PART 1 - AML/CTF Policy document

Anytime Conveyancing

Version control

Version	Date approved	Approved by	Summary of changes	Next review due
1.0	2/03/2026		This Policy document is based on, and represents a digital adaptation of, the AUSTRAC Starter Kit issued on 29/01/2026.	Click or tap to enter a date.
	Click or tap to enter a date.			Click or tap to enter a date.
	Click or tap to enter a date.			Click or tap to enter a date.
	Click or tap to enter a date.			Click or tap to enter a date.
	Click or tap to enter a date.			Click or tap to enter a date.

When we update this Policy document, we keep the previous version for 7 years.

Table of contents

Policy

Our practice has anti-money laundering and counter-terrorism financing (AML/CTF) obligations. These obligations apply when we provide the following services:

- conveyancing services: assisting in the planning or execution of a transaction to sell, buy or transfer real estate
- professional services: assisting in the planning or execution of a transaction to sell, buy or transfer a body corporate or legal arrangement

These services carry very different risks and are referred to throughout this Policy document as 'conveyancing services', 'professional services' or, when referred to collectively, 'designated services'.

What's in our policies

This Policy document details what our practice does, and when, to meet our AML/CTF obligations. It doesn't restate these obligations. Instead, it outlines the practical framework we use to meet them.

There are 3 parts to this Policy:

- Part 1: Personnel
- Part 2: Clients
- Part 3: Maintain our AML/CTF program.

How this works as part of our starter kit

This Policy document is supported by the:

- Risk assessment that describes the money laundering, terrorist financing and proliferation financing risks (known as ML/TF risks) faced by our practice
- process documents and forms that describe the steps our practice takes to comply with our obligations day-to-day.

These documents work together to meet our obligations to:

- manage the personnel we have in AML/CTF roles (such as our AML/CTF compliance officer)
- manage and mitigate the ML/TF risks posed by our clients
- report to AUSTRAC
- maintain our AML/CTF program to make sure it remains effective and stays up to date as ML/TF risks change.

Once approved, our practice must follow these policies.

Key terms and references

Risk assessment, forms and processes

Alongside the Process document, we are using TriSearch's AML solution to help put this Policy document into practice. Where we refer to relevant processes and forms, we highlight their names like this.

Where we refer to using a form or process, this either means using it directly or using the steps in the form or process in our own systems.

Where this policy refers to our Risk assessment, it means:

- for conveyancing services – the conveyancing Risk assessment
- for other professional services – the professional services Risk assessment

Material change

We use the term material change in this document. When we use this term, we mean that we've made updates to a process or document that impacts an outcome of complying with AML/CTF obligations and managing or mitigating ML/TF risks.

For example, carrying out a routine software update on this system, or a change in workflow to the order investigators see in a case management tool, aren't a material change to how the practice complies with its obligations or manages or mitigates risk. It doesn't involve minor changes, such as fixing typos and links.

Reasonable

Where we use the word reasonable, such as reasonable steps or reasonable grounds for suspicion, this means that a reasonable person in our position would have taken those steps or formed that suspicion based on the facts, circumstances and information available.

A reasonable person refers to a hypothetical person who displays reasonable or ordinary behaviour or judgement in the circumstances.

Single employee practice

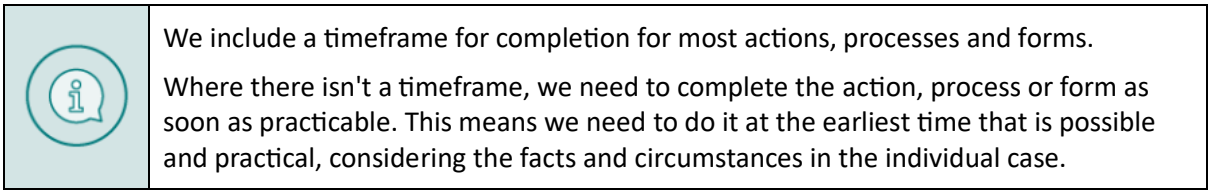
When we use the term single employee practice, we mean that only one person is working for the practice.

Escalating to an AML/CTF compliance officer

Where we refer to escalating something to an AML/CTF compliance officer, we mean where it's detected by:

- the compliance officer - they action the matter themselves
- other personnel - they escalate it to the compliance officer using either the:
    - Unusual activity report functionality within TriSearch's AML solution (for potential suspicious matters)
    - Escalation functionality within TriSearch's AML solution (for all other matters).

Timeframes



We include a timeframe for completion for most actions, processes and forms.

Where there isn't a timeframe, we need to complete the action, process or form as soon as practicable. This means we need to do it at the earliest time that is possible and practical, considering the facts and circumstances in the individual case.

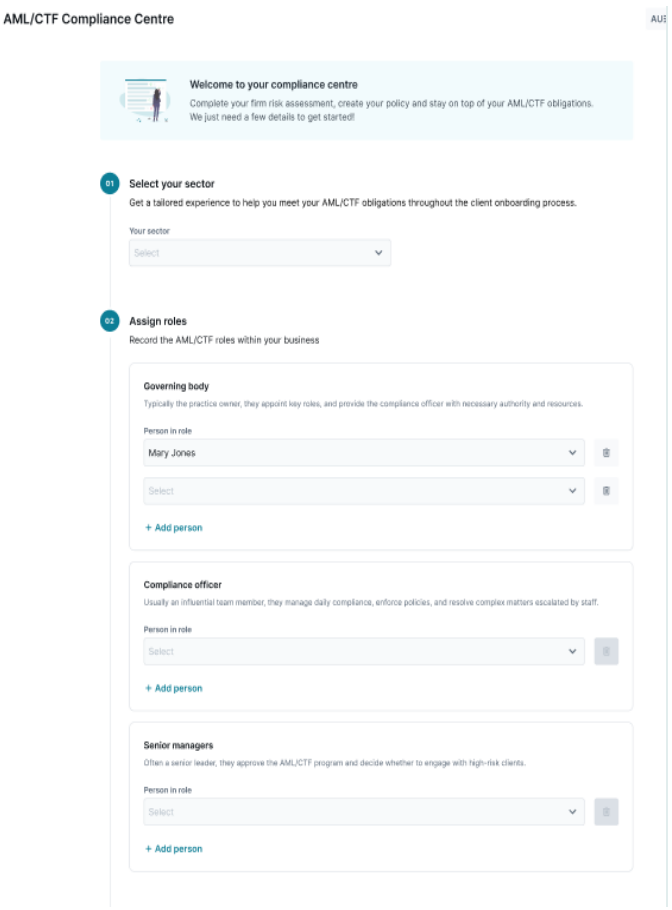
1 2 3

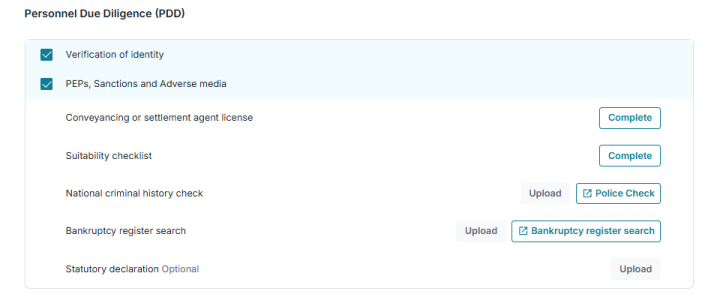
Part 1: Personnel

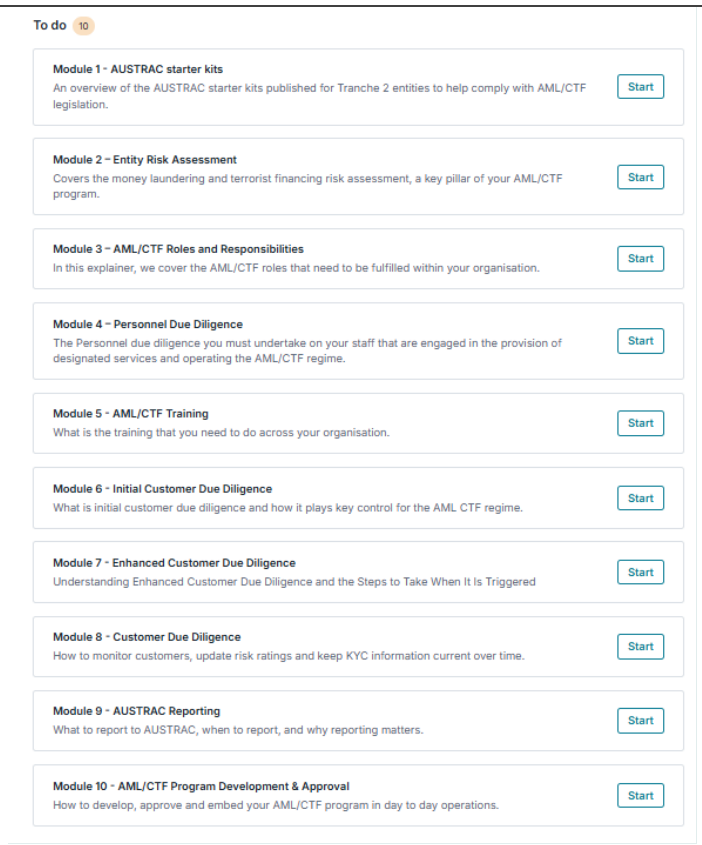
This section details how we'll appoint, support and manage the people responsible for our AML/CTF program.

What's in this section

This part has 3 sections. This table summarises the sections and the corresponding policies.

Section	Actions	Policy, tools and guidance
1. Align personnel to roles	Identify who will hold each key role: • governing body • senior manager • AML/CTF compliance officer • client-facing personnel. Assign responsibility for meeting the AML/CTF obligations to each role we've identified.	**Fill key AML/CTF roles policy** Processes and forms: • AML/CTF roles and responsibilities are captured digitally within TriSearch's AML platform. • Example of TriSearch system page where roles are captured:  Guidance:

		• Governance
2. Conduct personnel due diligence	Before confirming appointment, make sure individuals are suitable and meet the requirements for their roles. Make sure they remain suitable by conducting ongoing personnel due diligence. If a person in an AML/CTF role is no longer suitable, take appropriate action.	**Personnel due diligence policy** Processes and forms: We are using TriSearch's AML solution to perform and keep a record of following: • Personnel due diligence • Personnel due diligence for AML/CTF compliance officer • Personnel due diligence where the compliance officer and governing body are the same person form (for single employee practices to meet the policy). Example of TriSearch system page where personnel due diligence is facilitated:  Guidance: • Governance • Personnel due diligence
3. Deliver personnel training	Plan and deliver training to make sure our personnel understand their AML/CTF obligations and can apply the program in their day-to-day work.	We are using TriSearch's AML solution to meet personnel training obligations. TriSearch's AML training modules provide a comprehensive coverage of the AML and obligatory topics, which is mandatory for each personnel to complete. Training completion and progress is tracked within the platform. Example of TriSearch system where module-based training is facilitated:

		 To do 10 Module 1 - AUSTRAC starter kits An overview of the AUSTRAC starter kits published for Tranche 2 entities to help comply with AML/CTF legislation. Start Module 2 – Entity Risk Assessment Covers the money laundering and terrorist financing risk assessment, a key pillar of your AML/CTF program. Start Module 3 – AML/CTF Roles and Responsibilities In this explainer, we cover the AML/CTF roles that need to be fulfilled within your organisation. Start Module 4 – Personnel Due Diligence The Personnel due diligence you must undertake on your staff that are engaged in the provision of designated services and operating the AML/CTF regime. Start Module 5 - AML/CTF Training What is the training that you need to do across your organisation. Start Module 6 - Initial Customer Due Diligence What is initial customer due diligence and how it plays key control for the AML CTF regime. Start Module 7 - Enhanced Customer Due Diligence Understanding Enhanced Customer Due Diligence and the Steps to Take When It Is Triggered Start Module 8 - Customer Due Diligence How to monitor customers, update risk ratings and keep KYC information current over time. Start Module 9 - AUSTRAC Reporting What to report to AUSTRAC, when to report, and why reporting matters. Start Module 10 - AML/CTF Program Development & Approval How to develop, approve and embed your AML/CTF program in day to day operations. Start

1. Fill key AML/CTF roles

This section shows what we do to make sure our personnel are:

- appointed to AML/CTF roles
- eligible for those roles
- able to carry out the key duties of those roles.

If we become a single employee practice, one person will be doing all these roles.

1. Appoint people to key roles

1.1. We have eligible personnel in the following key AML/CTF roles:

a) governing body

b) senior manager(s)

c) AML/CTF compliance officer

d) any other personnel who will meet our AML/CTF obligations. This includes client-facing personnel (who need to monitor their activity).

1.2. We appoint eligible personnel to these roles by both:

a) completing the relevant Personnel due diligence using TriSearch's AML solution at 1.1 of the **Personnel due diligence policy**

b) keeping up to date records of who is in each role within TriSearch platform.

1.3. We appoint a suitable AML/CTF compliance officer no later than the following timeline (starting from 1 July 2026), within 28 days of:

a) providing designated services

b) our AML/CTF compliance officer becoming ineligible, changing roles or leaving our practice.

1.4. We notify AUSTRAC via AUSTRAC Online within 14 days of appointing a new AML/CTF compliance officer.

2. Responsibilities of the key roles

2.1. We assign responsibility for meeting our AML/CTF obligations to each key role using TriSearch platform.

2.2. We make sure personnel in each AML/CTF role meet their responsibilities on an ongoing basis.

2. Personnel due diligence

We conduct personnel due diligence (PDD) to make sure all personnel in key AML/CTF roles are suitable for their position and can meet their obligations.

1. Initial PDD

1.1. We complete initial PDD on personnel when any of the following occurs:

a) before new or existing personnel start in a key AML/CTF role, including when they move from one role to another (for example, compliance officer takes on senior manager role)

b) when there's a change in circumstance that may affect the suitability of personnel to perform the role. Such as criminal charges, financial distress, conflicts of interest or suspicious behaviour.

1.2. We complete initial PDD by filling out the following forms for the following roles:

Role	Relevant form or digital platform
Single employee practice, or Governing body is also our AML/CTF compliance officer	Personnel due diligence is done using TriSearch platform where the compliance officer and governing body are the same.
AML/CTF compliance officer who isn't also the governing body	Personnel due diligence for AML/CTF compliance officer is done using TriSearch platform.
For all other AML/CTF roles	Personnel due diligence is done using TriSearch platform.

2. Ongoing PDD

2.1. If we identify circumstances that may impact a person's ability to carry out an AML/CTF role, we reassess the suitability of that person. This includes their:

a) integrity – may include criminal investigations or charges, significant changes in financial arrangements, conflicts of interest or secondary employment

b) competence – performance reviews, training outcomes and observed conduct.

2.2. Our personnel in AML/CTF roles self-report any circumstances that may impact their suitability to hold this role.

2.3. We collect and verify any additional information we need to be satisfied that the person is still suitable for the role.

2.4. We record the results of ongoing personnel due diligence using the fields of the forms referred to at section 1.2 of this policy.

3. When personnel aren't suitable

3.1. Where we've assessed a person as not being suitable for a role, we take one or more of the following actions, as appropriate:

Issue	Treatment
Minor integrity concern	Take action to lower the risk this person will be exploited by criminal networks or reassign to a less important AML/CTF role
Significant integrity concern	Remove from AML/CTF-related duties
Minor competency issues	Correct through targeted training, formal warnings, disciplinary actions or reassign to a less difficult AML/CTF role

Issue	Treatment
Significant competency issues	Provide the support needed to make sure they gain the skills needed to perform their role. Or replace them in this role with someone with the required skills
Ineligible for a key AML/CTF role For example, an AML/CTF compliance officer is no longer an Australian resident	Make sure the role is filled by an eligible person

3. Personnel training

We train our personnel to make sure they can carry out their AML/CTF roles and responsibilities.

As a policy, we are using TriSearch's AML training module, which is a digital and has coverage across different training topics and requirements as outlined below.

1. Initial training

1.1. Personnel starting in an AML/CTF role, or transferring into a role, complete training that's relevant to that role and the responsibilities assigned to it under the roles and responsibilities as noted within TriSearch platform.

1.2. Personnel who don't complete mandatory training within the required timeframe may face disciplinary action.

1.3. Our AML/CTF compliance officer verifies that new starters have completed the required training before granting system access to AML/CTF related platforms.

2. Ongoing training

2.1. Our AML/CTF compliance officer assesses each personnel's AML/CTF competency in their assigned roles and responsibilities. If:

a) a person meets their responsibilities – only training about material changes to this program are needed

b) deficiencies in competency are identified – targeted training is provided to address them

c) deficiencies cannot be corrected through training – the role is reassigned.

2.2. Our personnel complete training that's specific to their AML/CTF role on any material changes to our AML/CTF program.

3. Training content and delivery

3.1. Our AML/CTF compliance officer determines the content, delivery format and frequency of training.

3.2. We develop training to help personnel understand:

a) the ML/TF risks we may reasonably face in providing designated services and indicators of criminal exploitation

b) the specific AML/CTF obligations that must be met in their role

c) how to apply the processes in our AML/CTF program to meet these obligations.

3.3. Training includes scenario-based exercises to test understanding and decision making.

3.4. When using third-party training providers, our AML/CTF compliance officer assesses and approves the content to make sure it meets our AML/CTF training requirements.

4. Role-specific training requirements

4.1. For personnel with an AML/CTF role, our training covers how to:

a) identify ML/TF risks and indicators of criminal activity, and the ML/TF risks we're willing to take on, as outlined in the Risk assessment

b) use this information to risk rate clients, identify suspicious matters, restrict service offerings and offboard clients as outlined in this Policy document

c) handle confidential material relating to reporting and avoid **tipping off**

d) meet our customer due diligence obligations when onboarding clients and throughout the course of our business relationship

e) detect and escalate matters that must be referred to our AML/CTF compliance officer

f) meet any other obligations assigned to the role.

5. Training program reviews and updates

5.1. Our AML/CTF compliance officer reviews training materials if:

a) ML/TF risks change

b) material changes are made to our AML/CTF program

c) AUSTRAC releases communications relevant to our practice.

5.2. Our training materials reflect all relevant updates, including regulatory changes, emerging ML/TF risks and changes to our practice processes.

1 2 3

Part 2: Clients

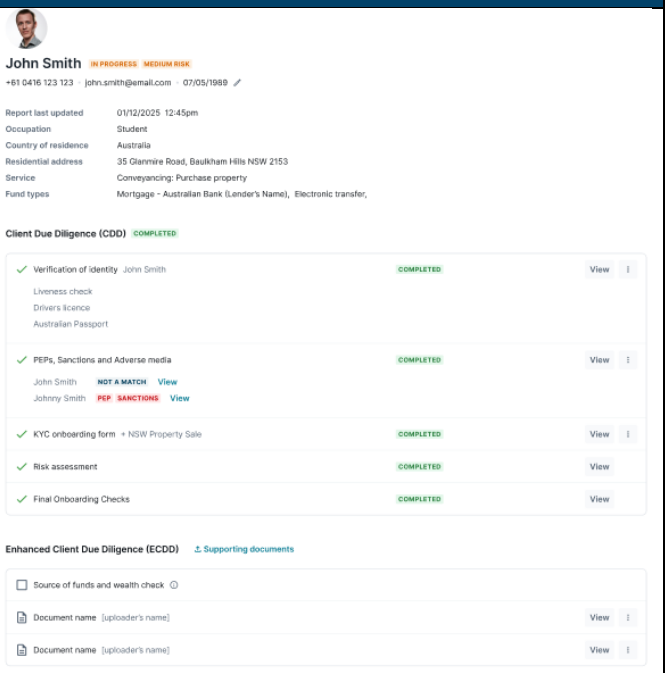
This section details how to:

- deal with clients
- conduct customer due diligence (CDD)
- report to AUSTRAC.

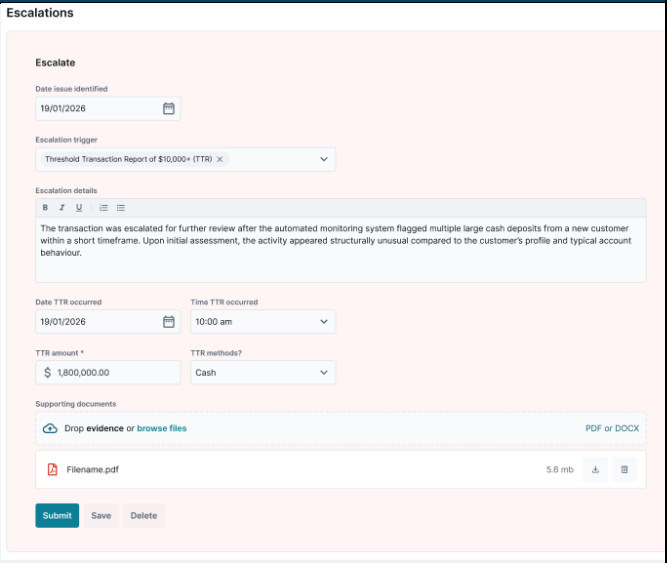
What's in this section

This part has 7 sections. This table summarises the sections and the corresponding policies.

Section	Actions	Policy, tools and guidance
1. Initial customer due diligence	Conduct initial CDD before starting to provide a client with a designated service. Follow the policy and: • Identify the kind of client - if they're an individual, trust, body corporate or government body. This determines the client forms we use. • Use the Onboarding form for the service requested to collect information from a client. • Use the Initial CDD form for the service requested to	Initial customer due diligence policy Processes and forms: We use TriSearch's AML solution to perform client due diligence, including initial, ongoing and enhanced due diligence, whereby the checks are performed digitally. In relation to the initial customer due diligence, we do the following: • Collect KYC information using TriSearch's digital form, in line with Onboarding form outlined in the AUSTRAC starter kit. • Verification of Identity and PEP, Sanction and Adverse Media check using TriSearch, aligned to AUSTRAC Initial customer due diligence form. Example of TriSearch system where CDD is facilitated:

Section	Actions	Policy, tools and guidance
	complete initial CDD. We'll complete more checks for complex and high-risk clients.	 Guidance: • Initial customer due diligence
2. Ongoing customer due diligence	Follow the policy to: • monitor our client's activity and changes in their information or ML/TF risk throughout our relationship • take appropriate action to mitigate and manage their ML/TF risks. • Use the client forms to record the results of:	**Ongoing customer due diligence policy** Processes and forms: We use TriSearch's AML solution to perform ongoing monitoring on customer. This includes periodically rechecking the identity of the customer, PEP, Sanctions and Adverse media checks as performed through TriSearch in accordance with • Trigger event review and update form • Periodic review and update form Guidance: • Ongoing customer due diligence

Section	Actions	Policy, tools and guidance
	• reviews triggered by changes in client information or ML/TF risk factors • periodic reviews of client information and ML/TF risk. We must conduct periodic reviews if we still have a business relationship with the client every: • year for high-risk clients • 2 years for medium-risk clients • 3 years for low-risk clients.	
3. Pre-commencement customer due diligence	Complete appropriate due diligence on all clients we were providing a designated service to on 1 July 2026.	**Pre-commencement customer due diligence policy**
4. Dealing with high risk or complex clients	We escalate the following to our AML/CTF compliance officer to action: • high-risk clients • reportable matters (see step 5) • positive sanctions checks • difficult beneficial	**Escalation and enhanced CDD policy** Our Escalation and enhanced customer due diligence process is managed using TriSearch platform. TriSearch's Escalation functionality has digitised the following forms and process. Example of TriSearch system where Escalation process is managed:

Section	Actions	Policy, tools and guidance
	ownership checks • kinds of services, clients, delivery channels, countries or ML/TF risks not in our Risk assessment .	 Processes and forms: • Escalation checklist process • Escalation register • Enhanced CDD form Guidance: • Reporting to AUSTRAC • Review and update your program • Enhanced CDD
5. Report to AUSTRAC	We use this policy to report the following to AUSTRAC. • suspicious matters • any physical currency transaction , or cross-border movement of physical currency and/or bearer negotiable instruments, valued at $10,000 or more • annual compliance reports.	**Reporting policy** Processes and forms: • Escalation checklist • Unusual activity information form • Unusual activity report review form • Annual compliance report process Guidance: • Reporting to AUSTRAC

Section	Actions	Policy, tools and guidance
6. Tipping off	Don't let clients know we think their behaviour is suspicious.	**Tipping off policy** Guidance: • Tipping off
7. Offboarding	Decline or stop providing services where clients fall outside our risk appetite or would cause us to fail to meet our AML/CTF obligations. Follow the policy and our risk appetite statement in the Risk assessment.	**Offboarding policy**

1. Initial customer due diligence

We complete initial customer due diligence (initial CDD) to:

- identify our clients and their representatives, beneficiaries and beneficial owners
- identify our clients' ML/TF risk
- manage and mitigate this ML/TF risk.

1. When we complete initial CDD

1.1. We complete initial CDD for conveyancing services before acting on instructions under a retainer agreement and before the following event (whichever happens first):

a) in a private treaty or where an auction doesn't meet reserve - when a buyer and seller, verbally or in writing, agree to the sale price of the property prior to the payment of any deposit or the exchange of any contract

b) in an auction that meets reserve, at the point a buyer is successful at auction.

1.2. We complete initial CDD for other professional services before we start to provide those services.

1.3. To ensure we meet this deadline, we can start completing initial CDD from the moment it is reasonable to conclude that an engagement may involve providing a professional service.

1.4. For conveyancing services, this is generally:

a) For the seller – Before acting on instructions under a retainer agreement

b) For the buyer – when the event at 1.1 occurs, as it is often not reasonable to conclude that a buyer will be successful in securing real estate until the moment they are successful (whether at auction or under private treaty). This means that it is generally necessary to delay initial CDD until the earlier of:

a. as soon as practicable
b. 15 days after exchange of contracts
c. before settlement.

The typical timeframes where a designated service will start to be provided are provided in AUSTRAC guidance.

Our relationships with clients, and the services we provide to them, are often fluid, changing throughout the course of the business relationship. We often won't be certain as to whether a professional service is going to be provided until just before it is requested or a person is successful in securing real estate.

Under the Privacy Act 1988 (Cth), we can collect personal information when it is reasonably necessary for our functions and activities, including to meet our legal obligations (Australian Privacy Principle 3.2).

The meaning of 'reasonably necessary' is further discussed in Chapter B: Key concepts and Chapter 3: APP 3 Collection of solicited personal information of the Office of the Australian Information Commissioner's APP guidelines. In addition to when personal information can be collected to meet AML/CTF obligations, reporting entities will also need to consider other factors set out in the OAIC's APP guidelines, including the amount of information needed to complete initial CDD (to avoid overcollection of personal information).

To comply with our obligations as set out in paragraphs 1.1 and 1.2, we can complete initial CDD in the window between:

- reasonably concluding that an engagement may involve providing a designated service

	• starting to provide a designated service. For example, if a seller of real estate approaches us seeking conveyancing services, we may conclude that they are very likely to be successful in selling their property, so complete initial CDD during client intake. For a prospective buyer of real estate, however, it is often uncertain as to whether they will be successful. For these buyers, we may use the delayed initial CDD parts of the conveyancing Initial CDD form to complete initial CDD on them after finding out that they were successful.

2. When we can delay initial CDD

2.1. We can delay initial CDD if permitted under:

a) For conveyancing services: the relevant conveyancing Initial CDD form

b) For other professional services: the relevant professional services Initial CDD form

2.2. We don't delay initial CDD just because the timeframes are inconvenient for us or our clients.

2.3. When we delay initial CDD, we do all of the following:

a) complete initial CDD in the permitted timeframe under the relevant Initial CDD form mentioned at section 2.1

b) don't deal with the client's money, property or virtual assets (other than holding in an account or on deposit) or make money, property or virtual assets available to them, before initial CDD is completed

c) mark contracts, correspondence and other documents issued to the client with the words 'unverified client'

d) any other actions that are appropriate to mitigate and manage the ML/TF risk.

3. How we complete initial CDD

3.1. We complete initial CDD for conveyancing services by doing all of the following:

a) determine if our client is an individual, body corporate, partnership, unincorporated association, trust or government body

b) collect the information in the conveyancing KYC Onboarding form through TriSearch, in line and in accordance with the Onboarding form for that kind of client

c) perform initial CDD through TriSearch, in line and in accordance with the conveyancing Initial CDD form for that kind of client

d) if required, work with another conveyancer or real estate agent to verify client information through TriSearch, in line and in accordance with the Request to verify information form

3.2. We complete initial CDD for other professional services by doing all of the following:

a) determine if our client is an individual, body corporate, partnership, unincorporated association, trust or government body

b) collect the information in the professional services through TriSearch, in line and in accordance with the Onboarding form for that kind of client

c) perform initial CDD through TriSearch, in line and in accordance with the professional services Initial CDD form for that kind of client

3.3. If any of the events at paragraph 1.1 of the **Escalation and enhanced CDD policy** occur, we escalate them to our AML/CTF compliance officer to action before completing initial CDD. We stop providing designated services until the compliance officer notifies us that we can continue.

3.4. This includes any of the following:

a) potential suspicious matters

b) high-risk clients

c) a new client, designated service, delivery channel, country or ML/TF risk factor, method or indicator that isn't in our Risk assessment

d) complex beneficial ownership checks

e) a positive match on a sanctions check.

3.5. If any of the events at paragraph 1.2 of the **Escalation and enhanced CDD policy** occur, we escalate this to our AML/CTF compliance officer to report but we don't need to stop providing designated services.

3.6. This includes any of the following valued at $10,000 or more (or the foreign currency equivalent):

a) physical currency (including notes and coins) transaction

b) cross-border movement of physical currency and/or bearer negotiable instruments.

2. Ongoing customer due diligence

We follow these policies to manage and mitigate our client's ML/TF risks from the moment they approach us for a designated service and throughout the course of our business relationship.

While we remain in a business relationship with a client, we:

- monitor them for reportable activity and changes in ML/TF risk
- review their information periodically and in response to triggers.

As a reminder, where this policy refers to a Risk assessment, it means:

- for conveyancing services – the conveyancing Risk assessment
- for professional services – the professional services Risk assessment

1. Ongoing customer due diligence

1.1. We monitor our client for all of the following:

a) unusual transactions and behaviours

b) any significant changes in the client's ML/TF risk, the information we've collected and verified on them or the nature of the business relationship

c) any matters referred to in the **Escalation and enhanced CDD policy**.

1.2. We record sufficient information about our clients, related transactions and behaviours to support effective monitoring. This includes, but isn't limited to, comparing information recorded from monitoring against:

a) any present ML/TF risk factors, ML/TF methods and indicators and indicators of unusual or criminal behaviour listed in our Risk assessment

b) any physical currency transaction, or cross-border movement of physical currency and/or bearer negotiable instruments, valued at $10,000 or more (or the foreign currency equivalent)

c) general client information, including previous transactions and behaviour recorded throughout the business relationship. This establishes a baseline for what is 'normal' and 'unusual' behaviour for each client.

2. Periodic client reviews

2.1. We do periodic reviews of the client's information by completing the Periodic review and update form.

2.2. Where a periodic review identifies that updates are needed to a client's information or ML/TF risk rating, we make these updates to make sure our client information is accurate and complete.

2.3. We conduct reviews at the following frequency, starting from the date that initial CDD was last completed on the client:

a) High risk client – Every 12 months

b) Medium risk client – Every 2 years

c) Low risk client – Every 3 years

2.4. If the review period has expired, we complete the periodic review before we continue to provide designated services to the client if we have doubts about the accuracy of existing client information. If we don't have doubts about the accuracy of existing client information, we complete the periodic review as soon as practicable.

2.5. As most designated services are resolved within 12 months, for many of our clients no periodic review is needed.

2.6. We conduct more frequent periodic reviews if justified by client activity or risk.

3. Triggers for review

3.1. We conduct a review of the client's information and ML/TF risk ratings by completing the Trigger event review form if any of the following occur:

a) there's been a change in our relevant Risk assessment which impacts how we identify and assess client ML/TF risk

b) there's a change in our client's details and beneficial ownership (for body corporates, government bodies and legal arrangements, who owns or controls them)

c) our client requests a new conveyancing service

d) our client becomes, or is identified as a foreign PEP, or a high-risk domestic or international organisation PEP

e) our client becomes a person designated for targeted financial sanctions

f) we identify unusual transactions or behaviours listed in our Risk assessment through client monitoring

g) any other event that causes us to question if the client's information or ML/TF risk rating is accurate, current or adequate.

3.2. If our triggered review identifies that we need to update the client's information or ML/TF risk rating, we make these updates to ensure our client information remains accurate and complete.

3. Pre-commencement customer due diligence

We conduct lighter due diligence on clients who were receiving designated services on 1 July 2026 (these are called pre-commencement customers).

1. Pre-commencement customers

1.1. We monitor these clients for changes in the nature and purpose of our business relationship which may result in any of the triggers under the **Escalation and enhanced CDD policy**.

1.2. If a suspicious matter report is submitted about the client during this business relationship, we complete initial CDD under the **Initial CDD policy**.

1.3. If a pre-commencement customer requests another designated service after 1 July 2026, we complete initial CDD on the client under the **Initial CDD policy** before starting to provide this service to the client.

4. Escalation and enhanced CDD

We escalate any of the matters in this policy to our AML/CTF compliance officer to action when we detect them. To implement this policy, we follow the Escalating matters to the AML/CTF compliance officer process.

1. What we escalate and action

1.1. We escalate the following to our AML/CTF compliance officer to action. We stop providing designated services unless the compliance officer informs us, we can continue.

Event	AML/CTF compliance officer action
Potential suspicious matter detected	Complete the unusual activity report through TriSearch, in line and in accordance with the Unusual activity report review form and report the suspicious matter to AUSTRAC if required. If there are no reasonable grounds for the suspicion, we can tell personnel to resume providing designated services If there are reasonable grounds for the suspicion, report the suspicion within the timeframes in the Reporting policy and proceed to the 'suspicious matter report will be made' event below
Client is high risk, and/or a suspicious matter report will be made and we decide to continue providing designated services to the client	Follow the steps through TriSearch, in line and in accordance with the Enhanced CDD form Obtain senior manager approval before telling our personnel they can resume providing designated services
A new client, designated service, delivery channel, country or ML/TF risk factor, method or indicator is detected that isn't in the Risk assessment	Review and update the program through TriSearch, in line and in accordance with the steps in the Maintain your program form Complete these steps before telling personnel they can resume providing designated services
Complex beneficial ownership checks - checking who owns or controls a trust, body corporate or government body	Follow the ownership and control mapping process and conduct and record the results through TriSearch, in line and in accordance with the Initial CDD form Complete these steps before telling personnel they can resume providing designated services
The client is on a sanctions list	We can't continue the transaction, handle their property or give them access to property Follow the Sanctions search done through TriSearch, in line and in accordance with the Sanctions check process and record the results using TriSearch, in line and in accordance with the Escalation register. Complete all these steps as soon as possible.

1.2. We escalate the following to our AML/CTF compliance officer to report. We don't stop providing designated services if we escalate any of these

Situation	Action
A designated service involves any physical currency transaction valued at $10,000 or more, or the foreign currency equivalent	Make a threshold transaction report via AUSTRAC Online within 10 days of the transaction by following the Reporting policy
Any cross-border movement of physical currency and/or bearer negotiable instruments valued at $10,000 or more, or the foreign currency equivalent	Make a cross-border movement report via AUSTRAC Online within the timeframes outlined under the Reporting policy

1.3. We make sure that all information provided to our AML/CTF compliance officer is accurate and sufficient to allow them to take appropriate action.

1.4. Our AML/CTF compliance officer will make sure that they provide personnel with information from the above actions that's relevant to the personnel's AML/CTF role. This includes if they can continue providing designated services to the client.

5. Reporting

We escalate reportable matters to our AML/CTF compliance officer, who reports them to AUSTRAC within the required timeframes.

1. Responsibilities

1.1. All our personnel:

a) detect potential suspicious matters, threshold transactions or cross-border movements by following our monitoring obligations under the **Ongoing customer due diligence policy**

b) escalate any potential suspicious matters, detected threshold transactions or cross-border movements to our AML/CTF compliance officer consistent with the **Escalation and enhanced CDD policy**.

1.2. Our AML/CTF compliance officer:

a) makes sure all reported information is accurate, complete and free from unauthorised change, is contained in the approved form and is reported within statutory timeframes

b) makes sure that all reports to AUSTRAC contain all reportable information that's known or reasonably available to our practice

c) investigates escalations of potential suspicious activity to determine if a suspicious matter report is needed

d) submits suspicious matter reports (SMRs) to AUSTRAC after notifying our governing body

e) reviews escalations relating to possible threshold transaction reports (TTR) and cross-border movement (CBM) reports

f) prepares and submits TTRs and CBM reports to AUSTRAC

g) notifies personnel of any information they need to help discharge their AML/CTF obligations (including, for SMRs, if they can start or continue to provide designated services to the client)

h) provides reports to AUSTRAC and our governing body on AML/CTF compliance at least annually.

1.3. Our governing body:

a) oversees AML/CTF compliance and reviews reports provided by our AML/CTF compliance officer

b) makes sure we have adequate resources, systems and appropriate oversight mechanisms to meet our reporting obligations.

2. Suspicious matter reports (SMRs)

2.1. Our AML/CTF compliance officer completes the steps through TriSearch, in line and in accordance with the Unusual activity report review form to determine if a suspicious matter report must be made.

2.2. Our AML/CTF compliance officer submits a suspicious matter report if both of the following are satisfied:

a) We are starting or proposing to provide a designated service, or someone asks for a designated service

b) Our AML/CTF compliance officer has reasonable grounds to suspect any of the following:

a. information our practice has may be relevant to an offence or proceeds of crime laws
b. a client, possible future client or their representative isn't who they claim to be

c. a person is planning an ML/TF offence using a designated service.

2.3. Where our AML/CTF compliance officer forms reasonable grounds for suspicion, they submit an SMR to AUSTRAC via AUSTRAC Online within:

a) 24 hours for suspicions relating to terrorism financing

b) 3 business days for all other suspicions.

2.4. Where a suspicious matter report needs to be submitted, and we decide to continue providing designated services to a client, we follow our **Escalation and enhanced CDD policy** in relation to the client.

2.5. Our AML/CTF compliance officer submits additional SMRs if new information leads to a further suspicion under section 2.2 of this policy.

2.6. Only our AML/CTF compliance officer, senior manager and governing body may access information about if an SMR was made or needs to be made.

2.7. We avoid providing any information to clients or other parties that could amount to a tipping off offence. See **Tipping off**.

3. Threshold transaction reports (TTRs)

3.1. Our AML/CTF compliance officer submits a TTR when our designated service involves a threshold transaction involving $10,000 or more in physical currency (such as bank notes or coins) or the foreign currency equivalent (known as a threshold transaction).

3.2. Our AML/CTF compliance officer submits a TTR to AUSTRAC via AUSTRAC online within 10 business days after the transaction takes place.

4. Cross-border movement (CBM) reports

4.1. Our AML/CTF compliance officer submits a CBM report when we accept or receive the cross-border transfer of physical currency and/or bearer negotiable instruments (BNIs) valued at $10,000 or more or the foreign currency equivalent.

4.2. Our AML/CTF compliance officer submits a CBM report to AUSTRAC via AUSTRAC Online:

a) before passing through customs when physically carrying physical currency and/or BNIs in or out of Australia

b) before mailing or shipping physical currency and/or BNIs in or out of Australia

c) within 5 business days of receipt, when physical currency and/or BNIs are received from outside Australia.

5. Annual compliance report (ACR)

5.1. We prepare and submit an ACR by following the Annual compliance report process.

5.2. We submit the ACR to AUSTRAC by 31 March via AUSTRAC Online.

5.3. A copy of the ACR is provided to the governing body after being submitted to AUSTRAC.

6. Tipping off

We won't disclose information on suspicious matter reports (SMRs) where this would or could reasonably be expected to prejudice an investigation.

1. Tipping off prohibition

1.1. We don't disclose any of the following information where doing so would or could reasonably be expected to prejudice an investigation:

a) information that establishes we submitted an SMR, or that a requirement to submit an SMR has been triggered

b) a report made or prepared for the purposes of meeting our SMR obligations, including unusual activity reports, or information that was recorded for the purpose of potentially including in an SMR

c) any document setting out information contained in an SMR, including the formation or existence of a suspicion, and including draft or final SMR

d) that we have given, or were required to give, information or produce a document, under sections 49 or 49B of the AML/CTF Act

e) a client is being investigated by AUSTRAC, a law enforcement agency or other government authority.

1.2. We may disclose information mentioned in this policy to the AUSTRAC CEO or an AUSTRAC entrusted person (including by submitting SMRs and providing information to AUSTRAC).

2. Contact with clients

2.1. We may request more information from a client to meet our AML/CTF obligations:

a) if a client asks for the reason, we say it's needed to meet AML/CTF obligations and/or practice policies

b) we do not disclose that the request is being made because of suspicious activity, or in response to an investigation or request to give information or produce a document under sections 49 or 49B of the AML/CTF Act.

2.2. If we offboard a client because of suspicious activity, and the client asks for the reason, we provide genuine reasons for doing so that don't mention the information at section 1.1 of this policy.

a) This may include that the client's conduct or ML/TF risk wasn't consistent with the terms of our retainer as outlined in the **Offboarding policy**.

3. Personnel knowledge of SMRs

3.1. Only the following persons may access information at section 1.1 of this policy:

a) the AML/CTF compliance officer, governing body and any senior manager

b) any person who needs access to the information for the practice to meet its obligations - for example, to legal counsel to obtain legal advice, AUSTRAC or law enforcement

c) any persons listed in section 1.2 of this policy.

3.2. We make sure that records of information listed in section 1.1 of this policy, are securely stored and only made available to these personnel.

3.3. After submitting an SMR, our AML/CTF compliance officer will:

a) inform the personnel who raised the suspicion of the information, including ML/TF risks, needed to meet their AML/CTF responsibilities

b) give the personnel who raised the suspicion any additional directions, which may include offboarding the client for the reasons outlined in the **Offboarding policy**

c) not disclose that they've submitted an SMR in relation to the client or were required to do so to anyone, but the personnel mentioned in section 3.1.

3.4. If personnel other than those mentioned in section 3.1 become aware of information listed in section 1.1 of this policy, they notify our AML/CTF compliance officer that they know this.

7. Offboarding

We follow this policy when we decline or stop providing designated services to clients that fall outside our risk appetite or would cause us to fail to meet our AML/CTF obligations.

1. Risk appetite and client acceptance

1.1. The ML/TF we're willing to accept, and what we'll do to avoid the risks we aren't willing to accept, are outlined in the risk appetite columns in our Risk assessment.

1.2. Risk avoidance measures may include limiting or placing conditions on designated services or refusing to provide designated services or offboarding a client when this risk factor arises.

2. Retainer conditions

2.1. Our standard retainer agreement includes clauses that allow us to:

a) decline new clients who fall outside our risk appetite

b) stop acting for clients where they fall outside our risk appetite

c) refuse or delay services where CDD information isn't provided

d) adjust services if controls are needed to manage risk

e) report suspicious matters despite confidentiality obligations and where the client is offboarded.

3. Offboarding triggers

3.1. We consider offboarding where:

a) required to offboard clients under the risk appetite columns of our Risk assessment

b) under the **Escalation and enhanced CDD policy**, our senior manager doesn't approve starting or continuing to provide designated services to a client

c) a client fails to provide the required information within a reasonable timeframe.

4. Decision making and documentation

4.1. Offboarding decisions are approved by a senior manager.

4.2. If we decide to offboard or keep a client, we record:

a) reasons for offboarding or keeping the client

b) all information requests and dates

c) client responses and dates

d) wording used to notify the client

e) controls applied where the relationship continues.

5. How to offboard a client

5.1. As outlined in the **Tipping off policy**, if we offboard a client because of suspicious activity, and the client queries the reason, we provide genuine reasons for doing so that don't mention the suspicious activity.

5.2. We offboard a client by both:

a) stopping providing designated services to this client

b) justifying this action to the client by referring to the clauses of our amended retainer at section 2.1 of this policy.

1 2 3

Part 3: Maintain our AML/CTF program

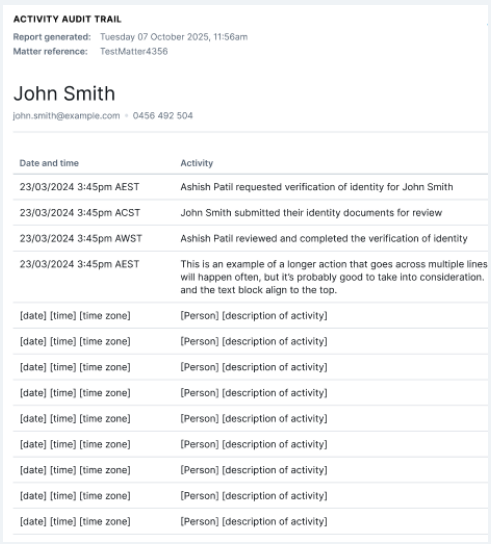
This section details how we'll keep our AML/CTF program up to date and continue to operate effectively.

What's in this section

This part has 5 sections:

Section	Actions	Policy, tools and guidance
1. Maintain the program	Make sure our AML/CTF program stays up to date as ML/TF risks change. Follow the policy to review and update our program in response to triggers. This includes significant changes to our services, delivery channels, clients or countries we deal with. Respond to new risks: • if personnel detect a new ML/TF risk, method or indicator of criminal activity they'll use the Escalation checklist process – factors not addressed in Risk assessment. • When a review and update is triggered, the AML/CTF compliance officer will use the: • Maintain the AML/CTF program form to record this and get senior manager approval for updates • Inherent risk rating and country risk	**Maintain the AML/CTF program policy** Processes and forms: • Escalation checklist process – factors not addressed in Risk assessment • AUSTRAC communications process • Maintain the AML/CTF program form • Inherent risk rating and country risk rating processes Guidance: • Review and update your AML/CTF program

Section	Actions	Policy, tools and guidance
	rating processes to assess the new ML/TF risks that arise.	
2. Conduct periodic effectiveness checks and reports	Make sure our AML/CTF compliance officer: • periodically checks if our program is working as intended and being followed • reports annually to our governing body on key compliance activities, the results of effectiveness checks and recommendations for improvement.	**Periodic effectiveness checks policy** **Reporting policy** Processes and forms: • Effectiveness check forms • Annual report to the governing body process • Annual report to the governing body form
3. Independent evaluations	Conduct and respond to independent evaluations of our AML/CTF program. Conduct an independent evaluation of our AML/CTF	**Independent evaluations policy** Processes and forms: • Independent evaluation process

Section	Actions	Policy, tools and guidance
	program at least once every 3 years. Record how we responded to any findings from the independent evaluation, particularly adverse findings.	• Independent evaluation response form Guidance: • Conduct an independent evaluation
4. Keep records	Keep sufficient records to help us comply with our AML/CTF obligations and demonstrate compliance to AUSTRAC. Use the forms referred to throughout this policy document to help meet this obligation.	**Record keeping policy** We use TriSearch platform to use digital versions of the forms outlined in AUSTRAC starter kits to comply with AML/CTF obligations. TriSearch platform keeps the record of all checks performed, and additional metadata for auditing purposes in accordance with our record keeping policy and AUSTRAC requirements for 7 years within their system. This data is stored securely and is readily available as required. Example of TriSearch system where audit logs and user activity is captured:  ACTIVITY AUDIT TRAIL Report generated: Tuesday 07 October 2025, 11:56am Matter reference: TestMatter4356 John Smith john.smith@example.com · 0456 492 504 Date and time / Activity 23/03/2024 3:45pm AEST — Ashish Patil requested verification of identity for John Smith 23/03/2024 3:45pm ACST — John Smith submitted their identity documents for review 23/03/2024 3:45pm AWST — Ashish Patil reviewed and completed the verification of identity 23/03/2024 3:45pm AEST — This is an example of a longer action that goes across multiple lines will happen often, but it's probably good to take into consideration. and the text block align to the top. [date] [time] [time zone] — [Person] [description of activity] Guidance: • Record keeping
5. Maintain AUSTRAC enrolment	Keep enrolment details accurate and up to date.	**AUSTRAC enrolment policy** Processes and forms: • AUSTRAC enrolment process

1. Maintain our AML/CTF program

We maintain our AML/CTF program to make sure it remains:

- current
- accurate
- compliant with regulatory obligations.

1. We keep our program up to date

1.1. Where an event below occurs, we escalate this to the AML/CTF compliance officer to review and, if necessary, update the program to make sure it addresses our ML/TF risks and meets our obligations.

Event	When we update the program	How we update the program
A significant change to any of the following: • kinds of designated (regulated) services we provide • delivery channels we use to provide those services • new or emerging technologies for those services or delivery channels • kinds of clients we provide these services to • the countries we deal with in providing these services.	If the change is within our control, before we provide the designated service. If the change isn't within our control, as soon as practicable.	For new country risks: use the Update country risk and risk ratings process. For all other risks: use the Update inherent risk and risk ratings process. For deficiencies with policies, procedures, systems and controls: by acting to effectively correct these deficiencies. Use the Maintain your AML/CTF program form to record any updates made within 14 days of the update. Obtain senior manager approval for any: • update to the Risk assessment • material change to our policies, procedures, systems and controls.
Any event that shows us our program isn't compliant with our obligations or doesn't address our ML/TF risks	If the event is within our control, before we provide the designated service. If the event isn't within our control, as soon as practicable.	
AUSTRAC communicates with us about relevant ML/TF risks or the conveyancing program starter kit. See **AUSTRAC communications policy**.	As soon as practicable	
An independent evaluation makes an adverse finding about our program	As soon as practicable	
If a periodic review and update of our program is due	Once every 3 years	

2. AUSTRAC communications

2.1. We monitor and action AUSTRAC communications that are relevant to our ML/TF risk by following the AUSTRAC communications process.

3. Communication and training

3.1. We provide written updates to our governing body when we update the Risk assessment.

3.2. We make sure approved updates to our AML/CTF program are given to any personnel with a relevant AML/CTF role.

3.3. Where updates affect operations or AML/CTF compliance responsibilities, training is delivered to affected personnel.

3.4. Our AML/CTF compliance officer is responsible for making sure personnel understand the changes and tracking completion of training.

2. Periodic effectiveness checks

Our AML/CTF compliance officer periodically checks whether our program is operating effectively and reports annually to the governing body.

1. When we do effectiveness checks

1.1. Our AML/CTF compliance officer does quarterly effectiveness checks covering:

a) suspicious matter reports (SMRs)

b) threshold transaction reports (TTRs)

c) AML/CTF compliance officer and senior manager functions

d) client onboarding, monitoring alerts, and all customer due diligence (CDD) processes (initial, ongoing, enhanced, pre-commencement).

1.2. When our AML/CTF compliance officer and governing body remain reasonably satisfied that our AML/CTF program is operating effectively, and they record their reasoning, these effectiveness checks are conducted less frequently.

1.3. At a minimum, we do effectiveness checks annually to inform our AML/CTF compliance officer's report to our governing body.

1.4. Additional effectiveness checks are to be performed whenever there are findings from the independent evaluation, particularly adverse findings, unusual personnel activity, or other compliance issues are identified.

1.5. We do effectiveness checks using the following forms:

a) Periodic effectiveness testing summary

b) SMR effectiveness check

c) TTR effectiveness check

d) CBM report effectiveness check

e) Compliance officer and senior manager effectiveness check

f) Enhanced CDD effectiveness check.

2. Corrective actions

2.1. All suggested actions to address matters identified in effectiveness checks must be approved by a senior manager before implementation.

2.2. Where corrective actions aren't approved, our AML/CTF compliance officer must follow the process set out in section 4 of the Maintain your AML/CTF program form.

2.3. If corrective action fails to correct the identified issue, new corrective actions must be developed and implemented.

3. Documentation and reporting

3.1. Effectiveness check outcomes must be available to our senior manager, governing body and AUSTRAC upon request.

3.2. The governing body must review periodic effectiveness check reports and direct additional action where deficiencies remain unresolved.

4. Communication and training

4.1. All affected personnel must be informed of changes to processes resulting from effectiveness checks.

4.2. Relevant personnel must receive training to make sure they understand and can apply updated processes.

5. Reporting to the governing body

5.1. Our AML/CTF compliance officer provides a written report to our governing body by following the Annual report to the governing body process and using the Annual report to the governing body form at least annually, covering:

a) compliance with our AML/CTF program

b) effectiveness of policies and controls

c) training and awareness activities

d) Risk assessment outcomes, including new or emerging risks

e) client onboarding numbers, including high-risk clients and PEPs

f) sanctions and watchlist screening results

g) SMR, TTR, CBM report volumes

h) records of AUSTRAC communications and actions taken.

5.2. Our AML/CTF compliance officer doesn't need to complete this report if both:

a) our practice is an individual (a sole trader practice)

b) Our AML/CTF compliance officer is also our governing body.

3. Independent evaluations

We have an independent evaluation of our program every 3 years, or more frequently if our governing body thinks it's needed due to our size, nature and complexity.

1. How we arrange an independent evaluation

1.1. We must arrange an independent evaluation and respond to adverse findings by following the Independent evaluation process.

2. Evaluator requirements

2.1. We select an evaluator that:

a) has suitable experience and knowledge of us, our industry, ML/TF risks and AML/CTF obligations

b) hasn't have been involved in developing, implementing or using our AML/CTF program, systems or controls

c) is independent of the work areas being evaluated

d) is granted access to all relevant materials.

3. Evaluation requirements

3.1. As part of the evaluation, our evaluator:

a) reviews the steps taken by us when undertaking or reviewing our ML/TF Risk assessment, including how ML/TF risks are identified, analysed, documented and rated

b) assesses if the ML/TF Risk assessment process complies with the requirements of the Act, the Regulations and the Rules

c) evaluates if the ML/TF Risk assessment is current and has been appropriately reviewed or updated in response to changes in our risk profile, products, services or regulatory obligations

d) evaluates if the design of the AML/CTF policies are appropriate to our nature, size and complexity

e) evaluates whether the design of our AML/CTF policies appropriately incorporate the mandatory elements required under the Act, the Regulations and the Rules

f) assesses if our AML/CTF policies clearly articulate obligations, roles, responsibilities and processes that enables us to comply with the law and effectively manage our ML/TF risks

g) tests the operational implementation of our AML/CTF policies, including sampling and review of customer due diligence files, reporting records, transaction monitoring outputs, governance documentation and any other relevant evidence of compliance

h) evaluates if any identified non-compliance is isolated or systemic, assess its potential ML/TF risk impact, and provide recommendations to address or remediate deficiencies in compliance with our AML/CTF policies

i) tests and evaluates the effectiveness of our ML/TF risk identification and assessment processes, including the accuracy, completeness and timeliness of risk identification across clients, transactions, products, services and delivery channels

j) tests and evaluates if our risk mitigation and control measures, including customer due diligence, transaction monitoring, reporting processes, governance arrangements and

assurance activities are effective in managing the ML/TF risks reasonably faced by us in providing our designated services.

4. Reporting

4.1. Our evaluator provides a written report containing the findings on the assessed matters to any senior manager responsible for approving changes to our AML/CTF program and, if separate, to our governing body.

4.2. The written report contains findings on the:

a) evaluation of the steps taken by us when undertaking or reviewing our ML/TF Risk assessment, against the requirements of the Act, the regulations and the Rules

b) evaluation of the design of our AML/CTF policies, against the requirements of the Act, the regulations and the Rules

c) testing and evaluation of our compliance with our AML/CTF policies

d) testing and evaluation if we're appropriately identifying, assessing, managing and mitigating the ML/TF risks that we may reasonably face in providing our designated services.

5. Findings and actions

5.1. All adverse findings must be reviewed.

5.2. If we accept the results of the findings, we'll create and implement an action plan, using the action plan in the Independent evaluation response form to resolve accepted deficiencies.

5.3. The action plan must be approved by our senior manager after being completed. Once approved it needs to be implemented.

5.4. The relevant Risk assessment and any relevant policy, procedure, system or control must be reviewed after approval of the action plan. Any changes to the relevant Risk assessment or relevant policy, procedure, system or control must be conducted under our **Maintain our program policy**.

5.5. If our governing body doesn't accept an adverse finding, the reason is documented using the Independent evaluation response form.

5.6. Our AML/CTF compliance officer implements the agreed action plan under the oversight of our senior manager.

4. Record keeping

We make and keep records relating to AML/CTF compliance and our AML/CTF program. We primarily use TriSearch platform to conduct CDD and to manage other obligations and forms. Therefore, the records are securely stored within TriSearch platform and are accessible to authenticated users as required.

1. How and when we keep quality records

1.1. We keep records of our Risk assessment and any updates to this Risk assessment, along with all records necessary to demonstrate compliance with this Policy document. This includes, but isn't limited to, any of the following referred to in the document:

a) a copy of any form, or completed field of a form

b) any record necessary to demonstrate compliance with a process.

1.2. We keep all CDD records for 7 years following the end of our business relationship or 7 years after the date of the last transaction.

1.3. We also keep records of transactions, including transaction records given to us by the client and the minimum records required to allow the reconstruction of individual transactions, including the following:

a) date and time the transaction was completed

b) the type of transaction, including the amount and currency used

c) the client's information

d) the payment method.

1.4. We keep transaction records for 7 years after the record is created or for 7 years from receiving the transaction record from the client (as applicable).

1.5. We keep all other records for 7 years from the point a previous version is no longer needed to prove compliance.

1.6. All records kept under this policy are:

a) securely stored and accessible only to authorised personnel

b) kept confidential

c) capable of being audited and accessible by authorised personnel

d) accurate and free from any unauthorised change

e) in the English language, or in a form that can be readily accessible and convertible into writing in the English language.

5. AUSTRAC enrolment

We to enrol with AUSTRAC and keep enrolment information accurate and up to date.

1. Initial enrolment

1.1. We submit our application to enrol with AUSTRAC:

a) if we will be providing a designated service on 1 July 2026 – no later than 29 July 2026

b) if we won't be providing a designated service on 1 July 2026 – no later than 28 days after the day we start providing a designated service from 1 July 2026.

2. Managing AUSTRAC enrolment

2.1. We make sure that:

a) all the mandatory fields in the AUSTRAC Business Profile Form are completed

b) our governing body is notified in writing once enrolment or updates to enrolment details are complete

c) enrolment information is kept accurate and up to date.

2.2. We update our AUSTRAC Business Profile with new or changed information, as required in the AUSTRAC Business Profile Form, about:

a) us or our designated services – within 14 days of this change

b) a change in our earnings for the past 12 months – within 14 days of the change.

3. Relevant processes

3.1. To meet this policy, we complete the AUSTRAC enrolment process and keep the records specified in this process.

PART 2 - AML/CTF Process document

[Organisation name]

Version control

Version	Date approved	Approved by	Summary of changes	Next review due
1.0	2/03/2026		This Process document is based on, and represents a digital adaptation of, the AUSTRAC Starter Kit issued on 29/01/2026.	
	Click or tap to enter a date.			
	Click or tap to enter a date.			
	Click or tap to enter a date.			
	Click or tap to enter a date.			

Table of contents

About this document

This document details the processes and standard operating procedures (SOPs) to meet your anti-money laundering and counter-terrorism financing (AML/CTF) obligations when using the AML/CTF program starter kit.

This document supports and aligns with the Policy document (PART 1).

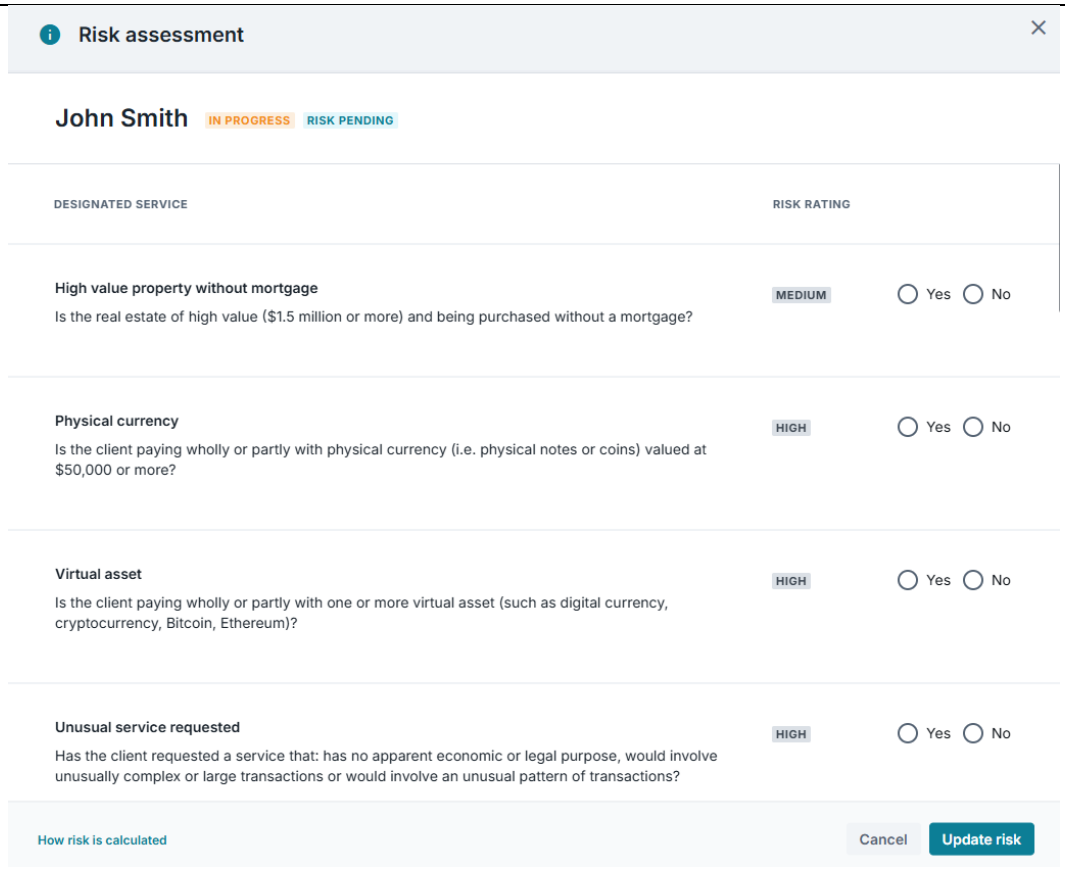
Client risk rating and ongoing customer due diligence process

This process details how to apply an ML/TF risk rating to a client when doing Initial customer due diligence. It also includes how to review their risk rating during our practice relationship with the client.

The process also sets out how to tailor our ongoing customer due diligence (CDD) in line with the ML/TF risk rating, including the level of appropriate ongoing monitoring.

Applying an ML/TF risk rating

Step	Actions
1.	We start by assessing if any of the medium or high-risk factors in the Initial customer due diligence apply to the client. We do this by referring to: • information the client provided in the Onboarding form or through any other means (for example, as part of enhanced CDD) • other information collected about the client when performing any other processes during initial or ongoing CDD (for example, documents provided by the client through Verification of Identity process conducted via TriSearch) • the ML/TF risk factors, methods and indicators listed in the Risk assessment • any other information we're aware of about the client, such as observations about interactions with the client or their representatives. • For any risk factors we believe may apply to the client, select YES in the relevant box. This is done digitally within TriSearch using the Risk assessment functionality.

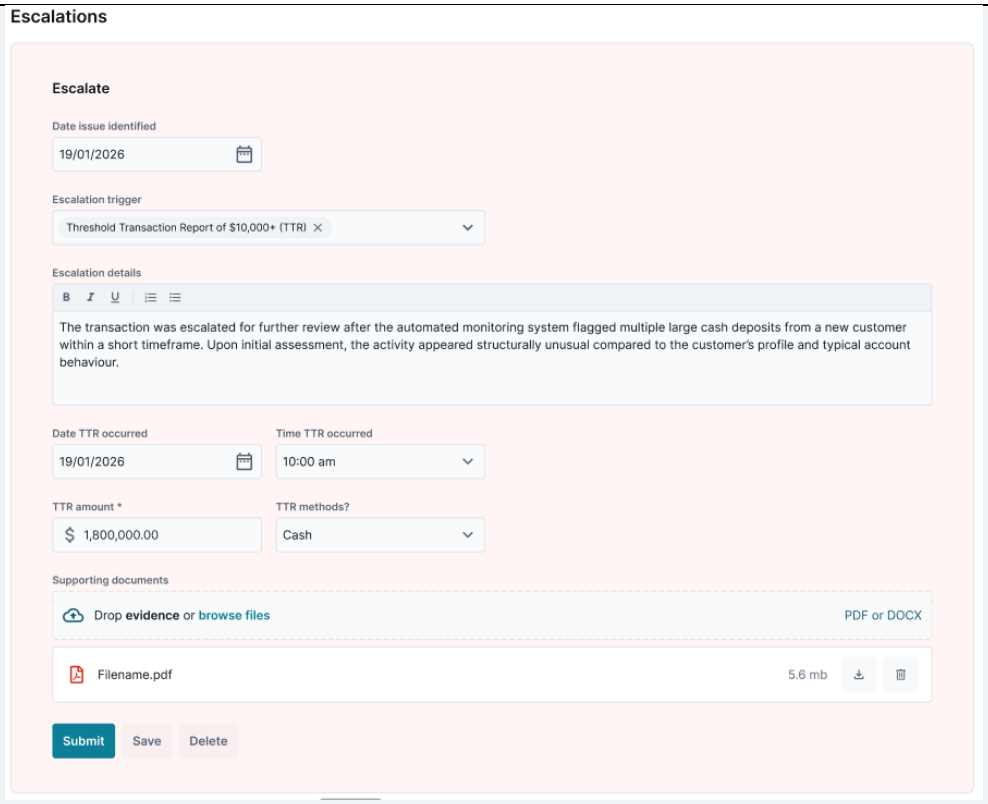


2.	We follow the instructions in Section A2 of the Initial customer due diligence form to select the appropriate risk rating for the client based on the boxes we marked in the risk factor table above.

Applying risk-based ongoing CDD

As part of your ongoing CDD obligations, we monitor our client from the first interaction with them until the end of our practice relationship. The table below shows the steps we take throughout practice relationships with our clients.

Step	Actions
1.	We monitor the client's behaviours during interactions with us and monitor how the client uses our services throughout the practice relationship. Monitor for the following types of activity, any: • unusual transactions and behaviours • transactions, behaviours or changes in their client profile which may indicate significant changes in the client's risk rating (for example, the client requests something which triggers a medium- or high-risk factor where you had previously selected NO, or where one of those risk factors no longer applies) • transactions involving $10,000 or more in physical currency as part of providing a designated service (for example, a client asks you to provide the proceeds of a $50,000 sale in cash) • cross-border movement of physical currency or bearer negotiable instruments (or a combination) valued at $10,000 or more as part of providing a designated service.
2.	Where any of the activities above occur, we use the Escalation triggers and actions process within TriSearch system to work out if you need to complete an Escalation and provide this to the AML/CTF compliance officer. Below is an example of how a transaction can be escalated within TriSearch system:

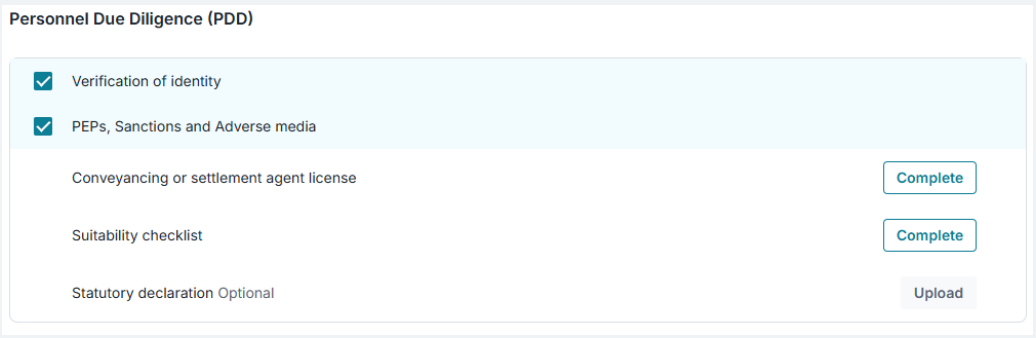
	
3.	In addition to ongoing monitoring, we review the following on a periodic basis to see if it's accurate and relevant to the client: • information we collected about the client during initial and ongoing CDD (for example, where our client is located, the reason our client is using our services, their occupation or practice activities) • the risk rating we applied to the client (based on if any of the activities in Step 1 occur)
4.	Where any of the activities in the steps above show that the client's risk rating may no longer be accurate or relevant, we use the steps under '1. Applying an ML/TF risk rating' to determine the client's current risk rating. If there's been a change in the client's information or their risk rating, update this either within the client's Onboarding form and Initial customer due diligence or in TriSearch system where we store this information.

The required level of ongoing monitoring and frequency of periodic reviews changes depending on the client's risk rating. The difference between each level of risk is in the table below.

Risk level	Actions during ongoing CDD
Low	Monitor the client's behaviours and transactions to detect any unusual activity throughout the practice relationship. If the practice relationship lasts longer than 3 years, conduct periodic reviews of information you hold on your client every 3 years (starting from the date you completed initial CDD).
Medium	Exercise a higher level of monitoring over the client's behaviours and transactions than you would for low-risk clients. If the practice relationship lasts longer than 2 years, conduct periodic reviews of information you hold on your client every 2 years (starting from the date you completed initial CDD).
High	Exercise a higher level of monitoring over the client's behaviours and transactions than you would for medium-risk clients. If the practice relationship lasts longer than one year, conduct periodic reviews of information you hold on your client every year (starting from the date you completed initial CDD).

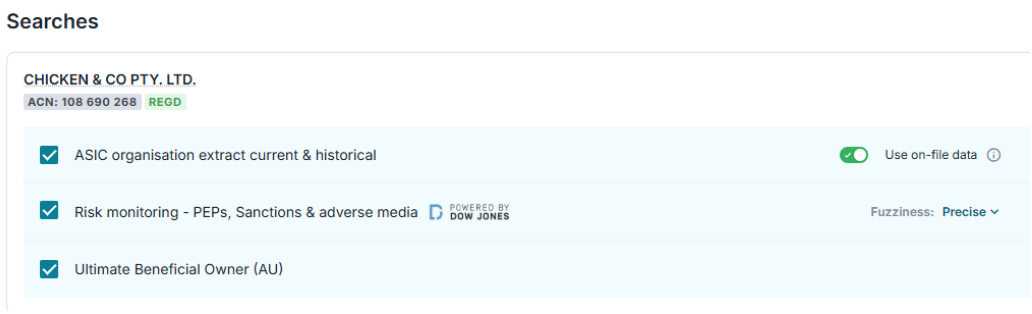
Statutory declaration process

This process details how to complete a statutory declaration for personnel who will perform AML/CTF functions, declaring any circumstances that may affect their suitability for the role.

Step	Actions
1.	We provide written information to the person that sets out what they must declare. This includes if they: • have been convicted of a serious offence (excluding spent or expunged convictions) • had any other adverse findings against them that may be relevant to their integrity or capability to perform the role (for example dismissed by a previous employer) • have a conflict of interest and, if they do, what they'll do to manage this conflict of interest • are willing and able to discharge the duties provided in the role description.
2.	We ask the person to complete the statutory declaration using the information provided. The person can complete either a Commonwealth statutory declaration or a statutory declaration from the state or territory in which they reside. These documents are available online and come with instructions for how they must be filled out.
3.	Ensure the statutory declaration includes the required information and has been correctly witnessed and signed by an appropriate person. If not, request that the person take the necessary steps to do so. The persons who are allowed to witness a statutory declaration are usually included as an appendix to the document.
4.	Keep a record of the statutory declaration for at least 7 years within TriSearch. 

Verify the nature and purpose of the practice relationship process

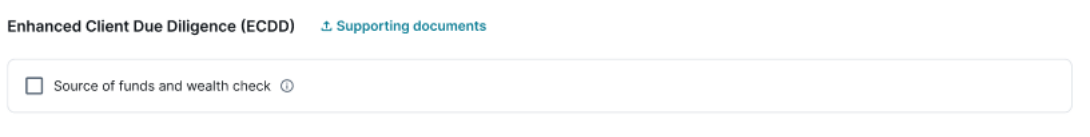
This process details out how to we verify the nature and purpose of a practice relationship as part of carrying out CDD obligations.

Step	Actions
1.	We use TriSearch system to send out digital Onboarding form to collect information from the client about the nature and purpose of our practice relationship with them. This includes information about why they're requesting a service from our practice and what the client will do with the services we provide.
2.	We determine if we can verify the nature and purpose with information already provided by the client. We do this by: • comparing the claimed nature and purpose with other information from the client, including their stated occupation, practice activities and other requirements as part of their request • considering if the claimed nature or purpose to be normal within the scope of your professional experience.
3.	We attempt to confirm the information provided by the client using reliable and independent sources (including ASIC and other Searches available via TriSearch platform) and other sources directly relevant to the client (including their website). 
4.	We ask the client to provide evidence which supports the information they've already provided about the nature and purpose of the practice relationship. For example, evidence of the client's occupation or practice activities, or evidence of what the client intends to do with funds generated from a sale.

Source of funds and source of wealth check process

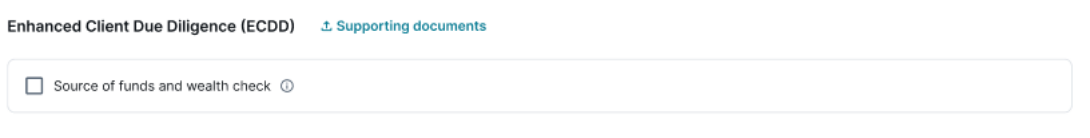
This process details how an AML/CTF compliance officer can establish a client's source of funds and source of wealth.

Source of funds

Step	Actions
1.	We ask the client to provide information about where they sourced the funds for the particular transaction or designated service. For example, this may be their salary or wages, or another source, such as the previous sale of a property.
2.	We collect documents or other forms of evidence from the client which you can use to verify the information provided on reasonable grounds. This is done using TriSearch system, using below option:  If the information provided initially is unclear or from an unusual source, we ask the client to provide further information. We can explain that this is required under your AML/CTF obligations. Examples of acceptable evidence include: • reliable and independent online sources such as government databases and credible media reporting • a signed letter from the client's certified practicing accountant confirming their source of funds • a payslip summary or employer letter confirming employment and salary details • a letter from the executor of an estate confirming the distribution of assets to the customer as inheritance • a copy of the sale record or title deed from the sale of property.
3.	Using the information gathered, we consider we have reason to suspect that: • the client's funds may have originated from criminal activity • the information provided by the client appears inconsistent with their known profile and financial state • any part of the client's funds cannot be linked to legitimate sources.

	If any of the above apply to the client, we complete the Unusual activity report review through TriSearch and submit an SMR to AUSTRAC in the appropriate timeframe (See Policy document for obligations relating to SMR).

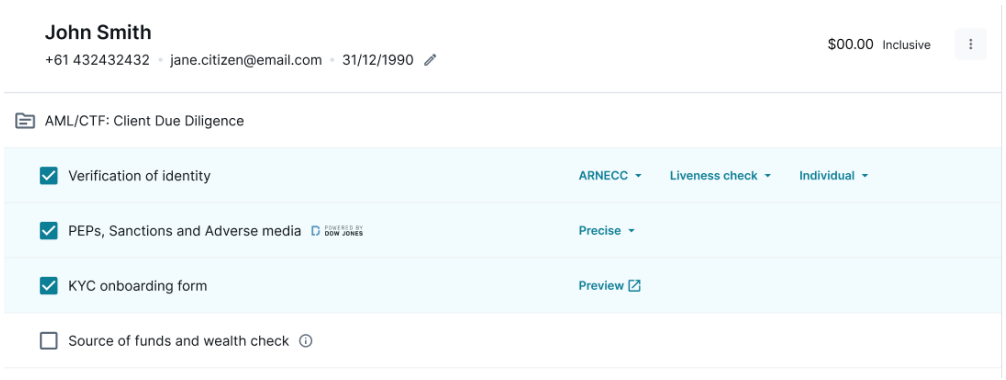
Source of wealth

Step	Actions
1.	We ask the client to provide information about how they acquired their overall wealth and assets. Most clients will have accumulated wealth from multiple sources over time. For example, funds from their salaries, returns from their investments, inheritance.
2.	We collect documents or other forms of evidence from the client which you can use to verify the information provided on reasonable grounds. This is done using TriSearch system, using below option:  If the information provided initially is unclear or from an unusual source, we ask the client to provide further information. We explain that this is required under your AML/CTF obligations. Examples of acceptable evidence include: • reliable and independent online sources such as government databases and credible media reporting • a signed letter from the client's certified practicing accountant confirming their sources of wealth • pay summaries from current and past employers which indicate wages accumulated over time • a letter from the executor of an estate confirming the distribution of assets to the client as inheritance • a copy of the sale record or title deed from the sale of property.
3.	Using the information gathered, we consider if we have reason to suspect that: • the client's wealth may have originated from criminal activity • the information provided by the client appears inconsistent with their known profile and financial state • part of the client's wealth is explainable from legitimate sources, but most of it is not If any of the above apply to the client complete the Unusual activity report review through TriSearch and submit an SMR to AUSTRAC in the appropriate timeframe (See Policy document for obligations relating to SMR).

Sanctions check process

The process details how to check if a client is designated for targeted financial sanctions.

Personnel carrying out a sanctions check

Steps	Action
1.	We use TriSearch to conduct PEP, Sanctions and Adverse media check digitally through their system. As an example, below:  TriSearch's search is provided by Dow Jones, an established, trusted and well-respected provider of PEP, Sanctions and Adverse media lists.
2.	If the person is a close match for a person appearing on the List: • stop engaging with the client immediately • don't provide services to the client • don't deal with their assets • don't return any assets which are currently under your control.
3.	Escalate the matter using the Escalation triggers and actions and Escalation function within TriSearch, notifying the AML/CTF compliance officer **immediately**.
4.	Document all sanctions checks performed in the relevant Initial customer due diligence, including: • details about the client and the sanctioned individual or entity • the 'last updated' date of the List that contained the match • screening results • any actions taken by the practice.

Responding to a positive sanctions check

Steps	Action
1.	Review the Escalation form and document findings using the Escalations register confirming the positive match using TriSearch system.
2.	After we confirm a positive match for sanctions: • inform the senior manager(s) and governing body • stop all client activity and freeze any client assets under the control of the practice • notify the Australian Sanctions Office and Australian Federal Police.

Politically exposed persons check process

This process sets out how to identify if an individual is a current or former politically exposed person (PEP) as part of initial or ongoing customer due diligence. You must conduct PEP checks on:

- the client (if they're an individual)
- anyone representing the client
- all beneficial owners of the client.

Steps	Action
1.	Review the client's Onboarding form and if they've disclosed that they are, or any representatives or beneficial owners are: • a domestic PEP • a foreign PEP • an international organisation PEP • a related person of a domestic, foreign or international organisation PEP. As outlined above in the Sanctions check process, we conduct PEP search digitally using TriSearch.
2.	If an individual client or other related individual has disclosed that they are or have formerly been a PEP: • search the name of the individual and any other information provided to verify the claim and determine which type of PEP they are or were. • review relevant articles, webpages, news items, and other sources returned by the search prompts. Assess up to the first 3 pages of results from TriSearch.
3.	If we identify that: • the person is a foreign PEP – they are a high-risk client and you will need to complete the Enhanced CDD using TriSearch • the person did not tell the truth about their PEP status – consider whether this was intentional or a mistake. If we believe this is intentional, this is an unusual matter that you must either: • escalate to your compliance officer using the Unusual activity report information or • if you are the compliance officer – determine if this is a suspicious matter that must be reported to AUSTRAC by using the Unusual activity report review form.
4.	Document the results of PEP checks performed in the Initial customer due diligence, including: • the search terms used • the sources reviewed in making the assessment • outcomes of the checks.

Adverse media check process

This process sets out how to check for adverse (negative) media associated with your clients or personnel.

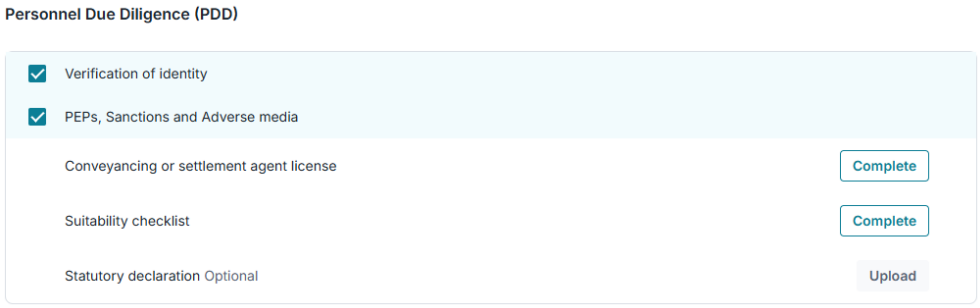
Use this process to help you determine:

- For personnel – their suitability to hold a particular AML/CTF role
- For clients, their representatives, their beneficial owners and persons on whose behalf the client is receiving the designated service – the client's ML/TF risk rating and if there is suspicious behaviour.

Step	Actions
1.	As outlined above in the Sanctions check process, we conduct PEP search digitally using TriSearch.
2.	We determine if the media sources being used are reliable and independent. This includes, but isn't limited to, media articles that refer to: • settled criminal convictions • charges • executed law enforcement powers • arrests • findings of fact in civil proceedings verified through official court of government references. Don't consider any spent or expunged convictions.
3.	We consider the context and relevance of any reports. Are the alleged offences a type that could generate significant profits? For example: • money laundering • fraud or corruption • financial crimes • drug trafficking • people smuggling • other serious or organised crimes. Place lower weight on minor or non-profit-generating offences, or offences that are less likely to alter the level of ML/TF risk (such as drink driving). Consider any relevant findings of misconduct or other activity.
4.	If we identify that the person has allegedly committed a significant profit-generating offence or there is another significant finding from adverse media. For personnel – treat this as a factor that may affect their suitability to hold a particular AML/CTF role. For clients, their representatives and their beneficial owners – treat this as a factor for their ML/TF risk rating and if you're required to submit a suspicious matter report to AUSTRAC.

Identify personnel process

This process sets out the steps to verify the identity of personnel during personnel due diligence.

Step	Actions
1.	We use TriSearch system to do the Personnel due diligence. This process includes doing a Verification of Identity, which collects the required information and ID documents, doing a PEP, Sanctions and Adverse Media check. As an example, below functionality is used within TriSearch to conduct due diligence on client facing personnel.  We obtain the following information from the person: • legal name • any other names they're known by • date of birth • residential address • unique identifier (license or passport number) • expiry date related to the unique identifier (if any).
2.	We obtain an original or reliable copy (physical or electronic) of one of the following types of documents to verify their identity: • One primary photographic identification document • One primary non photographic identification document As outlined in Annexure A. Check the document against the identifying information provided to make sure they're consistent.
3.	Confirm the person is who they claim to be.

	If the person has provided photo identification, check their appearance against the photo provided. If the person has provided non-photographic identification documents, examine the reference material provided.
4.	If you identify any inconsistencies, ask the person to provide additional identification documents to resolve the inconsistency.

Annexure A: Identification documents

Primary photographic identification documents

- Australian passport
- Australian proof of age card
- Australian driver's license
- Foreign passport
- Foreign identity card

Primary non-photographic identification documents

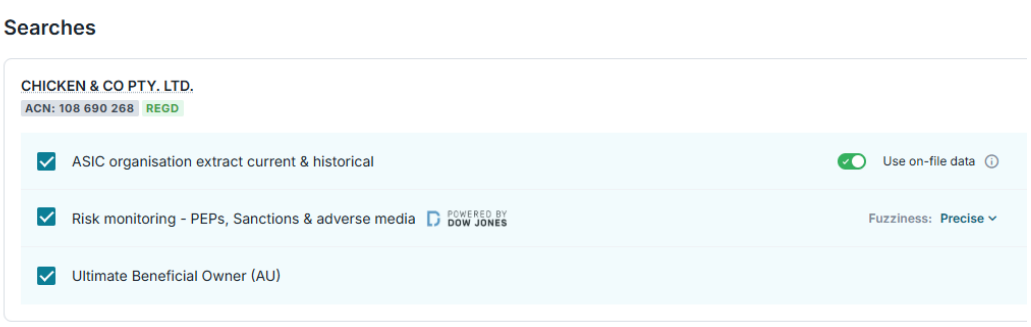
- Australian birth certificate or birth extract
- Australian citizenship certificate
- Australian concession card (pensioner concession card, health care card, senior's health card)
- Medicare card
- Veteran card
- Change of name certificate
- Marriage certificate
- Foreign birth certificate
- Foreign citizenship certificate

Beneficial ownership process

This process details how to trace and identify how a non-individual client is owned and controlled. The process includes identifying every entity and beneficial owner in the ownership and control chain and tracing it back to the individuals who ultimately own or control the client (see **possible beneficial owners).**

Steps

The process starts from the client entity, analysing how they're owned and controlled, including through layers of intermediate entities.

Step	Actions
1.	We conduct ASIC, Ultimate Beneficial Owner (AU), PEPs, Sanctions & adverse media checks using TriSearch, which provide extensive reports to accurately identify and collect required details and documents needed for identifying beneficial owners. 

Step	Actions
2.	Ask the client for original documents or reliable copies and extracts that show ownership and control, such as: • a company extract (lists directors and shareholders) • a partnership agreement • a trust deed • an existing ownership and control chart certified by a qualified professional (including a solicitor or certified practicing accountant). If a document collected may be subject to change (for example, extracts from the ASIC Company Register), the document should be no more than 6 months old. Request further documents with details of changes made (for example, deeds of variation, ASIC change of officeholder forms). Where documents are unavailable or unclear, ask for alternative independent documents and record the reason. Keep copies of all documents collected for our records.
3.	Verify if the documents submitted are: • original documents, or reliable copies or extracts of the original document • current (or not more than 6 months old if the information could be subject to change) • originate from an independent and reliable source (for example, government register) Where documents are certified, note that certification confirms only that the copy matches the information on the document presented. If we're unsure of the authenticity or accuracy of a document, you may wish to verify this by requesting: • the original document • all variations/amendments in chronological order • third-party confirmation from the individual who drafted the document or other professional who can certify the contents If there are still doubts about the document's authenticity, consider if this is unusual and if we fill out an Unusual activity report. Where necessary, cross-check information provided against other documents (if available) or online sources. Record verification outcomes, including: • all documents provided and their source • how you verified those documents • any limitations or issues identified in those documents.
3.	Identify and trace all individuals and entities who own or control the client, including through shareholdings, voting rights, practical influence and ability to appoint or remove directors or trustees.

Step	Actions
	A list of common owners and controllers for each entity type can be found below. Refer to 'Possible beneficial owners' in the Supporting information section below. Where it has been determined that the client is: • a listed public company subject to public disclosure requirements (for example, ASX) – end the process and document your findings • a subsidiary of a listed public company subject to public disclosure requirements (for example, ASX) – continue the process until you reach the listed public company then end the process and document your findings.
4.	If any owner or controller is another entity (for example, another company or trust), repeat Steps 1 to 3 for each intermediary entity. Keep tracing through each layer until you've identified and documented all individuals who ultimately own or control the client.
5.	Document findings by mapping out the ownership and control structure of our client in the Initial customer due diligence step. This can be done by creating a simple flow chart or table with the details of each entity and individual within the structure. This should include a detailed breakdown outlining: • each ownership layer, including a breakdown by percentage of ownership of the client • each beneficial owner with ownership and aggregated ownership percentage • each beneficial owner and the way they control the client • clearly label nominee arrangements (for example, 'Nominee for [Name]')
6.	Identify if any parts of the ownership and control structure align with risk factors in the Risk assessment, such as: • nominee arrangements (for example, shareholders or directors) • offshore entities • complex ownership. Where a nominee arrangement is identified, don't treat the nominee as the beneficial owner. Attribute the ownership or control to the underlying beneficial owner and request written confirmation from the nominee declaring the person they're acting for.
7.	Use the ownership and control structure to determine if there are any individuals who directly or indirectly own 25% or more of the client.
8.	Use the ownership and control structure to determine if any individual exercises control of the client, regardless of ownership percentage. This includes through decision-making authority or influence. For example, the trustee of a trust exercises control over a trust through their position, rather than by 'owning' the trust. For reference, use the tables below under possible owners and controllers and documents for each entity type below (for example, a director, senior manager, or trustee).
9.	If no beneficial owners can be identified through Steps 8 and 9, or if none exist, we must: • identify and verify the CEO (or equivalent senior officer) for the client

Step	Actions
	• record the steps you took to identify beneficial owners, along with the reason why they couldn't be established.
10.	Document all findings in the Initial customer due diligence step and keep records of any workings while determining the beneficial owners.

Supporting information

Documents for each entity type

We use the table below to identify which documents you may collect for the client's entity type.

Entity type	Suggested documents
Body corporate	• the company extract or annual statement indicating all shareholders and persons with control (or foreign equivalent) • a copy of the constitution, charter or rules (or equivalent document) • ownership and control charts, if available
Association	• an extract from a register of incorporated associations (if relevant) • a distribution(s) of member statements • the constitution or rules • governance chart, if available
Partnership	• a copy of the partnership agreement and any amendments or variations • partnership structure charts, if available
Trust	• the trust deed (or relevant extracts) and any deeds of variation • a disclosure certificate that verifies information about the trust • letters or documents from an independent professional services firm, such as lawyer or accountant for the trust (not the trustee)
Government body	• list of individuals with governance responsibility (for example, board, CEO, secretary) • organisation charts, if available

Possible beneficial owners

The table below details common beneficial owners for each entity type.

Entity type	Beneficial owners
Body corporate	• directors/board members • individuals who own more than 25% of shares • individuals with more than 50% of voting rights • individuals who determine financial or operational decisions (e.g. CEO, managing director)

Entity type	Beneficial owners
Partnership	• individuals holding 25% or more of partnership interests • individuals who exercise control over the management, operations or finances of the partnership • individuals with more than 50% voting rights • general partner in a limited partnership (or the individual who owns or controls the general partner)
Trust	• all trustees who are individuals • for a corporate trustee, individuals who own or control the trustee • any settlors (if they can exercise control) • any appointors, protectors, controllers or other individuals with control over elements of the trust Unit trust: • any individuals holding 25% or more of units Discretionary/family trust: • individuals (beneficiaries) entitled 25% or more of distributions, if identifiable Bare trust: • the beneficiary
Association	• all Responsible People, including members of the governing body, or those directing or guiding the strategic direction of the charity • any other individual with authority to direct decisions, access funds or control management and decision making
Government body	• individuals with primary responsibility for governance and executive decisions (for example, CEO, department secretary, board of commissioners) • authorised signatories

Annual report to the governing body process

This process details what the AML/CTF compliance officer needs to do to prepare the annual report to the governing body on the operation and effectiveness of the AML/CTF program. The report summarises:

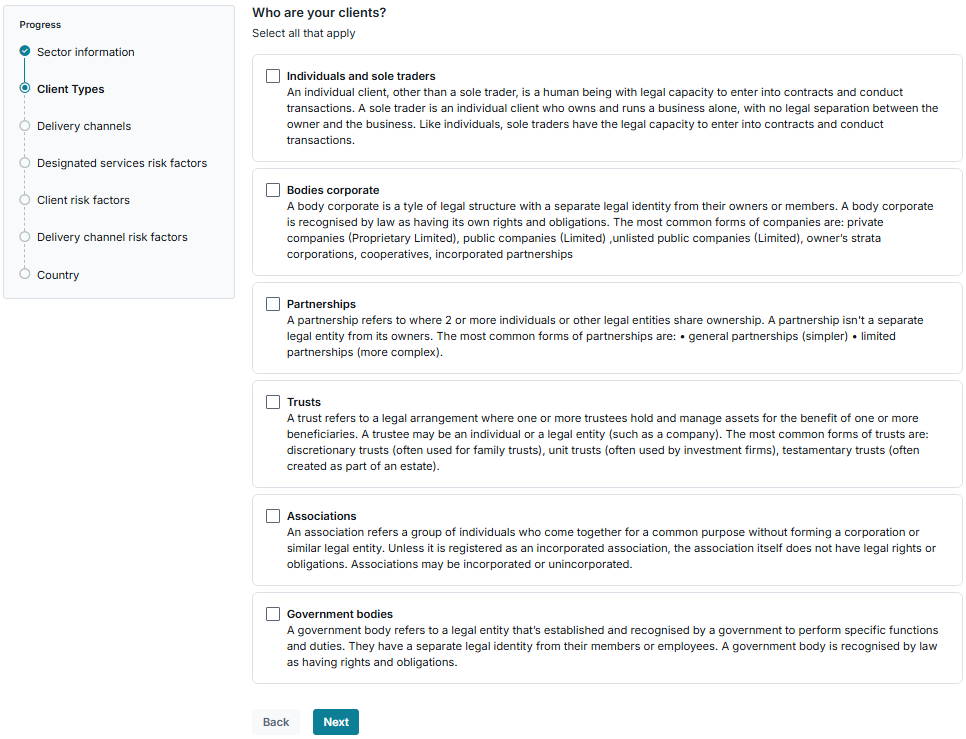
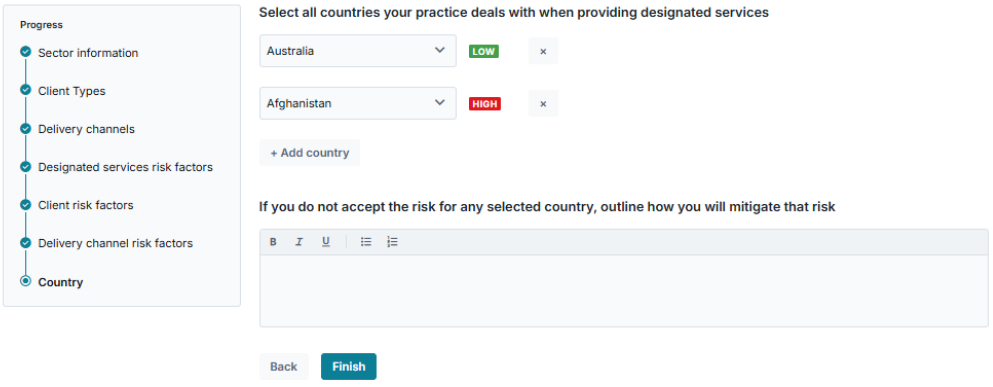
- key compliance activities
- testing results
- recommendations for improvement.

Step	Action
1.	Complete the report details section including: • date of report • reporting period covered • who completed the report • who reviewed the report (if applicable).
2.	Provide key recommendations for the governing body to consider or note. Summarise any actions or decisions the governing body should consider. For example, changes to program resources, staffing or risk controls List relevant updates, developments or emerging risks that the governing body should be aware of.
3.	Summarise key AML/CTF activities and events that occurred during the period. Include: • AUSTRAC communications (notices, guidance, or feedback received) • changes in ML/TF risk or client profiles • training delivered to personnel • internal or external reviews undertaken, such as independent evaluations • any identified breaches relating to compliance with AML/CTF policies and action taken • any identified breaches relating to compliance with the AML/CTF Act, Rules or regulations and action taken • any other breaches or incidents identified, and action taken.
4.	Summarise key training activities and events that occurred during the period. Include: • training delivered to personnel • if it was delivered within the required timeframes • are there any capability gaps and how they were addressed.
5.	Summarise reporting for the year. Include all reports submitted during the reporting period, including the total number of reports (per report). These include: • SMRs, TTRs, CBM reports and UARs • number of internal escalations • number of high-risk clients

Step	Action
	• number of complex clients.
6.	Provide an overview and trends of the high risk or complex clients that received a designated service during the reporting period.
7.	Include any changes made to the AML/CTF program during the reporting period. Include: • updates to ML/TF Risk assessment • new or revised policies, processes or controls • changes in system capability or data handling • amendments from AUSTRAC feedback or regulatory updates.
8.	Include the results of testing activities done during the reporting period for client: • Onboarding and verification. Include the results of testing activities for the following reports, indicate if the reports were timely, accurate and contained all the required information: • SMR testing and TTR testing. Include the results of any assurance and independent review findings, include if there were any deficiencies, breaches or recurring issues. This includes any: • independent evaluation outcomes • AUSTRAC engagement or feedback.
9.	Record outcomes and identify any deficiencies, breaches or recurring issues identified during effectiveness tests. Summarise how these will affect your practice's ability to mitigate and manage ML/TF risk. Describe what actions were taken or are planned to address them. For example, remediation steps, enhancements to policies, system improvements, and additional training undertaken or scheduled.
10.	Provide a clear statement addressing: • if AML/CTF policies are appropriately managing and mitigating ML/TF risks • any areas requiring review or enhancement • overall risk exposure relative to the practice's ML/TF Risk assessment • the level of confidence in the effectiveness of the AML/CTF framework.
11.	Include all attachments referred to in the report, such as: • ML/TF Risk assessment updates • updated policies or process documents • any independent evaluation reports • copies of AUSTRAC communications.
12.	Complete the declaration to confirm that the information is accurate and complete.

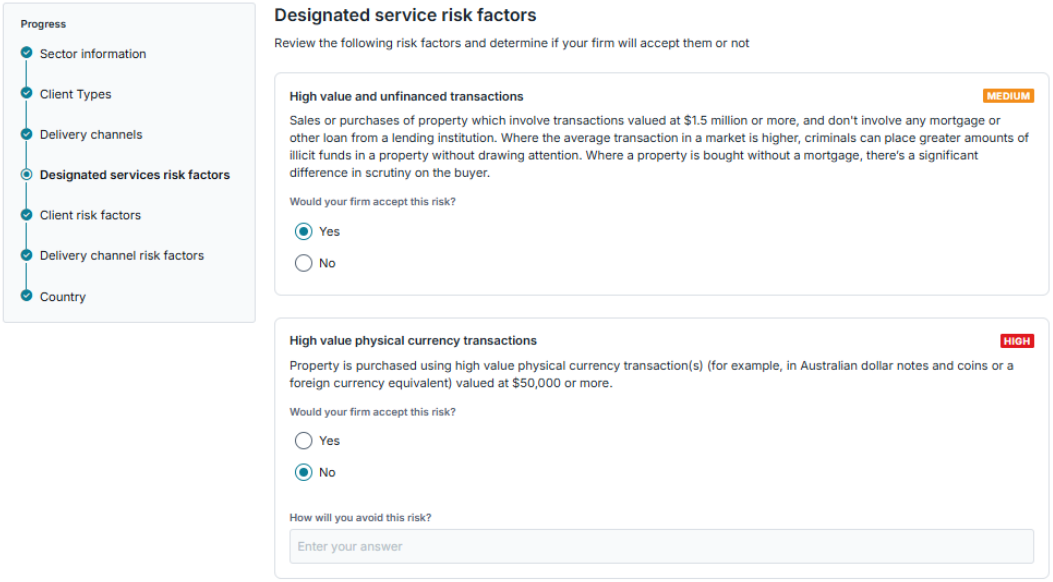
Update country risk and risk ratings process

This process outlines the steps to update your **Country: Risk assessment** in the Risk assessment.

Step	Actions
1.	We use TriSearch to digitally perform firm risk assessment in accordance with the Risk assessment form as outlined in AUSTRAC starter kit. This captures the countries we and the clients we deal with are located. The country risk rating automatically populates in the system based on Basel AML Index. Example of Risk assessment done via TriSearch.  Example of Country related risk assessment: 

Updating inherent risk and risk ratings process

This process details how to add or reassess an inherent risk or risk factor in our Risk assessment and how to determine the appropriate rating. This process excludes country risk ratings.

Step	Action
1.	This process in done digitally using TriSearch system's Risk assessment tool. Example of how we determine inherent risk. 
2.	Seek approval through TriSearch system, record for all updates and changes by following the Maintain your AML/CTF program form
3.	Once updates are approved, communicate changes to all affected personnel as soon as practicable and provide training if required. We keep the previous version of the Risk assessment within TriSearch for at least 7 years from the date of the change.

AUSTRAC communications process

This process details the steps for receiving, assessing and actioning communications from AUSTRAC.

Step	Actions
1.	The AML/CTF compliance officer will: • list themselves as the practice contact person through AUSTRAC Online. • subscribe to AUSTRAC guidance updates and AUSTRAC InBrief.
2.	If any other personnel receive or identify any communications directly from AUSTRAC, such as a letter, they must forward it to the AML/CTF compliance officer as soon as practicable.
3.	Review the communication to determine if it's relevant to the practice's ML/TF risks. If so, review the Risk assessment and affected parts of the AML/CTF program to identify if updates are needed. Record the communication in the table under Risk assessment sources in the Risk assessment.
4.	If updates are needed, draft proposed changes in line with the Maintain our AML/CTF program policy and Maintain your AML/CTF program form. Continue to Step 4. If no updates are needed, document that the communication was considered and the reason no updated are needed. This process is then complete.
5.	Submit any proposed changes to the senior manager for review and approval before implementation. If the senior manager rejects proposed changes, record the reasoning and follow the process outlined in Section 4 of the Maintain your AML/CTF program form.
6.	Once approved, update the relevant documents, and systems and controls. Make sure updates are published and accessible to personnel. Provide communication and training to personnel if required.

Independent evaluation process

This process sets out the steps for arranging, conducting and finalising an independent evaluation of the AML/CTF program.

Step	Action
1.	We appoint a qualified and independent evaluator (see **Independent evaluations** in the Maintain our AML/CTF program policy). Provide the evaluator with access to relevant AML/CTF policies, systems and records.
2.	The evaluator reviews the AML/CTF program against legal obligations and effectiveness, providing a written report with findings and recommendations.
3.	The evaluator submits the report directly to the senior manager, and if separate, to the governing body. The senior manager and governing body must review the report as soon as practicable. If there are no adverse findings, go to Step 8.
4.	We use the Independent evaluation response form to address any adverse findings. If findings: • aren't accepted – document the rationale in writing • are accepted – develop an action plan.
5.	Senior manager and governing body develop and document an action plan that: • categorises findings • assigns each finding to an appropriate personnel member • defines actions, timelines and responsibilities.
6.	We implement action items and record actions using the Maintain your AML/CTF program form We follow the action plan to make updates to the AML/CTF program. We submit the updated AML/CTF program to the senior manager for approval. We implement approved updates and provide personnel training if required. Save evaluation reports, action plans, forms and correspondence in the compliance records folder.
7.	We test implemented updates to confirm they're effective. Provide a written update to the senior manager and governing body. If updates are ineffective, investigate and repeat the process from Step 5 until effective.
8.	Once the evaluation is complete and, if applicable, all findings have been addressed, close the evaluation process and save all records in the compliance records folder. Add the next evaluation due date in a compliance calendar or register.

Annual compliance report process

This process details the steps for completing and submitting an annual compliance report (ACR) to AUSTRAC.

Step	Actions
1.	We make sure that the practice contact email is up to date in AUSTRAC Online. They will be notified about the compliance report. Schedule a reminder to prepare the report at the start of each calendar year.
2.	When notified by AUSTRAC, we review the compliance report preview questions to prepare.
3.	When the reporting period opens on 1 January: • determine if information is needed from other teams and areas in the practice. • gather information required to complete the report. • complete the report questions. It doesn't need to be completed in one sitting.
4.	We review and submit the report, checking the report for accuracy and completeness. Submit to AUSTRAC by 31 March via AUSTRAC Online and provide a copy to the governing body. Keep a record of the report for at least 7 years from the date submitted.

AUSTRAC enrolment process

This process details how to complete initial enrolment and update AUSTRAC enrolment details.

Enrol with AUSTRAC

Step	Action
1.	Go to the AUSTRAC website to enrol and register
2.	If you're starting a new application, select Sign up to enrol a new practice. If you're continuing an existing application, sign into your AUSTRAC Online account.
3.	Complete the AUSTRAC Practice Profile Form. Submit the form to AUSTRAC through AUSTRAC Online no later than 28 days after the day you start providing a designated service from 1 July 2026. For practices that provide a designated service on 1 July 2026, this will be no later than 29 July 2026. Save the confirmation message, completed form and related correspondence in the compliance records folder. Notify the governing body that enrolment is complete, unless the compliance officer is also the governing body.

Update AUSTRAC enrolment details

Step	Action
1.	Sign into your AUSTRAC Online account.
2.	Follow the instructions in AUSTRAC Online to update your enrolment details.
3.	Update the AUSTRAC practice profile with new or changed information on: • designated services or the practice – within 14 days of any relevant change • the earnings of the practice for the preceding 12 months – within 14 days of any change. Save the confirmation message, completed form and related correspondence in the compliance records folder. Notify the governing body that enrolment is complete, unless the compliance officer is also the governing body.

Escalating matters to the AML/CTF compliance officer process

This process details:

- matters that need to be escalated to the AML/CTF compliance officer
- how to escalate the matter
- what the AML/CTF compliance officer must do to action the escalated matter.

The steps we take under this process will depend on whether the escalation trigger is detected:

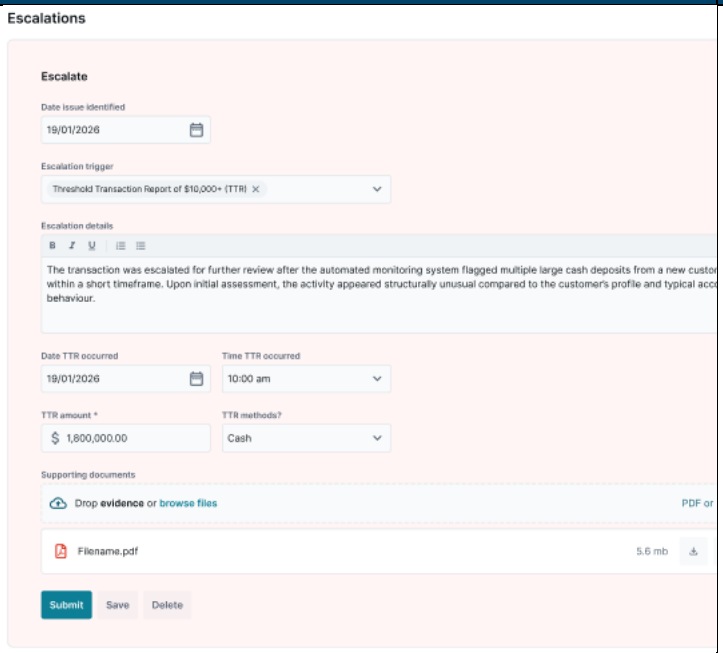
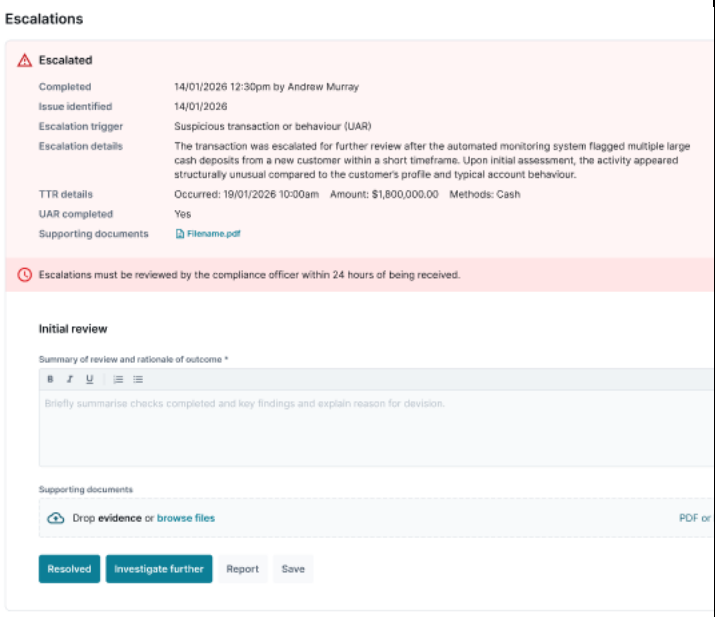
- by the AML/CTF compliance officer – Just follow the steps in 'how to action for the compliance officer' except those that relate to reviewing escalated information (you will have received this information yourself)
- by another person – Escalate to the compliance officer by following the steps at 'how to escalate'. The compliance officer then actions by following the steps at 'how to action for the compliance officer'.

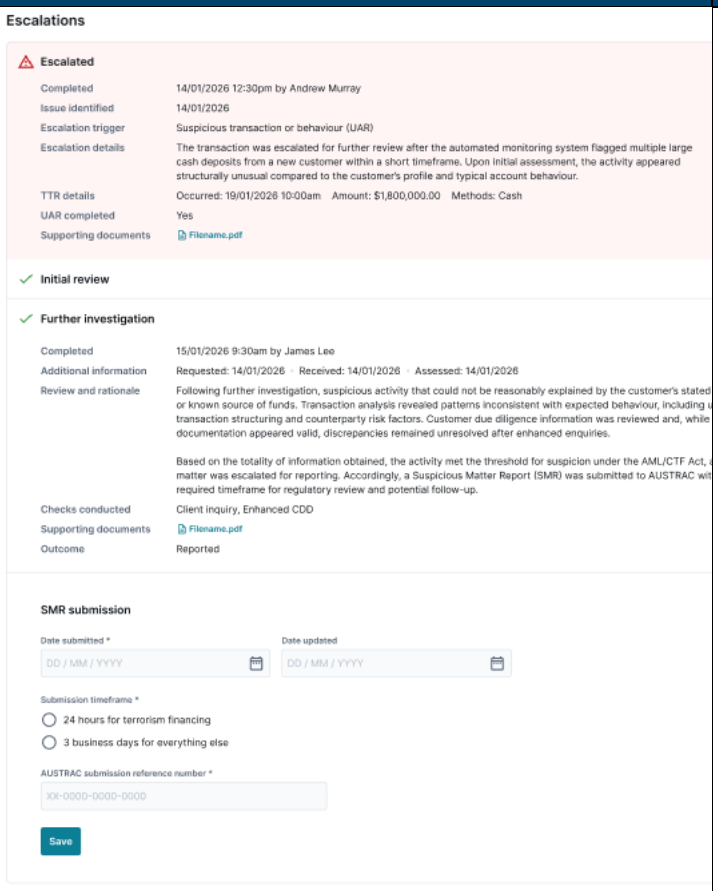
Where an action, process or form does not mention a timeframe, you must complete it as soon as practicable.

Escalation triggers and actions

The table below sets out triggers for escalation, and the actions that must be taken to escalate matters to the AML/CTF compliance officer for review and actioning.

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
If we're required to carry out enhanced CDD, where both: • your client is high risk and/or a suspicious matter report will be made • you decide to continue providin	Our Escalation process is managed digitally within TriSearch. The escalation option is available for client facing staff members to escalate transactions to the Compliance Officer.	We carry out enhanced CDD when the client is a high ML/TF risk client or you are required to make a suspicious matter report in relation to them. If either of these triggers occur, we perform Enhanced CDD including the following processes and checks: • Adverse media check process • Source of funds and source of wealth check process

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
g designated services	 Upon submission, the escalation is received and reviewed by the Compliance Officer within TriSearch system.  Escalation can either be resolved or can result into SMR submission.	• Verify the nature and purpose of the practice relationship process • obtain senior manager approval before starting, or continuing, to provide the designated service • collect and verify any additional information as appropriate to the ML/TF risk If initial CDD hasn't been completed, you must complete initial CDD in addition to any required enhanced CDD. If a senior manager doesn't approve starting or continuing to provide designated services to the client, no other checks need to be completed. Don't provide any further designated services to the client. Inform the personnel who escalated the matter to you if they can continue providing designated services to the client. Provide any necessary information to the personnel to help

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
		meet their AML/CTF responsibilities. Follow our Tipping off policy and, where applicable, Offboarding policy if you're required to offboard a client. If we identify potential suspicious matters through the information you collect, go to information relating to potential suspicious matters below.
Potential suspicious matters	Suspicious matter reporting (SMR) obligations start from the moment the practice provides, or proposes to provide, a designated service, or someone asks for a designated service. Escalate information when we suspect any of the following: • information the practice has may be relevant to an offence or proceeds of crime laws • a client, future client or their agent isn't who they claim to be • a person is planning an ML/TF offence using a designated service. This will typically occur when you identify unusual client behaviour or transactions. Escalate this by completing the following to send relevant information to the AML/CTF compliance officer: • Unusual activity report – in which you will record the key information required to determine if an SMR needs to be made to AUSTRAC	We make a suspicious matter report if you suspect on reasonable grounds that: • information the practice has may be relevant to an offence or proceeds of crime laws • a client, future client or their agent isn't who they claim to be • a person is planning an ML/TF offence using a

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
	• Escalation within TriSearch system – in which you can include any other relevant information about what triggered the suspicious or unusual matter. Hold off on providing, or continuing to provide, designated services until directed by the AML/CTF compliance officer. We avoid tipping off the client by following our Tipping off policy.	designated service. Complete the Unusual activity report review to determine if you need to take any of the following actions: • if there are clear reasonable grounds for a suspicion – record reasons, conduct enhanced CDD and submit a suspicious matter report to AUSTRAC • if further information is required – record reasons and gather further information • if there are no reasonable grounds for a suspicion – record reasons and take no further action. Once you reach a suspicion on reasonable grounds, a suspicious matter report must be made: • within 24 hours, if the suspicion relates to terrorism financing

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
		• within 3 practice days, for any other suspicion. We make sure that any information you report is accurate, complete and free from unauthorised change. You must also inform your governing body before an SMR is made. We inform the personnel who escalated the matter to you if they can provide designated services to the client (depending on if senior manager approval is given to do so under enhanced CDD) and of any other information they require to help discharge their responsibilities. You must not inform them that an SMR has been made or was required to be made. You must avoid tipping off the client by following your Tipping off policy. If you need to offboard clients, you must do so consistent with your Offboarding policy.

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
Positive sanctions check	Escalate this matter when we receive a positive match after following the Sanctions check process on any of the following: • our client • representatives • beneficial owners • people that the client is receiving a service on behalf of. If the result is positive, we follow the steps for personnel carrying out a sanctions check in the Sanctions check process. This will involve ceasing dealing with the client, or their assets, and escalating the matter to the AML/CTF compliance officer as soon as possible using the Escalation, including all relevant information. Hold off on providing, or continuing to provide, designated services until directed by the AML/CTF compliance officer.	We follow the steps at Sanctions check process - to take appropriate action in response to positive sanctions checks as soon as possible. We record the steps you have taken by filling out the fields in the Escalations register. We inform the personnel who escalated the matter to you if they can provide designated services to the client and of any information they require to help discharge their responsibilities.
Risks not addressed in the Risk assessment	This applies where we're considering providing a designated service after encountering any of the following that are either not in the Risk assessment or within your risk appetite as recorded in this Risk assessment: • a client type, designated service, delivery channel for a designated service, new and emerging technology relating to a designated service or channel or country you deal with • an ML/TF risk or method, or indicator of criminal or unusual activity. If we still want to provide the designated service, complete an Escalation, including all relevant information, and submit to the AML/CTF compliance officer. Include accurate information on the: • client type, designated service, delivery channels or country (if any) that you've encountered	We do the following and record relevant details in the Maintain your AML/CTF program form: • If the factor isn't included in the Risk assessment, or is a factor that's marked in the Risk assessment as outside your risk appetite, update the Risk assessment and associated controls to

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
	• ML/TF risk factors, ML/TF method or indicator of criminal or unusual activity (if any) that you've encountered • date when the factor was identified • the nature of the factor and how it was identified. Hold off on providing, or continuing to provide, designated servicgees until directed by the AML/CTF compliance officer.	manage and mitigate ML/TF risks by: ○ for new client types, designated services, delivery channels or ML/TF risk factors – following the Updating inherent risk ratings process ○ for new countries – following the updating country Risk ratings process ○ for new methods or indicators – updating the ML/TF methods and typologies and indicators of unusual

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
		or criminal behaviour sections of the Risk assessment and making any necessary changes to controls. ○ make any further changes necessary to appropriately mitigate and manage the ML/TF risk, method or indicator. • Seek senior manager approval for all updates to your Risk assessment and any material updates to the rest of your AML/CTF program. • Ensure that the personnel who escalated the matter to you does anything additional

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
		required under the amended controls, including (as appropriate) re-assessing the ML/TF risk of their client.
Complex beneficial owner check	Where we've identified a client that has a difficult or complex control structure and/or beneficial ownership, and you cannot carry out relevant beneficial ownership checks yourself, you must do the following: • accurately complete an Escalation, including all relevant information and documentation and submit to the AML/CTF compliance officer. • make sure the 'Client details' aspect of the relevant Onboarding form is complete and accurate including the kind of client, the service they're requesting, and their intended method of engagement with the practice. • make sure the Initial customer due diligence is complete (to the best of your ability) and accurate. • document our understanding of the control structure, and/or beneficial ownership of the client with reference to the documents received where this information is detailed. Hold off on providing, or continuing to provide, designated services until directed by the AML/CTF compliance officer.	We do the following and record relevant details in the Initial customer due diligence (for initial CDD) or Escalation register (for beneficial ownership checks made after initial CDD). You must: • review the Escalation to make sure the details are correct • conduct a beneficial owners check by following the Beneficial ownership process using TriSearch • record the steps taken to identify the beneficial owners, and the identity of the beneficial owners, in the relevant fields of the form. • inform the personnel who escalated the matter to you if they can provide

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
		designated services to the client and any information they need to help discharge their AML/CTF responsibilities.
Cross-border movements (CBM) of bearer negotiable instruments or physical currency	If we identify any international movement of physical currency or bearer negotiable instruments (BNIs), or a combination, valued at $10,000 or more (or the foreign currency equivalent), you must complete the Escalation and submit the form to the AML/CTF compliance officer.	We review the Escalation. If we identify any international movement of physical currency or BNIs (or a combination) valued at $10,000 or more (or the foreign currency equivalent), submit a CBM report via AUSTRAC Online within: • 5 practice days (for physical currency or BNIs received from overseas) • before any physical currency or BNI's are sent overseas.
Threshold transactions	If a transaction involves physical currency of $10,000 or more (or the foreign currency equivalent), complete the Escalation form and submit the form to the AML/CTF compliance officer.	We review the Escalation form. If the transaction involved $10,000 or more in physical cash (or equivalent foreign currency), submit a TTR to AUSTRAC within 10 practice days after the transaction took place.