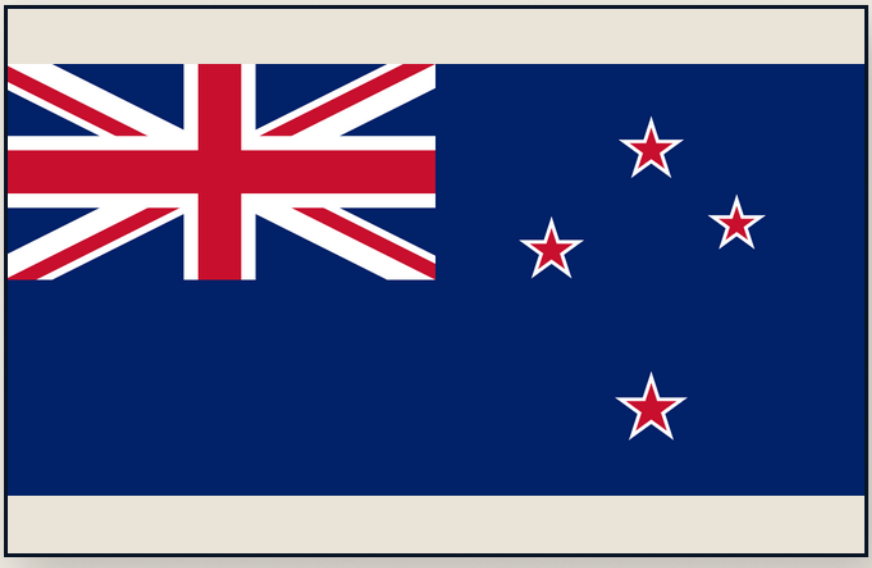
VOVE ID

VOVE COUNTRY CONTROL FILE

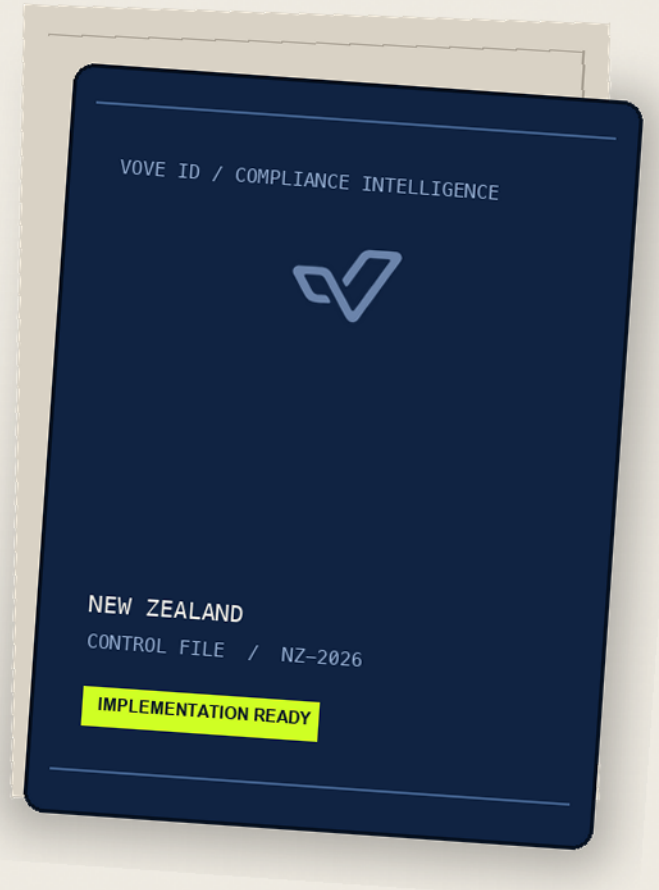
KYC / KYB / AML

2026 EDITION

NEW ZEALAND



NEW ZEALAND / NZ



KYC / KYB / AML

COMPLIANCE CHECKLIST

2026 EDITION

IMPLEMENTATION CHECKLIST / NOT LEGAL ADVICE

READ THIS FIRST

New Zealand KYC, KYB & AML Compliance Checklist

An implementation checklist for New Zealand customer due diligence, beneficial ownership, reporting, sanctions, virtual assets, privacy and biometric-processing controls under the post-July 2026 single-supervisor regime.

AML/CFT supervisor	**Department of Internal Affairs (single supervisor since 1 July 2026)**
FIU and reporting route	**New Zealand Police FIU through goAML**
SAR timing	**As soon as practicable, but no later than 3 working days after forming suspicion**
Prescribed transactions	**Physical cash NZ$10,000 or more; international wire transfer NZ$1,000 or more**
AML retention	**Generally at least 5 years; the statutory start event depends on record type**
Privacy and biometrics	**Privacy Act 2020 and Biometric Processing Privacy Code 2025, including 2026 amendments**
Payments	**No standalone e-money or payment-service licence; FSPR, dispute-resolution and product-specific duties may apply**
FATF public lists	**Not listed at 19 June 2026**

Scope and legal framework

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009, current regulations, rules, notices and codes govern reporting entities. Since 1 July 2026 the Department of Internal Affairs is the single AML/CFT supervisor; the New Zealand Police Financial Intelligence Unit receives suspicious and prescribed transaction reports.

FATF context

New Zealand was absent from the FATF increased-monitoring and call-for-action lists dated 19 June 2026. FATF's July 2024 enhanced follow-up records 9 compliant, 25 largely compliant and 6 partially compliant Recommendations. 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 29 September 2026. Confirm the reporting-entity perimeter, current rules and notices, any exemption, filing specifications, sector licensing, sanctions designation and privacy position with DIA, the FIU and qualified New Zealand 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 the actual service and New Zealand nexus before assigning controls.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether each activity makes the operator a reporting entity.	Map financial activities, casinos, specified legal, accounting, real-estate, trust-and-company, money-transfer and virtual-asset services to the current Act, regulations, rules, notices and exemptions.	Entity and service map, funds flows, customer locations, statutory analysis and counsel sign-off.	AML/CFT Act 2009, sections 5-6 and current regulations, rules, notices and exemptions
Apply the post-1 July 2026 single-supervisor model.	Register or enrol and communicate with DIA as the AML/CFT supervisor; preserve FIU reporting and law-enforcement channels separately.	DIA enrolment, supervisor correspondence, FIU registration and responsibility matrix.	AML/CFT Act 2009, sections 130-135 as amended; Ministry of Justice 2026 legislative-change guidance
Assess financial-service registration, licensing and dispute-resolution duties separately.	Map each service to the FSPR and Financial Markets Conduct Act; register and obtain any product-specific licence before service and join an approved dispute-resolution scheme where retail-service rules require it.	FSPR extract, licence analysis, approvals, scheme membership and conditions register.	Financial Service Providers (Registration and Dispute Resolution) Act 2008; FMA fintech guidance

2. GOVERNANCE AND ML/TF RISK ASSESSMENT

Governance and ML/TF risk assessment

The risk assessment and programme must be specific, current and independently tested.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Maintain a documented ML/TF risk assessment.	Assess customers, countries, institutions, products, services, transactions, delivery channels, technology and other prescribed factors; update for material change and new risk information.	Methodology, current assessment, data sources, approvals, change log and residual-risk decisions.	AML/CFT Act 2009, section 58
Maintain an AML/CFT programme based on the risk assessment.	Document CDD, monitoring, reporting, record, vetting, training, agent, correspondent, review and escalation controls proportionate to the identified risks.	Approved programme, control map, procedures, training and issue register.	AML/CFT Act 2009, sections 56-57
Appoint an AML/CFT compliance officer with sufficient access and authority.	Appoint an eligible employee or senior person, document duties and resources, and ensure governing-body visibility of material risks and breaches.	Appointment, role description, reporting packs, minutes and escalation records.	AML/CFT Act 2009, section 56
Arrange independent audit at the required risk-based interval.	Use a suitably qualified person independent of programme establishment, test design and operation, and track findings to verified closure.	Independence assessment, audit plan, report, response and closure testing.	AML/CFT Act 2009, sections 59-59B

3. NATURAL-PERSON IDENTIFICATION

Natural-person identification

CDD must cover the customer, beneficial owners and persons acting for the customer.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Apply standard CDD when the statutory circumstances arise.	Before establishing a business relationship or conducting a covered occasional transaction or activity, obtain required identity, address or registered-office, authority, nature-and-purpose and risk information unless an express timing exception applies.	CDD record, relationship purpose, risk rating, verification and completion timestamp.	AML/CFT Act 2009, sections 14-17 and 37
Identify and verify individuals using reliable, independent evidence.	Obtain full name and date of birth and take reasonable risk-based steps to verify identity; use the 2026 Identity Verification Code of Practice as a safe-harbour method only when its conditions are met.	Identity attributes, source provenance, verification result, exception rationale and fraud checks.	AML/CFT Act 2009, sections 13, 15-16 and 67; DIA Identity Verification Code of Practice 2026
Identify persons acting on behalf and verify authority.	Identify the representative, establish the relationship to the customer, take risk-based verification steps and validate the mandate before accepting instructions.	Representative KYC, mandate, authority checks, scope limits and instruction log.	AML/CFT Act 2009, sections 15-16
Do not proceed where required CDD cannot be completed.	Do not establish the relationship or conduct the transaction or activity; terminate an existing relationship when section 37 requires it and consider a suspicious activity report without tipping off.	Failure record, restriction or exit decision, SAR assessment and communications review.	AML/CFT Act 2009, section 37

KYB, registries, and beneficial ownership

Registry information is an input, not a substitute for understanding natural-person ownership and control.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Verify the legal person or arrangement and its authority structure.	Collect current name, legal form, identifier, registered office, governing documents, directors, trustees or partners and reliable registry evidence appropriate to the customer type.	Companies Register or other extract, constitutional documents, officer list and discrepancy resolution.	AML/CFT Act 2009, sections 15-17; DIA customer-due-diligence guidance
Identify and risk-appropriately verify every beneficial owner.	Determine the natural persons with effective control or who own a prescribed threshold or more; trace layered, nominee and trust arrangements and apply current DIA beneficial-ownership guidance rather than relying on the register alone.	Ownership chart, control analysis, source documents, verified identities and rationale.	AML/CFT Act 2009, sections 5, 15-16; DIA Beneficial Ownership Guidance, July 2026
Identify trust and legal-arrangement parties under the applicable CDD level.	Record trustees, settlors, beneficiaries or classes, protectors, appointors and other controllers required by law and risk; obtain source-of-funds or wealth information where enhanced CDD applies.	Trust deed, party schedule, powers analysis, verification and source evidence.	AML/CFT Act 2009, sections 22-25; DIA trust and enhanced-CDD guidance
Reconcile company records without treating them as a complete AML ownership register.	Check directors, shareholders, share parcels and ultimate holding company information; account for the public register's limits and independently resolve ultimate ownership and control.	Register extracts, company share register, declarations, independent corroboration and discrepancy log.	Companies Act 1993; Companies Office register and annual-return guidance

PEPs, enhanced due diligence, and remote onboarding

Apply enhanced measures to statutory triggers and higher-risk relationships.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Determine whether relevant persons are politically exposed persons.	Use reasonable risk-based steps to identify applicable foreign PEPs, family members and close associates; obtain senior management approval and source-of-wealth or funds measures where the Act requires them.	Screening, relationship map, approval, source corroboration and review history.	AML/CFT Act 2009, section 26
Apply enhanced CDD to each statutory trigger.	For trusts, companies with nominee shareholders or bearer shares, qualifying PEPs, higher-risk countries, unusual activity and other section 22 or 22A cases, obtain and verify the additional information required by the relevant trigger.	Trigger, additional CDD, source evidence, approval and enhanced monitoring plan.	AML/CFT Act 2009, sections 22-25
Control remote verification and biometric processing.	Assess impersonation, document authenticity and liveness; before biometric processing document lawful purpose, necessity, effectiveness, safeguards and proportionality, provide required notices and offer alternatives where the Code requires them.	Method assessment, privacy impact record, notices, alternative path, vendor tests and exception review.	Biometric Processing Privacy Code 2025, rules 1-4; DIA Identity Verification Code of Practice 2026

Monitoring and suspicious activity reporting

Ongoing scrutiny and documented suspicion timing drive FIU reporting.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Conduct ongoing CDD and account monitoring.	Regularly review relationship information, keep CDD current and examine transactions and activities for consistency with the customer's profile, purpose and risk.	Monitoring scenarios, alerts, case decisions, refresh records and quality testing.	AML/CFT Act 2009, section 31
Identify the moment reasonable grounds for suspicion arise.	Assess transactions, proposed transactions, services, attempted activity and other relevant information promptly; record the facts and timestamp without waiting for proof of an offence.	Alert chronology, information reviewed, suspicion decision and decision-maker.	AML/CFT Act 2009, sections 39A-41
Submit a suspicious activity report to the FIU on time.	File through goAML as soon as practicable and no later than three working days after forming suspicion; complete required fields and preserve the acknowledgement.	Suspicion timestamp, SAR, goAML receipt and any correction record.	AML/CFT Act 2009, sections 40-41; New Zealand Police FIU guidance
Protect SAR information and prevent tipping off.	Restrict SAR content and related information to authorised use and assess any disclosure against the statutory permissions before release.	Access controls, disclosure register, legal review, training and incident log.	AML/CFT Act 2009, sections 46-47

Prescribed transactions, wires, and virtual assets

Thresholds are report-specific and do not replace suspicious-activity assessment.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Report prescribed large cash transactions.	Report a transaction involving NZ$10,000 or more in physical currency, or foreign-currency equivalent, through goAML within the prescribed period and retain the submission trail.	Cash data, aggregation and conversion logic, PTR and receipt.	AML/CFT Act 2009, sections 48A-48B; Prescribed Transactions Reporting Regulations 2016; FIU PTR guidance
Report prescribed international wire transfers.	Report an international wire transfer of NZ$1,000 or more, or foreign-currency equivalent, through goAML within the prescribed period; distinguish ordering, intermediary and beneficiary roles.	Transfer fields, role analysis, currency conversion, PTR and receipt.	AML/CFT Act 2009, sections 48A-48B; Prescribed Transactions Reporting Regulations 2016; FIU PTR guidance
Carry and verify required wire-transfer information.	Collect, include, retain and review prescribed originator and beneficiary information and apply controls for missing or incomplete data.	Field matrix, message samples, validation rules, repair queue and dispositions.	AML/CFT Act 2009, sections 27-28; current requirements regulations
Map virtual-asset services to AML and financial-service obligations.	Treat covered cryptoasset exchange, transfer, custody or related services as likely financial-institution activity; assess DIA supervision, FSPR registration, dispute resolution and any FMC licensing before launch.	Service and wallet-flow analysis, DIA position, FSPR record, licensing memo and monitoring tests.	AML/CFT Act 2009, section 5 definition of financial institution; FMA cryptoasset-service-provider guidance

8. TARGETED FINANCIAL SANCTIONS

Targeted financial sanctions

Sanctions and terrorist-property controls apply separately from AML screening.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Screen current United Nations, terrorist and New Zealand sanctions designations.	Screen customers, beneficial owners, controllers, representatives and transactions at onboarding and on list changes; assess ownership and control rather than exact-name matches only.	List versions, update logs, configuration tests, match analysis and disposition.	United Nations Act 1946; Terrorism Suppression Act 2002; Russia Sanctions Act 2022
Stop prohibited dealings and report terrorist property.	Do not make property or financial services available contrary to applicable prohibitions; freeze or hold where legally required and promptly use the Police/FIU reporting route for suspicious property or sanctions-related reports.	Match analysis, restriction timestamp, report, authority correspondence and release approval.	Terrorism Suppression Act 2002, including sections 9-10 and 43; applicable sanctions regulations
Use exemptions, permits or releases only under verified authority.	Identify the governing sanctions regime, obtain written authority before activity, implement conditions and document expiry, reporting and release decisions.	Regime analysis, permit or exemption, conditions, monitoring and release record.	Applicable regulations under the United Nations Act 1946 and Russia Sanctions Act 2022

9. RECORDS AND REGULATOR ACCESS

Records and regulator access

Apply the correct five-year trigger to each record class and preserve retrieval.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Retain transaction records for at least five years from completion.	Keep records sufficient to reconstruct covered transactions and identify the parties, amounts, dates and nature; apply longer legal holds where required.	Retention schedule, transaction sample, trigger calculation, legal hold and deletion log.	AML/CFT Act 2009, sections 49 and 52-55
Retain identity and verification records for the statutory period.	Keep CDD and verification records for at least five years after the end of the business relationship or completion of the occasional transaction or activity, as applicable.	Relationship-end or completion date, archive sample, retrieval test and deletion approval.	AML/CFT Act 2009, section 50 and sections 52-55
Preserve SAR, programme, risk and audit evidence.	Keep SAR and prescribed-report material, risk assessments, programmes, audits and supporting records for the applicable statutory periods in readily retrievable form.	Record-class matrix, access controls, sample case pack and DIA production test.	AML/CFT Act 2009, sections 49A and 51-55

10. PRIVACY, BIOMETRICS, AND TRANSFERS

Privacy, biometrics, and transfers

KYC processing must satisfy the Privacy Act and any applicable biometric rule.

CONTROL	IMPLEMENTATION ACTION	EVIDENCE	SOURCE
Collect and use identity data for a lawful, necessary purpose.	Map each data element to a lawful function, collect no more than necessary, give required collection notice, maintain accuracy and restrict later use and disclosure.	Data inventory, purpose and authority map, notices, access controls and accuracy reviews.	Privacy Act 2020, information privacy principles 1-8 and IPP 3A
Comply with the Biometric Processing Privacy Code.	Before using automated biometric verification, assess necessity, effectiveness and proportionality, implement privacy safeguards, provide clear notice and control use, disclosure, security, retention and disposal under the Code.	Biometric assessment, safeguards, notices, alternatives, accuracy tests, vendor review and deletion controls.	Biometric Processing Privacy Code 2025, as amended in 2026
Assess and notify notifiable privacy breaches.	Contain and assess incidents promptly; notify the Privacy Commissioner and affected people as soon as practicable when serious harm has occurred or is likely, unless a statutory exception applies.	Incident chronology, harm assessment, notifications, exception analysis and remediation.	Privacy Act 2020, sections 112-122
Control overseas disclosures and processors.	Before disclosing personal information outside New Zealand, satisfy IPP 12 through comparable safeguards, qualifying recipient status or informed authorisation; contract for security, incidents, return and deletion.	Transfer map, IPP 12 analysis, contract, recipient diligence and monitoring.	Privacy Act 2020, information privacy principle 12

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 results, purpose, risk, privacy records, approvals and exceptions under stable identifiers.	Complete sampled onboarding pack and retrieval result.	Operational control supporting AML/CFT Act 2009, sections 11-38 and 50
Maintain a reconstructable FIU and sanctions case pack.	Link activity, alert, suspicion chronology, threshold analysis, submission, acknowledgement, confidentiality, asset restrictions and authority communications.	Complete sampled case pack, timeline and controlled-access record.	Operational control supporting AML/CFT Act 2009, sections 40-55 and Terrorism Suppression Act 2002
Maintain a launch and change pack.	Record perimeter, DIA enrolment, FSPR or licensing, approved programme, reporting connectivity, sanctions, privacy, vendors, testing and unresolved uncertainty before launch or material change.	Signed launch pack, source register, tests, approvals and uncertainty log.	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 Countering Financing of Terrorism Act 2009 - current version
New Zealand Legislation · Primary legislation
Open official source

Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Regulations 2011
New Zealand Legislation · Primary delegated legislation
Open official source

Anti-Money Laundering and Countering Financing of Terrorism (Prescribed Transactions Reporting) Regulations 2016
New Zealand Legislation · Primary delegated legislation
Open official source

2026 AML/CFT legislative changes
Ministry of Justice · Official reform guidance
Open official source

AML/CFT guidance library for trust and company service providers
Department of Internal Affairs · Official supervisor guidance
Open official source

AML/CFT frequently asked questions
Department of Internal Affairs · Official supervisor guidance
Open official source

Identity Verification Code of Practice 2026
Department of Internal Affairs · Official code guidance
Open official source

New Zealand Financial Intelligence Unit
New Zealand Police · Official FIU guidance
Open official source

Prescribed Transactions Reporting
New Zealand Police · Official reporting guidance
Open official source

Companies Register search guidance
New Zealand Companies Office · Official registry guidance
Open official source

Companies Register annual-return guidance
New Zealand Companies Office · Official registry guidance
Open official source

Privacy Act 2020 - current version
New Zealand Legislation · Primary legislation
Open official source

Biometric Processing Privacy Code 2025
Office of the Privacy Commissioner · Official privacy code
Open official source

Terrorism Suppression Act 2002 - current version
New Zealand Legislation · Primary legislation
Open official source

Russia Sanctions Act 2022 - current version
New Zealand Legislation · Primary legislation
Open official source

Fintech regulatory and licensing requirements
Financial Markets Authority · Official licensing guidance
Open official source

Cryptoasset service providers
Financial Markets Authority · Official sector guidance
Open official source

E-money and payment service providers
Financial Markets Authority · Official sector guidance
Open official source

FATF New Zealand country profile and 2024 follow-up
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

New Zealand flag - use in advertising
Manatu Taonga Ministry for Culture and Heritage · Official national-symbol guidance
Open official source

Document control

Version 1.0 / Published 29 September 2026 / Last reviewed 29 September 2026 / Owner: VOVE ID Compliance Research

General regulatory information, not legal advice or a licence determination. Reviewed as applicable on 29 September 2026. Confirm the reporting-entity perimeter, current rules and notices, any exemption, filing specifications, sector licensing, sanctions designation and privacy position with DIA, the FIU and qualified New Zealand counsel before launch.