testing and issue closure.	AML/CTF Act 2006, Part 1A; AML/CTF Rules 2025, Parts 3-5
Assign senior-manager oversight and notify the governing body.	Name accountable senior managers, give them sufficient authority and resources, record approvals and ensure material non-compliance and risk changes reach the governing body.	Appointments, role descriptions, approval minutes, reporting packs and escalation records.	AML/CTF Act 2006, Part 1A; AML/CTF Rules 2025, governance provisions
Arrange independent evaluation of the program.	Use a suitably independent and competent evaluator, scope the entire program at the risk-based frequency, provide access and track findings to verified closure, including applicable transition timing.	Independence assessment, plan, report, management response and closure tests.	AML/CTF Act 2006, Part 1A; AML/CTF Rules 2025; Transitional Rules 2026, Part 7

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

Initial CDD must establish prescribed matters on reasonable grounds before service, except where a controlled statutory exception applies.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Complete initial CDD before commencing a designated service.	Establish identity, relevant represented or acting persons, authority, PEP and sanctions status, purpose and relationship or transaction risk before service unless a specific delayed-verification rule applies.	CDD record, sources, verification results, risk decision, timestamp and exception approval.	AML/CTF Act 2006, sections 28-30; AML/CTF Rules 2025, Part 6
Identify and verify each individual customer on reasonable grounds.	Collect risk-appropriate KYC information and use reliable and independent data or documents to establish that the person is who they claim to be; resolve inconsistencies.	Identity attributes, source provenance, verification result, fraud checks and discrepancy resolution.	AML/CTF Act 2006, section 28; AML/CTF Rules 2025, sections 6-1 and 6-5
Verify representatives, authority and persons behind the service.	Identify a person acting for the customer and establish authority; identify any person on whose behalf the customer receives the service and apply risk-appropriate verification.	Representative KYC, mandate, underlying-person record, scope limits and activity log.	AML/CTF Act 2006, section 28(2)(b)-(c); AML/CTF Rules 2025, sections 6-5 and 6-6
Control delayed, simplified and enhanced CDD separately.	Use only an express rule, satisfy every condition, apply transaction restrictions and completion deadlines, and withdraw simplified treatment when risk or suspicion changes.	Eligibility checklist, legal source, approval, restriction tests, completion timestamp and withdrawal trigger.	AML/CTF Act 2006, sections 29-33; AML/CTF Rules 2025, sections 6-12 to 6-22

KYB, registries, and beneficial ownership

Establish legal existence, authority and the natural persons who ultimately own or control the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify legal-person or arrangement identity and existence.	Collect current name, type, identifiers, registered address, governing documents, officers or trustees and reliable registry evidence appropriate to the customer type.	ASIC or other registry extract, constitutional or trust documents, identifier checks, officer list and discrepancies.	AML/CTF Act 2006, section 28; AML/CTF Rules 2025, sections 6-2 to 6-4
Identify each natural person who ultimately owns or controls the customer.	Follow ownership chains to individuals and assess control by other means; where the Rules require it and no owner or controller is identified, establish the prescribed senior manager rather than inventing a universal percentage.	Layered ownership chart, registry sources, control analysis, verified identities and fallback rationale.	AML/CTF Act 2006, sections 5 and 28; AML/CTF Rules 2025, sections 6-7 and 6-8
Identify relevant trust and legal-arrangement parties.	For trusts or foreign equivalents, establish the trust, trustees, settlors or contributors, beneficiaries or classes, appointors, protectors and other controllers as required by the current Rules and risk.	Trust deed, party schedule, control powers, verification and change monitoring.	AML/CTF Rules 2025, sections 6-3 and 6-7
Keep AML beneficial ownership separate from company-register disclosure.	Use ASIC registers and company member records as evidence inputs, resolve nominee or non-beneficial holdings, and do not assume a public extract proves ultimate ownership or control.	ASIC extract, member register, declarations, independent corroboration and unresolved-gap escalation.	Corporations Act 2001, sections 168-178; ASIC members-register guidance; AML/CTF Act 2006, section 28

PEPs, enhanced due diligence, and remote onboarding

PEP, sanctions, high-risk and non-face-to-face exposure require risk-sensitive measures.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Establish whether relevant persons are PEPs.	Screen customers, beneficial owners, represented persons and representatives for foreign, domestic and international-organisation PEP status and applicable family or close-associate relationships.	Screening result, source, relationship map, rationale and refresh history.	AML/CTF Act 2006, section 28(2)(e); AML/CTF Rules 2025, sections 1-5 and 6-23
Apply enhanced CDD when the Act or Rules require it.	Obtain senior approval where required, corroborate source of wealth and funds, gather additional information, increase monitoring and manage unusual or high-risk services.	Trigger, approval, source corroboration, enhanced monitoring plan and reviews.	AML/CTF Act 2006, section 32; AML/CTF Rules 2025, sections 6-20 to 6-22
Control remote identity fraud and biometric processing.	Test document authenticity, liveness, impersonation and device risk; collect biometrics only where lawful, necessary and appropriately consented or otherwise authorised, and protect templates as sensitive information.	Method assessment, test results, notices, consent or authority, vendor diligence and exception review.	AML/CTF Act 2006, section 28; Privacy Act 1988, section 6 and APPs 3 and 11

Monitoring and suspicious matter reporting

Ongoing CDD and prompt suspicion decisions must feed timely AUSTRAC reporting.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing CDD and transaction monitoring.	Keep KYC and beneficial-ownership information current and scrutinise transactions against expected purpose, behaviour and risk; escalate material inconsistencies promptly.	Monitoring scenarios, alerts, case analysis, refresh record and dispositions.	AML/CTF Act 2006, section 30, and section 32 where enhanced CDD applies; AML/CTF Rules 2025, section 6-35
Form and document suspicion without waiting for proof.	Review relevant information as soon as practicable, record when reasonable grounds arose and assess provided, proposed, requested and attempted services within the statutory test.	Alert chronology, information reviewed, suspicion decision, decision-maker and legal basis.	AML/CTF Act 2006, section 41; AUSTRAC suspicious-matter-report guidance
Submit SMRs within the applicable statutory clock.	Report through AUSTRAC Online within 24 hours for terrorism-financing suspicion or within three business days after the day other suspicion is formed; apply the limited five-business-day LPP claim timing only when its conditions are met.	Suspicion timestamp, classification, SMR, submission receipt and LPP assessment if used.	AML/CTF Act 2006, section 41(2); AUSTRAC suspicious-matter-report guidance
Protect SMR information and avoid tipping off.	Restrict report, suspicion and AUSTRAC-request information to authorised need-to-know use and review any disclosure against the statutory exceptions before release.	Access controls, disclosure register, legal review, training and incident record.	AML/CTF Act 2006, sections 123 and 124

7. THRESHOLD REPORTS, TRANSFERS, AND VIRTUAL ASSETS

Threshold reports, transfers, and virtual assets

Reporting amounts, forms and transition dates are report-specific.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report covered A$10,000 physical-currency transactions.	For a designated service involving A$10,000 or more in physical currency or foreign-currency equivalent, submit a TTR within 10 business days and do not apply the amount to non-cash activity.	Cash data, currency conversion, report, submission receipt and exception analysis.	AML/CTF Act 2006, sections 5 and 43; AUSTRAC TTR guidance
Apply the correct international-transfer reporting transition.	Until the entity's IVTS reporting transition date, continue applicable legacy IFTI reporting; prepare for section 46 IVTS reporting and document any substitute transition date.	Transition analysis, transfer map, forms, submission receipts, nominated date and tests.	AML/CTF Act 2006, section 46; Transitional Rules 2026, Part 4
Carry prescribed transfer information and manage missing data.	Collect, transmit and retain required originator and beneficiary information for relevant money, property and virtual-asset transfers and apply repair, restriction or rejection procedures.	Field matrix, message samples, validation rules, exception queue and disposition.	AML/CTF Act 2006, Part 5; AML/CTF Rules 2025, transfer-of-value provisions
Register and control covered virtual-asset services.	Obtain AUSTRAC registration before providing a registrable VASP service, except where Transitional Rules 2026 section 14 permits a provider of only newly registrable services that applied by 29 July 2026 to continue pending AUSTRAC's decision; map services and travel-rule controls.	Service analysis, application timing, registration or transition eligibility, conditions, wallet and funds flows, travel-rule tests and renewal calendar.	AML/CTF Act 2006, Parts 6 and 6A; Transitional Rules 2026, section 14; AUSTRAC VASP guidance

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Australian sanctions are distinct from AML screening and require immediate control of covered assets.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen against the current Australian Consolidated List.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding, during the relationship and when DFAT updates the list; assess ownership and control beyond exact names.	List version, update logs, configuration tests, match analysis and disposition.	Charter of the United Nations Act 1945; Autonomous Sanctions Act 2011; DFAT Consolidated List
Freeze and report a covered asset as soon as possible.	Do not use, deal with or make assets available to a designated person or entity; hold a suspected freezable or controlled asset, inform the Australian Sanctions Office and notify the AFP through the official route.	Match and ownership-control analysis, freeze timestamp, ASO and AFP notifications and system blocks.	Charter of the United Nations (Dealing with Assets) Regulations 2008, regulation 42; Autonomous Sanctions Regulations 2011, regulation 24
Use permits and releases only under verified authority.	Identify the specific sanctions framework, obtain any required DFAT permit before activity and document licence conditions, expiry, reporting and release authority.	Framework analysis, permit application and decision, conditions, monitoring and release record.	DFAT sanctions framework and permit guidance

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Start each seven-year clock from the record-specific statutory event.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain CDD records for seven years from the correct trigger.	For a business relationship, retain CDD records for seven years after it ends; for an occasional transaction, retain them for seven years after completion.	Relationship and transaction end dates, retention calculation, archive sample and deletion approval.	AML/CTF Act 2006, section 111
Retain transaction and AML/CTF program records for their statutory periods.	Keep designated-service transaction records for seven years from completion and program records until seven years after they cease to be relevant to demonstrating compliance.	Record-class schedule, trigger logic, retrieval test, legal holds and deletion log.	AML/CTF Act 2006, Part 10, including sections 107 and 116
Keep records accessible in English and producible to AUSTRAC.	Use stable identifiers and controlled access so the full customer, transaction, monitoring, reporting and governance trail is promptly retrievable and convertible into English.	Sample case pack, language and conversion test, access review, request log and delivery receipt.	AML/CTF Act 2006, sections 111 and 116

Privacy, biometrics, and data breaches

Map Privacy Act coverage and applicable exceptions before processing identity or biometric data.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Collect and use KYC data under an applicable privacy basis.	Determine whether the entity is an APP entity, collect only information reasonably necessary for functions or activities, provide required notice and limit use or disclosure to the primary purpose or an applicable exception.	Coverage memo, data inventory, purpose and authority map, notice, consent and access controls.	Privacy Act 1988; APPs 1, 3, 5 and 6
Apply heightened controls to biometrics and other sensitive information.	Treat biometric information used for automated identification or verification and biometric templates as sensitive information; obtain consent unless a statutory exception applies and document necessity and proportionality.	Biometric assessment, consent or exception, minimisation, accuracy tests, security and deletion controls.	Privacy Act 1988, section 6; APP 3
Protect data and assess eligible breaches promptly.	Take reasonable security steps, contain incidents, conduct a reasonable and expeditious assessment and take all reasonable steps to complete it within 30 days after becoming aware of grounds for suspicion; notify the OAIC and affected individuals as soon as practicable when required.	Security controls, incident chronology, assessment, OAIC statement, notices and remediation.	Privacy Act 1988, APP 11 and Part IIIC, including section 26WH
Control cross-border disclosure and vendors.	Before overseas disclosure, take reasonable steps to ensure the recipient does not breach the APPs unless an exception applies; contract and monitor security, incidents, subprocessing, return and deletion.	Data-flow map, APP 8 assessment, contract, recipient diligence, monitoring and incident cooperation.	Privacy Act 1988, sections 16C and APP 8

11. PRACTICAL EVIDENCE PACKS

Practical evidence packs

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

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a reconstructable onboarding pack.	Bundle identity, authority, KYB, beneficial ownership, PEP and sanctions screening, purpose, risk, privacy records, approvals and exceptions under stable identifiers.	Complete sampled onboarding pack and retrieval result.	Operational control supporting AML/CTF Act 2006, Part 2 and section 111
Maintain a reconstructable reporting and sanctions pack.	Link transaction, alert, suspicion chronology, statutory clock, submission, acknowledgement, confidentiality, freeze actions and authority communications.	Complete sampled case pack, timeline and controlled-access record.	Operational control supporting AML/CTF Act 2006, sections 41 and 43 and Australian sanctions laws
Maintain a transition-aware launch pack.	Record the service perimeter, enrolment and registration, current or legacy CDD regime, program approval, reporting forms, transfer rules, sanctions, privacy, vendors and validation before launch.	Signed launch pack, source register, transition matrix, 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 and Counter-Terrorism Financing Act 2006 - current compilation
Federal Register of Legislation · Primary legislation
Open official source

Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 - current compilation
Federal Register of Legislation · Primary delegated legislation
Open official source

Anti-Money Laundering and Counter-Terrorism Financing Transitional Rules 2026 - current compilation
Federal Register of Legislation · Primary delegated legislation
Open official source

AML/CTF transitional rules 2026
AUSTRAC · Official transition guidance
Open official source

Changes to AML/CTF obligations from 2026
AUSTRAC · Official regulator guidance
Open official source

Initial customer due diligence overview
AUSTRAC · Official regulator guidance
Open official source

Ongoing customer due diligence overview
AUSTRAC · Official regulator guidance
Open official source

Suspicious matter reports
AUSTRAC · Official reporting guidance
Open official source

Threshold transaction reports
AUSTRAC · Official reporting guidance
Open official source

Record keeping overview
AUSTRAC · Official regulator guidance
Open official source

Virtual asset service providers overview
AUSTRAC · Official registration guidance
Open official source

ASIC company and organisation registers
Australian Securities and Investments Commission · Official registry guidance
Open official source

Company members-register requirements
Australian Securities and Investments Commission · Official registry guidance
Open official source

Australian sanctions Consolidated List
Department of Foreign Affairs and Trade · Authoritative sanctions list
Open official source

Privacy Act 1988 - current compilation
Federal Register of Legislation · Primary legislation
Open official source

Australian Privacy Principles
Office of the Australian Information Commissioner · Official privacy guidance
Open official source

Australian Privacy Principles guidelines
Office of the Australian Information Commissioner · Official privacy guidance
Open official source

FATF Australia country profile and follow-up reports
FATF · Authoritative current assessment
Open official source

Australia's fifth-round FATF mutual evaluation
Department of Home Affairs · Official evaluation-cycle guidance
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

Use of the Australian National Flag
Department of the Prime Minister and Cabinet · Official national-symbol guidance
Open official source

Document control

Version 1.3 / Published 23 September 2026 / Last reviewed 23 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 23 September 2026. Confirm the designated-service perimeter, transitional position, current Rules, AUSTRAC forms and guidance, sector licensing, sanctions measures, state or territory professional rules and privacy coverage with the competent authority and qualified Australian counsel before launch.