



The Law Society
OF NEW SOUTH WALES

The Law Society of NSW
**AML/CTF Implementation
Guide: for medium and
large practices**

June 2026

Acknowledgement

The Law Society of New South Wales is deeply grateful to the Anti-Money Laundering and Counter-Terrorism Financing Compliance Officers (**AMLCO**) Discussion Forum, whose combined expertise helped shape this important piece of work.

At the time of publication, the Law Society's AMLCO Discussion Forum includes:

- Addisons
- Allens
- Ashurst
- Avant Law
- Baker McKenzie
- Bartier Perry Lawyers
- Brydens Lawyers
- Carroll & O'Dea Lawyers
- Clayton Utz
- Clifford Chance
- Clyde & Co
- Corrs Chambers Westgarth
- Dentons
- DLA Piper
- Gadens
- Gilbert + Tobin
- Hall & Wilcox
- Herbert Smith Freehills Kramer
- Hicksons | Hunt & Hunt | Holman Webb
- HWLE Lawyers
- Johnson Winter Slattery
- K&L Gates
- Kennedys
- Lander & Rogers
- LegalVision
- Longton Blackwell
- Maddocks
- Mallesons
- Marque Lawyers
- McCabes
- McCullough Robertson
- Meridian Lawyers
- Mills Oakley
- MinterEllison
- Moray & Agnew
- Norton Rose Fulbright
- Pinsent Masons
- Piper Alderman
- Russell Kennedy
- Swaab
- Turks
- Turner Freeman Lawyers

This guide is current as at 1 June 2026, including references to external links. Content will be reviewed periodically and updated as required.

Contents

Introduction	4
Suitability assessment	5
Nature, size and complexity	5
Conducting the suitability assessment	6
Methodology	6
Reviewing the suitability assessment	11
Suitability assessment outcome	11
Risk Assessment	12
Risk Assessment structure and format	12
Risk appetite	14
Heightened risks	14
Inherent risk	15
Residual risk and control effectiveness assessments	20
Risk profiles	22
Risk assessment examples	23
Policy	26
Part 1: Personnel	26
Part 2: Clients	27
Part 3: Maintaining your AML/CTF program	28
Processes	29
AUSTRAC enrolment process	29
Client risk rating and ongoing customer due diligence process	30
Pre-commencement clients	31
Using delayed initial customer due diligence	32
Statutory declaration process	32
Verify the nature and purpose of the practice process	33
Source of funds and source of wealth check process	33
Sanctions check processes	33
Politically exposed person checks	34
Adverse media check processes	34
Beneficial ownership processes	35
Annual report to the governing body process	36
Independent evaluation process	36
Escalating matters to the AMLCO process	37
Additional guidance	38
Reporting groups	38
Item 3 designated services	38
Director Identification Numbers	39
Annexure - Risk Assessment Guide	40

Introduction

Even if your practice does not meet all the criteria of a small legal practice outlined by the Australian Transaction Reports and Analysis Centre (**AUSTRAC**), AUSTRAC has stated that you are able to consider whether the AML/CTF Program Legal Profession Program Starter Kit and Conveyancing Program Starter Kit (**Starter Kits**) can be adapted to develop your Anti-Money Laundering and Counter-Terrorism Financing Program (**AML/CTF program**).

This Implementation Guide: for medium and large practices (**the Guide**) has been produced by the Law Society of New South Wales to support practices that are larger and/or more complex than the practices for which the Starter Kits were intended and, therefore, cannot rely on the Starter Kits to fully meet AUSTRAC's regulatory expectations of an appropriate AML/CTF program.

This Guide comprises three key components:

1. a suitability assessment to assist practices to determine the extent to which the Starter Kits can be adapted to suit their practice
2. a risk assessment that practices of medium complexity may consider suitable to adopt in its entirety and large practices can consider in informing their approach to risk assessment
3. guidance for practices of medium complexity on how to adapt the Starter Kits to suit their practice and, for practices of high complexity, insights into our profession's approach to compliance; and suggestions to consider for adoption or adaptation.

Regardless of the approach adopted, your AML/CTF program must reflect the size, nature and complexity of your practice and the money laundering (**ML**), terrorism financing (**TF**) and proliferation financing (**PF**) risks it will reasonably face. The following guidance provides general information and is not a substitute for obtaining legal advice.

Terminology

Throughout this guide, by:

- **small practice(s)** we mean practices with 15 or fewer employees, whose matters are of sufficiently low-level complexity that the AUSTRAC Starter Kits are suitable for the practice. This Guide is not intended for small practices - please see our [AML/CTF Implementation Guide: for sole practitioners and small practices](#)
- **medium complexity** we are referring to practices of medium size and complexity, with a suitability score of between six and 14, using our suggested self-assessment tool
- **high complexity** we are referring to larger sized practices, typically with 100 or more employees, a national or international presence and/or international clients. Larger practices will have a suitability score of 15 or over using our suggested self-assessment tool.

Unless otherwise stated, the terminology adopted in this Guide is consistent with the terminology adopted in the Law Society of New South Wales [Implementation Guide: for sole practitioners and small practices](#).

Suitability assessment

Nature, size and complexity

Understanding the nature, size and complexity of your practice is a key step in being able to undertake the suitability assessment. The information provided below details some of (but not all of) the considerations that will form your determination of your nature, size and complexity.

The nature of a legal practice is represented by the following indicators and its associated impact on ML/TF risk.

Table 1.1. Indicators of a law practice’s nature, and their effect on ML/TF risk

‘Nature’ indicator	Potential effect on ML/TF risk
Services designated by the <i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)</i> (AML/CTF Act) that are provided to clients	Different services attract different inherent ML/TF risks depending on whether they involve client funds, transactional assistance, structuring or crossborder elements.
Regulatory environment	The legal and professional regulatory framework influences governance, oversight, reporting obligations and interactions with other regulated entities.
Mutuality (i.e. reciprocation and strength of client-lawyer relationship)	Strong or longstanding client relationships may increase reliance on professional judgement and familiarity, which can affect how consistently client due diligence (CDD), monitoring and escalation processes are applied.

The size of a legal practice is represented by the following indicators, and their associated impact on ML/TF risk.

Table 1.2 Indicators of a law practice’s size, and their effect on ML/TF risk

‘Size’ indicator	Potential effect on ML/TF risk
Number of clients	The number of clients influences the scale of onboarding, ongoing client due diligence and monitoring activity, and the volume of customer risk assessments that must be maintained.
Number of matters	Higher matter volumes can increase transactional complexity and make it harder to identify unusual patterns without aggregated oversight.
Number of employees	A larger workforce may increase reliance on training, supervision and consistent application of AML/CTF controls.
Number of partners	More partners can introduce diversified risk appetites and decision-making, increasing governance and oversight complexity.
Number of offices	Multiple offices may operate with different practices or service focuses, increasing control and consistency challenges.
Cities and countries of operation	Geographic spread increases exposure to differing customer bases, delivery channels and country risk factors, including foreign jurisdictions.
Revenue generated (year-on-year)	Changes in revenue over time can indicate growth, contraction or shifts in the nature or scale of services provided, which may affect client mix, transaction volumes and ML/TF risk exposure; and help contextualise whether existing controls remain proportionate.

Understanding these concepts and having the relevant data available will help you complete your suitability assessment.

Conducting the suitability assessment

The Law Society of New South Wales has created a [suitability assessment tool](#). If your practice is outside the criteria specified by AUSTRAC, you can use the suitability assessment tool to determine whether your practice is sufficiently close to the criteria that you can nevertheless rely on/adapt the AUSTRAC Starter Kits to comply with your AML/CTF obligations or whether it is sufficiently large and complex that the Starter Kits are not appropriate.

The suitability assessment tool contains a list of questions you can use to assess the nature, size and complexity of your practice, and it produces three outcomes:

1. You are likely a small practice but slightly larger than that specified in the AUSTRAC criteria, and the Starter Kits can be used with minor or no adaptations.
2. You are likely a practice of medium complexity and will need to consider adapting elements of the Starter Kits to create your AML/CTF program.
3. You are likely a practice with high complexity (and therefore high ML/TF risks). The Starter Kits are therefore not suitable for your practice but can be used as guidance when developing your AML/CTF program.

If you have completed the suitability assessment and determined that the Starter Kits can be adapted to your practice, the following sections provide guidance on considerations when adapting the Starter Kits to your program.

High-complexity practices can still consider elements of the Starter Kits as guidance in developing their own AML/CTF programs. Where the guidance is adopted, we suggest adapting it to ensure it aligns with their legal practice.

Methodology

The suitability assessment methodology considers a range of factors that are indicative of the nature, size and complexity of different practices to determine whether your practice is likely a small practice, a practice of medium complexity or a practice of high complexity.

This suitability assessment tool comprises 13 questions that assess:

1. whether your practice provides only legal designated services as outlined within table 6 of section 6 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**)
2. if your practice provides other designated services, what percentage of your business comprises designated services within section 6, table 6, of the AML/CTF Act, as against other designated services listed in the AML/CTF Act
3. how many offices your practice has within Australia
4. how many different states/territories your practice operates in
5. how many staff you have in Australia
6. how many staff you have outside Australia but involved in the provision of designated services
7. how many different practice areas you have that provide designated services
8. your annual revenue for the previous 12 months
9. whether all personnel providing designated services hold a legal practising certificate
10. the percentage of clients that are considered high risk
11. the percentage of matters involving overseas clients
12. the percentage of clients that are provided with designated services on a fully remote basis
13. whether your practice is part of a large reporting group, foreign branch or subsidiary.

Each question includes a series of predefined responses that carry a weighted score. The following table outlines the possible responses to each of the above questions, the relative weight applied to each response and a description outlining the rationale behind the weighted scores.

Table 2.1 Suitability assessment methodology

Question	Response	Response score	Description
1 Do you provide only professional designated services as outlined in Table 6 of section 6 of the AML/CTF Act?	Yes	0	The Starter Kits are intended for practices that only provide legal services. Therefore, practices that answer yes to this question will receive a score of zero.
	No	1	It is acknowledged that some practices will provide a small number of ancillary designated services; therefore, a score of 1 is given to those practices that answer no to this question. A further assessment is made in question 2 to determine the extent to which a practice provides other designated services.
2 If you answered 'no' to Question 1, what percentage of your matters comprise services outlined in Table 6 of section 6 of the AML/CTF Act?	N/A	0	Practices that answer yes to question 1 should answer N/A (not applicable) to this question.
	More than 90%	1	For practices that provide other designated services, the question provides a tiered response, depending on the percentage of those designated services against the overall designated service population. The Starter Kits have been designed for practices that only provide designated services within table 6 of section 6 of the AML/CTF Act. Nevertheless, it is recognised that, from time to time, some smaller/simpler legal practices may provide other designated services (such as providing advice relating to financial products). In order to be able to leverage and adapt the Starter Kits, these additional services should be ancillary to the legal practice services. There is no fixed threshold under the law that determines whether a service is ancillary, but, generally, if a practice provides more than 90% of its services as legal services, it would likely indicate that other services are ancillary. Where the other services provided are greater than 10% of the overall service offering, it is likely more questionable as to whether these meet the definition of an 'ancillary service'. Where those services are greater than 20% of the overall service provided, it is highly likely this would be considered a main (not ancillary) service.
	More than 80%	2	
	Less than 80%	15	
3 How many offices does your practice have in Australia?	One	0	
	Two or three	1	The number of offices is indicative of the relative size and complexity of a practice - practices with more offices are likely to be larger practices.
	Four or five	3	
	More than five	6	

Question	Response	Response score	Description
4 How many different states/territories do you operate in?	One	0	<p>Question 4 assesses the number of states or territories a practice operates within.</p> <p>The Starter Kits were designed for small practices that will likely operate with a single office in a single state. It is likely that, the higher the number of states a practice operates within, the larger the size of the practice.</p> <p>Some smaller to medium complexity practices may operate across a couple of states, but practices operating across more than three states will likely be of high complexity in nature.</p>
	Two	2	
	Three or more	8	
5 How many staff do you have in Australia?	15 or fewer	0	<p>Question 5 assesses the number of staff employed by a practice. The Starter Kits are designed for practices that have 15 or fewer staff.</p> <p>It is recognised that some practices may have over 15 staff but would generally still be smaller legal practices. This would be indicated by selecting between 16 and 30, for which there is a minor addition to the overall score.</p> <p>As the number of staff grows, so does the associated scoring, with practices employing more than 100 staff being considered of high complexity, for whom the Starter Kits would not be appropriate.</p>
	Between 16 and 30	1	
	Between 31 and 50	3	
	Between 51 and 100	6	
	More than 100	9	
6 How many staff do you have outside of Australia providing designated services?	None	0	<p>Question 6 assesses the extent to which a practice uses staff outside Australia to provide designated services within Australia.</p> <p>Generally, the Starter Kits will be suitable for practices that operate solely within Australia. However, practices that have some staff overseas may be able to use the Starter Kits, but the higher the number of staff based overseas, the higher the suitability assessment score.</p>
	Fewer than five	1	
	Fewer than 10	5	
	More than 10	10	
7 How many practice areas within your business provide designated services?	Between one and three	0	<p>Question 7 assesses the number of different practice areas a practice has. Generally, smaller practices will likely have fewer practice areas, with larger practices having more practice areas.</p> <p>However, it is recognised that some traditionally smaller practices may operate across multiple practice areas; therefore, this question is not considered definitive.</p>
	Between three and five	1	
	Between five and seven	3	
	Eight or more	5	

Question	Response	Response score	Description
8 What was your annual revenue in the last 12 months?	Less than \$10 million	0	Question 8 assesses the annual earnings of the practice over the last 12 months. Practices that have annual earnings of more than \$200 million are automatically assessed as large practices that will need to design and implement their own AML/CTF programs. Other responses are tiered, reflecting an increased score for a greater level of earnings.
	Between \$11 million and \$30 million	1	
	Between \$31 million and \$50 million	3	
	Between \$51 million and \$100 million	6	
	Between \$101 million and \$200 million	10	
	More than \$200 million	15	
9 Do all personnel providing designated services hold a legal practising certificate?	Yes	0	Question 9 assesses whether all personnel providing designated services hold a legal practising certificate. This is a binary question as a matter of suitability for the Starter Kits. It is a requirement for all persons providing legal services to hold a practising certificate. It should be noted this question does not apply to conveyancers, who are not required to hold a legal practising certificate. Practices that only provide conveyancing services using conveyancers should answer 'N/A'. Legal practices that provide conveyancing services as part of their service offering should treat these staff as not requiring practising certificates and answer in accordance with the composition of personnel providing legal services.
	No	15	
	N/A	0	
10 What percentage of your overall client base in the last 12 months have you assessed as high-risk?	Less than 1%	0	Question 10 assesses how many high-risk client types a practice has had over the last 12 months. The Starter Kits have been designed for smaller businesses that are likely to face less complex and limited risk exposure; therefore, the Starter Kits are less suitable for practices that have a higher number of high-risk clients.
	Less than 5%	1	
	Less than 10%	2	
	More than 10%	12	

Question	Response	Response score	Description
11 What percentage of your matters in the last 12 months involved overseas clients?	Less than 1%	0	<p>Question 11 assesses the percentage of matters that involve dealing with overseas clients.</p> <p>The Starter Kits are designed for small practices that will conduct business within Australia, with clients based in Australia.</p> <p>The suitability assessment acknowledges that smaller practices may conduct some international business, such as providing white labelled advice or engaging with clients based overseas. However, in order to rely on, use or adapt the Starter Kits, this type of business should be ancillary to the practice's overall business.</p> <p>There is no relevant legal definition to establish what constitutes an ancillary service; however, generally, a service consisting of less than 10% of the overall service would likely be considered ancillary. Practices that conduct more than 10% of their business on an international basis will be less likely to be viewed as an ancillary service, and practices conducting over 20% of their business on an international basis will not be considered ancillary.</p>
	Less than 5%	1	
	Less than 10%	3	
	Less than 20%	8	
	More than 20%	15	
12 What percentage of clients do you service on a fully remote basis?	Less than 1%	0	<p>Question 12 assesses the extent to which a practice provides services on a fully remote basis.</p> <p>The Starter Kits are designed for small practices that do not offer services on a fully remote basis.</p> <p>The suitability assessment acknowledges that some small and medium practices may provide remote services on an ancillary basis. Where these services are few in nature, it will be more permissible to leverage and adapt the Starter Kits.</p> <p>Generally, practices that provide less than 10% of their designated services on a remote basis are more likely to be considered to be providing these services on an ancillary basis, and practices providing fully remote services more than 20% of the time are less likely to be considered ancillary.</p>
	Less than 10%	1	
	Less than 20%	4	
	More than 20%	8	
13 Are you part of a large reporting group, foreign branch or subsidiary?	No	0	<p>Question 13 assesses whether a practice is part of a large reporting group.</p> <p>The Starter Kits are designed for small practices that by their nature would not be forming reporting groups.</p> <p>Should a practice be part of a reporting group, the Starter Kits will not be appropriate for their practice.</p>
	Yes	15	

The score of each question is then aggregated to arrive at an overall score which can be used to assess the overall nature, size and complexity of your practice in accordance with the table below.

Table 2.2 Suitability assessment outcomes

Total score	Suitability Assessment outcome	Description
0-5	Small practice	You are likely a small practice and can rely on the Starter Kits with minimal or no adaptation.
6-15	Practice of medium complexity	You are likely a practice of medium complexity and can use elements from the Starter Kits, but these will need to be adapted to your business and own AML/CTF program. The risk assessment in this Guide may be suitable for you.
>15	Practice of high complexity	You are likely a practice with more complex risks and the Starter Kits are not appropriate for your practice.

We suggest documenting the suitability assessment and its outcome so that it can be reported to your senior managers and governing body.

The Law Society of New South Wales has created a [suitability assessment tool](#).

Practices that have completed the suitability assessment and determined that the Starter Kits can be adopted, despite their practice not fully meeting the AUSTRAC criteria, may wish to refer to the Law Society's [Implementation Guide: for sole practitioners and small practices](#) for further information on how to interpret and use the Starter Kits.

Reviewing the suitability assessment

The suitability assessment will need to be reviewed periodically to ensure it remains accurate and up to date.

This means the suitability assessment should be reviewed in accordance with any triggers for reviewing and updating the risk assessment; and in line with any periodic review timeframes for the risk assessment.

This includes updating the suitability assessment when:

- there is a change to the type of clients engaged by a practice (e.g. providing services to legal persons where previously these had only been provided to natural persons)
- new designated services are provided
- new methods of delivering those services are provided
- the business deals with new jurisdictions
- there is any other change that may impact the risk profile of the practice (e.g. mergers and acquisitions, entry into new practice areas, opening of new offices).

Suitability assessment outcome

For practices that have completed the suitability assessment and determined that the Starter Kits can be adapted to their practice, the following sections provide guidance on considerations when adapting the Starter Kits to your AML/CTF program.

Practices of high complexity can still consider elements of the Starter Kits as guidance in developing their own AML/CTF program; where the guidance is adopted, we suggest adapting it to ensure it aligns with their legal practice.

Risk Assessment

The Starter Kit Risk Assessment provides a good baseline for practices of medium and high complexity to identify and understand their risks, but, if the Starter Kit Risk Assessment is used, it will need to be tailored and adapted for each individual practice.

A Risk Assessment is the foundation of the risk-based approach which requires practices to adopt a structured way of identifying, assessing and managing ML/TF/PF risks so that effort and resources are applied proportionately to areas of highest exposure, rather than treating all risks or matters equally. In practices of medium or high complexity, this means recognising that different services (e.g. trust and company services, property transactions, litigation), clients, jurisdictions and delivery models carry different levels of ML/TF/PF and other financial crime risks and tailoring controls accordingly. The approach is embedded in governance, regularly reviewed and supported by existing clearly documented information available to practices of medium and high complexity, such as business data about client and vendor jurisdiction, client sectors, matter type, personnel training and trust account flow. Use and documentation of such information is likely to demonstrate that risk judgements are reasoned, consistent and responsive to changes in the firm's risk profile.

Where a practice is not relying on the Starter Kit Risk Assessment, we suggest that your risk assessment be based on a blend of the requirements of the AML/CTF Act, AML/CTF Rules and Starter Kit Risk Assessment, as applicable to your practice.

Risk Assessment structure and format

We suggest that the first consideration for practices of medium and high complexity is the structure and format of the Risk Assessment. The Starter Kit Risk Assessment requirements are established within

sections 26C and 26D of the AML/CTF Act and apply equally to all types of practice. However, there are considerations for each of these requirements that will need to be addressed for practices of medium and high complexity given they account for the intricacies of the practice (including the size) and the ML/TF risk the practice faces day to day.

Risk Assessments for practices of medium or high complexity will need to reflect the organisational complexities these practices may have, such as having multiple offices; providing a range of different services, including both professional and non-professional designated services; and shared service reporting arrangements. For example, where a practice provides both a non-item 3 designated service as well as trustee services as described in section 6, table 6, item 3 (receiving, holding and controlling (including disbursing) or managing client funds in relation to that advice), it may be helpful to consider the steps outlined in Table 3.1 below.

It is noted that section 6(5C)(e) of the AML/CTF Act may be interpreted to provide an exemption where the item 3 designated service is integral to, or an essential element of, providing a non-item 3 designated service,¹ meaning that the item 3 designated service is not required to be assessed separately.

However, the below table may still be useful to help consider, wholistically, the ML/TF risks involved in providing a designated service, given the very broad scope and variety of fact scenarios that may arise in the course of legal practices providing designated services.

Table 3.1 Suggested steps to conduct risk assessment

Step	Evaluation focus	Activity
1	Map the designated services and risk drivers	<p>Separate the practice into:</p> <ol style="list-style-type: none"> 1. legal advice 2. trustee/holding client funds. <p>Identify key ML/TF/PF risk drivers for each. Trustee services typically carry higher inherent risk due to custody/movement of funds and potential for layering.</p> <p>Example: Legal advice is provided on dispute strategy (no funds moved). Trustee service involves receiving client funds into a trust account and disbursing to third parties (higher risk).</p>

¹ For instance, holding funds on behalf of a buyer and disbursing trust funds at settlement, or organising for release of deposit to the seller, where assisting to plan or execute a transaction to buy, sell or transfer real estate.

Step	Evaluation focus	Activity
2	Assess where and how each service is delivered	<p>Determine whether the trustee service is delivered centrally (e.g. one trust team) or across multiple offices/partners and whether workflows differ by location or team. Differences increase inconsistency risk.</p> <p>Example: One office has a dedicated trust accounting team with daily reconciliations and another office relies on a partner's assistant to manage receipts/disbursements, creating process variability.</p>
3	Compare professional versus non-professional service exposure	<p>Evaluate how the risk profile changes when the practice moves from advice (professional judgement, usually less direct control of funds) to trustee activity (direct handling/transfer of client money).</p> <p>Example: For legal advice, the practice provides counsel only; for trustee work, the practice receives \$250,000 and is instructed to pay to multiple offshore counterparties - higher exposure to ML/TF risk, increased 'Know Your Client' (KYC) to understand the transaction and stronger controls implemented to manage that risk.</p>
4	Evaluate customer types and source-of-funds complexity	<p>Identify whether trustee matters involve different customer segments (e.g. corporates, foreign trusts, intermediaries) and whether the practice receives sufficient information about source of funds/wealth and beneficial ownership.</p> <p>Example: Legal advice clients are mainly domestic individuals; trustee clients include private companies with layered ownership and funds coming from overseas accounts, increasing inherent risk.</p>
5	Review shared services and reporting arrangements	<p>Check whether AML/CTF tasks (CDD, monitoring, escalation, Suspicious Matter Report (SMR) and Threshold Transaction Report (TTR) triggers) are shared across the practice or handled differently for trustee matters and whether escalation pathways are clear.</p> <p>Example: Compliance supports the legal advice practice generally, but trust account operations sit outside standard compliance workflows, leading to delayed escalation of unusual disbursement patterns.</p>
6	Assess governance and accountability for trustee work	<p>Confirm there is clear accountability for trustee risk. Who owns the risk: lead partner, trust account manager, compliance? Trustee services often require tighter oversight given direct funds handling.</p> <p>Example: The AML/CTF compliance officer (AMLCO) reports on legal practice onboarding metrics, but there is no standing governance agenda item for trust account anomaly trends or high-risk disbursements.</p>
7	Test whether controls are tailored to trustee money handling	<p>Determine whether controls for trustee services go beyond generic legal practice controls - for example, payment verification, dual authorisation, beneficiary checks, sanctions screening for payees and enhanced scrutiny of fund flows.</p> <p>Example: Legal advice matters use standard CDD at onboarding; trustee matters also require verification of payee identity, dual approval for payments, and documented rationale for third-party payments - if not present, residual risk remains high.</p>
8	Reflect the complexity in risk outcomes (do not average it away)	<p>Ensure the overall risk assessment outcome shows distinct ratings: legal advice may remain lower/medium inherent risk, while trustee services may be higher inherent risk and require stronger controls to reduce residual risk.</p> <p>Example: Business-level rating is 'medium' overall, but the trustee service line is rated 'high inherent risk' due to funds custody and third-party disbursements; residual risk remains 'medium-high' without stronger transaction controls.</p>

“Risk Assessments for practices of medium or high complexity will need to reflect the organisational complexities these practices may have, such as having multiple offices; providing a range of different services, including both professional and non-professional designated services; and shared service reporting arrangements.”

The AUSTRAC Starter Kits consist of an inherent Risk Assessment that is designed for small businesses and tailored to the risk profile of those types of practices, with a single inherent risk rating used throughout the document. Practices of medium complexity can also utilise this but may need to adapt it, given the complexities a medium-sized business presents over those of a smaller sized business. For practices of high complexity, AUSTRAC has determined that the Starter Kit Risk Assessment is not suitable and should serve purely as a guide or starting point in the development and customisation of a thorough and detailed ML/TF risk assessment.

We consider that, generally, practices of medium and high complexity are expected to develop a risk assessment methodology that outlines how the risk assessment is to be performed; which methods the practice uses for assessing inherent risk; and, if required, how the practice would conduct a control effectiveness assessment and determine residual risk. They are also expected to have a defined risk appetite statement that establishes acceptable tolerances for the risks they face. This risk appetite statement may also take the form of a risk register, depending on how much detail the practice considers appropriate to include.

Practices of high complexity may also have a wider array of risks and may consider conducting a financial crime risk assessment that considers other types of risks, such as sanctions and bribery and corruption risks or incorporating with other types of risk assessment, as covered below.

Risk appetite

Under ISO 31000, a ‘risk appetite statement’ is a governance-level statement that articulates the nature and amount of risk an organisation is willing to accept in pursuit of its objectives. It provides boundaries for decision-making and informs how risks should be assessed and treated, but it is not itself a risk rating. The appetite helps determine whether those underlying exposures are fundamentally acceptable for the practice, acceptable only with strong controls, or outside tolerance altogether.

For practices of medium complexity, and particularly practices of high complexity, this distinction is important, given the mix of designated and non-designated services, varying client types and levels of complexity, trust account activity and practice-group autonomy. While risk appetite is conceptually set with reference to inherent risk, it is most useful when expressed as a clear narrative statement in the risk assessment framework and tested at the residual risk level. This allows the practice to assess whether the risk remaining after controls is consistent with what the governing body of the practice is prepared to accept. Framing risk appetite in this way avoids treating it as another scoring flag and instead positions it as a benchmark that supports consistent decisions about control uplift, client acceptance, service delivery models or exiting activities where residual risk exceeds the firm’s stated tolerance.

Heightened risks

Proliferation financing risks

‘Proliferation financing risks’ (**PF risks**) refers to the threat of funds being used to support the spread of weapons of mass destruction, including nuclear, chemical and biological arms. Indicators that may be identified by Australian businesses include links to high-risk jurisdictions, unusual activity consistent with trade-based ML, or clients who are evasive in providing their identity or the ultimate beneficiary:

- Legal practices may be exposed to these risks through clients or counterparties that are owned or controlled by individuals or entities sanctioned under the United Nations or Australian Autonomous Sanctions, even if the client itself is not directly listed. Maintaining an effective and appropriate sanctions screening capability is essential for achieving PF compliance with obligations under the AML/CTF Act.
- PF risk is heightened when the client is linked to high-risk jurisdictions for proliferation, such as Iran or the Democratic People’s Republic of Korea (**DPRK**).
- Certain industries (such as those dealing in dual-use goods, advanced technology, research or maritime shipping) likely face greater PF risks due to their potential for misuse in weapons development or delivery. This can include business in research (such as universities) that are involved in computing, artificial intelligence, drones et cetera.

It is also important to recognise that all Australian businesses, regardless of their client portfolio, may encounter PF risks externally. For example, DPRK IT worker fraud schemes are specifically targeting Australia, and organisations with remote workers need to ensure they have robust identity verification procedures across the board.

The Australian Sanctions Office provides detailed guidance on PF risks, including advisory notes on PF risks, which can be found on the [Department of Foreign Affairs and Trade website](#).

Sanctions risks

It should be noted that sanctions obligations are broader than the obligations set out in the AML/CTF Act, encompassing stricter asset definitions and beneficial ownership thresholds under the *Autonomous Sanctions Act 2011* (Cth) and the *Charter of the United Nations Act 1945* (Cth). If you identify sanctions risks associated with your business activities, you should consider whether you require a sanctions compliance policy alongside your AML/CTF policy.

- In regard to AML/CTF sanctions requirements, sanctions risks arise when legal practices act for clients owned or controlled by individuals or entities listed under United Nations or Australian Autonomous Sanctions, including through beneficial ownership arrangements.
- Exposure can occur even if the client is not directly listed through beneficial ownership arrangements, making ongoing monitoring of Australia's Consolidated List essential. Sanctions lists do not remain static; it is recommended you subscribe for updates to Australia's Consolidated List to ensure you are working against the current list.² Sanctions risks may also be triggered by geopolitical events, which could result in rapid changes in the sanctions environment.
- Risks are heightened when handling or transferring funds to or from sanctioned jurisdictions (such as Russia, Iran and Myanmar), where enhanced due diligence is required.
- Assets owned or controlled by sanctioned persons must be frozen and reported to the Australian Federal Police and the Australian Sanctions Office. Business dealings with sanctioned individuals and entities are generally prohibited unless a sanctions permit (such as the Legal Services Permit issued by the Minister for Foreign Affairs as of April 2026) is obtained and relevant conditions are met, including reporting requirements.

The Australian Sanctions Office provides detailed guidance on sanctions risks and compliance, including guidance on sanctions compliance for legal professionals which can be found on the [Department of Foreign Affairs and Trade website](#).

Bribery and corruption risks

- Client risk factors: Acting for clients operating in jurisdictions with high perceived corruption risk, particularly where public officials or politically exposed persons (PEP) are involved.
- Matter and service risks: Assisting with large or unusual payments, commissions or 'consultancy fees' with unclear rationale.

- Third-party and relationship risks: Use of agents, lobbyists, consultants or intermediaries to engage with government bodies.

Practices that are exposed to such matters should ensure that their Risk Assessment meets the requirements of the AML/CTF Act and Rules.

The Attorney-General's Department has published guidance on adequate procedures to prevent the commission of foreign bribery, which practices of medium or high complexity should consider when assessing the bribery and corruption risks and designing and implementing mitigating controls. This can be found on the [Attorney-General's Department website](#).

Additional resources

In assessing the level of ML, TF and PF risks they face, practices of medium or high complexity will need to review public information and guidance relevant to their industry and practice type, including that published by AUSTRAC, like their InBrief updates or formal documents like the *Money laundering and terrorism financing (ML/TF) risk assessment framework - quick guide for lawyers* to determine an inherent risk rating. In accordance with their methodology, practices could also consider applying a residual risk methodology to assess the residual risk to their business, which would need to follow an agreed methodology for determining residual risk in line with the relevant sections within this guidance.

Inherent risk

AUSTRAC has not prescribed a singular scoring model/methodology for inherent risk. Any methodology adopted by a practice should be appropriate to its business, with defensible reasoning to support its approach to risk assessment. A defensible methodology is one that separates judgement from controls, applies consistent logic, is informed by the risk indicators set out in the AUSTRAC Starter Kits and produces outcomes that visibly drive AML/CTF decisions.

Law practices can use qualitative ratings (low/medium/high) or a simple numeric aggregate scoring method (e.g. 1-5) with written explanation of what each score within that range means in terms of risk level; however, the dominant approach for practices of medium or high complexity is a hybrid of the two. The hybrid scoring system combines numeric scoring (discipline and prioritisation) with qualitative narrative (judgement and explainability) to assess a legal practice's inherent AML/CTF risk in a way that is defensible, practical and aligned to the risk indicators as set out in the AUSTRAC Starter Kit Risk Assessments.

A step-by-step method a practice may consider adopting may include the following components. Bear in mind the example below considers designated service risk (but may be also relevant to assessing client, channel and jurisdiction risk factors).

² Department of Foreign Affairs and Trade, Australian Government, *Australia and sanctions: Consolidated List*, DFAT website, n.d.

Suggested step 1: Define the scoring framework upfront

In this first step, the law practice documents:

- their numeric scale (e.g. 1 = low, 2 = low-medium, 3 = medium, 4 = high, 5 = very high)
- what each score means - for example:
 - 3 (moderate): Recognised misuse potential (e.g. simple company setup) but typically limited funds movement/complexity
 - 5 (very high): Known ML typology with high values and complex structures (e.g. commercial property)
- the risk drivers that influence scoring (as identified in the AUSTRAC Starter Kit Risk Assessments):

- transaction value
- handling client money
- ownership/structural complexity
- third-party involvement
- cross-border/jurisdiction
- known typologies for the service.

Defining the framework first prevents score-creep and hindsight/anecdotal bias later in the process.

Suggested Step 2: Score each designated service

The second step in this methodology is to give each designated service a numerical value.

Below is an example of assigning a numeric score.

Table 3.2 Example risk scoring of designated services

Service (and item description)	Numeric score
Residential conveyancing (Item 1: Assisting to buy, sell or otherwise transfer real estate (and often))	3
Business or entity transfers (Item 2: Assisting to buy, sell or otherwise transfer a body corporate or legal arrangement (e.g. business sale))	4
Dealing with client money/assets (Item 3: Receiving, holding or controlling client money or assets)	5
Equity or debt financing (Item 4: Assisting in the organisation, planning or execution an equity or debt financing transaction. Note - no client money is handled)	2
Shelf company sales (Item 5: Selling or transferring a shelf company, in the course of carrying on a business)	4
Company Incorporation (Item 6: Assisting in the creation of a body corporate or legal arrangement)	4
Acting as office-holder (Item 7: Acting as, or arranging a person to act as, a director, secretary, partner or similar office holder)	3
Nominee shareholder or trustee (Item 8: Acting as, or arranging a person to act as, a nominee shareholder or trustee)	3
Registered office/business address (Item 9: Providing a registered office or principal place of business address)	4

Suggested Step 3: Attach qualitative rationale to each score (ensuring language aligns with the Starter Kits)

The rationale should reflect considerations of:

- typical transaction value
- degree of ownership or structural complexity

- whether client money is handled
- frequency of third-party involvement
- whether the service is referenced in AUSTRAC / Financial Action Task Force (FATF) typologies.

Suggested Step 4: Combine scoring and rationale

Below is an example of assigning a numeric score, risk rating and rationale.

Table 3.3. Example of combined risk scoring of designated services with reasons

Designated service	Inherent risk score	Rationale (inherent, pre-controls)
Residential conveyancing (Item 1: Assisting to buy, sell or otherwise transfer real estate (and often) where the transaction is facilitated and money is not handled like in item 3)	3 - Medium	Residential conveyancing typically involves moderate to high transaction values and is a recognised ML/TF typology due to the use of real property for value placement. While client money is not always handled directly, the service facilitates asset transfers that may involve third parties and external funding arrangements, creating elevated inherent risk prior to controls.
Business or entity transfers (Item 2: Assisting to buy, sell or otherwise transfer a body corporate or legal arrangement (e.g. business sale))	4 - High	Business and entity transfers commonly involve higher transaction values, complex ownership structures and changes in beneficial ownership. These transactions are regularly referenced in AUSTRAC and FATF typologies as mechanisms for layering and concealment, resulting in high inherent risk, even where client funds are not directly handled.
Dealing with client money/assets (Item 3: Receiving, holding or controlling client money or assets)	5 - Very high	Direct handling and control of client funds or assets, including the ability to receive and disburse value, creates maximum exposure to placement and layering risk, justifying the highest inherent risk rating prior to controls.
Equity or debt financing (Item 4: Assisting in organising, planning or executing an equity or debt financing transaction. Note - no client money is handled)	2 - Low-medium	Where the service involves advisory assistance for a domestic financing transaction with transparent ownership, without handling client funds or managing assets. While financing arrangements can be misused in some circumstances, the absence of funds control, complex structures or cross-border elements limits inherent risk prior to controls.
Shelf company sales (Item 5: Selling or transferring a shelf company, in the course of carrying on a business)	4 - High	The sale or transfer of shelf companies is a recognised gateway service for obscuring beneficial ownership and enabling misuse of corporate vehicles. The absence of operating history, frequent third-party involvement, and alignment with offshore or complex structures elevates inherent risk notwithstanding that funds may not be handled directly.
Company incorporation (Item 6: Assisting in the creation of a body corporate or legal arrangement)	4 - High	Company creation is a recognised gateway service that can enable structural opacity and later layering, resulting in clear misuse potential, but the lack of funds handling or high-value transactions keeps inherent risk at a moderate level pre-controls.
Acting as office holder (Item 7: Acting as, or arranging a person to act as, a director, secretary, partner or similar office holder)	3 - Medium	Acting as, or arranging a person to act as, an office holder positions the practice within governance and control structures, often without handling client funds. While transaction values are not inherent, the role may facilitate influence over entities and enable misuse in more complex arrangements, resulting in moderate inherent risk prior to controls.

Designated service	Inherent risk score	Rationale (inherent, pre-controls)
Nominee shareholder or trustee (Item 8: Acting as, or arranging a person to act as, a nominee shareholder or trustee)	3 - Medium	Nominee arrangements present inherent opacity risks by separating legal ownership from beneficial control. Although the service does not typically involve handling client assets, its frequent association with concealment typologies and third-party structures supports a medium inherent risk rating before controls are applied.
Registered office/business address (Item 9: Providing a registered office or principal place of business address)	4 - High	When service is limited to providing a registered address for simple, domestic entities with transparent ownership and no other designated services, the risk may be low/low-medium (1 or 2). However given the size and complexity of the structures medium and large practices deal with for their clients, this is elevated to high.

An example of a one-paragraph summary a practice could include in their AML/CTF policy is:

‘The practice’s inherent risk ratings are determined using a hybrid scoring methodology that is informed by the risk indicators set out in the AUSTRAC Starter Kits; those indicators guide judgement and rationale rather than being applied as a mechanical scoring calculation.’

Likelihood and impact assessment

Another way of assessing inherent risk is by conducting a likelihood and impact assessment in accordance with ISO 31000 Risk Management Standards. A likelihood and impact assessment is a structured way of assessing and evaluating risk by assessing the probability that a risk event will occur and the severity of any consequences should it occur.

Likelihood and impact assessments are typically conducted using either a three- or five-point scale to determine the likelihood and impact of a risk event occurring. The likelihood and impact assessment is then used to arrive at an overall inherent risk rating expressed through a risk matrix.

Generally, a three-point scale would be more appropriate for a small practice, with a five-point scale more appropriate for large practices.

Likelihood assessment

The likelihood assessment estimates the probability of a risk event occurring. This can be expressed using qualitative or quantitative methods across either a three- or five-point scale.

The table below demonstrates how this could be conducted using a five-point scale method.

Table 3.4. Likelihood rating definitions

Likelihood rating	Definition
Improbable	The risk is highly unlikely to occur and would arise only in exceptional circumstances.
Unlikely	The risk could occur but is not expected under normal circumstances. It may occur once within a five-year period.
Likely	The risk could reasonably occur from time to time given the nature of the practice’s services, clients or transactions. It may occur more than once within a five-year period.
Very likely	The risk is expected to occur periodically due to the practice’s services, client profile or transaction types. It is likely to occur annually or multiple times over a five-year period.
Almost certain	The risk is expected to occur frequently or in most circumstances due to the nature of the practice’s operations.

If a practice determines that a three-point scale would be preferable, this can be achieved by removing the top and bottom rating categories.

Impact assessment

In assessing impact, the practice considers the potential consequences should the ML/TF/PF risk materialise. This can include potential regulatory, legal, financial, operational and reputational impacts, as well as potential professional or ethical consequences for the practice and its governing body.

Table 3.5. Impact rating definitions

Impact rating	Definition
Insignificant	Minimal impact with no material regulatory, financial, operational or reputational consequence.
Minor	Isolated issue requiring limited remediation; no material breach or external impact but may indicate control weakness if repeated.

Impact rating	Definition
Significant	Notable control failure or risk exposure requiring management action; potential for noncompliance if not addressed.
Major	Material compliance failure or breach requiring regulatory notification and significant remediation effort.
Severe	Critical regulatory breach or systemic control failure with significant and sustained impact across the firm.

Practices of high complexity could expand the impact assessment to consider potential regulatory, legal, financial, operational and reputational impacts, as well as potential professional or ethical consequences for the practice and its governing body, as below.

Table 3.6. Example impact rating and scoring

Impact rating and score	Regulatory/legal risk	Reputational risk	Financial risk	Operational risk	Client relationship risk
Insignificant (1)	No regulatory engagement or compliance concern	No reputational impact or external awareness	Financial loss <0.1% of annual firm revenue	No disruption to normal business operations	No impact on client relationships or service delivery
Minor (2)	Informal regulatory enquiry or clarification with no formal action	Limited internal awareness; no external or media attention	Financial loss between 0.1% and 0.5% of annual firm revenue	Minor disruption requiring limited management attention	Minor client inconvenience with no lasting impact on relationships
Significant (3)	Formal regulatory request for information, review or remediation	Reputational impact within parts of the market or client base	Financial loss between 0.5% and 2% of annual firm revenue	Noticeable disruption requiring active management oversight	Client dissatisfaction impacting individual matters or confidence
Major (4)	Regulatory investigation or enforcement action with potential penalties, undertakings or enforceable actions	Significant reputational damage, including negative media coverage	Financial loss between 2% and 5% of annual firm revenue	Major disruption requiring extensive remediation or resource reallocation	Loss of key clients or disruption to significant client relationships
Severe (5)	Major regulatory enforcement action, including substantial penalties, legal proceedings or licence-threatening outcomes	Major and sustained reputational damage affecting market standing	Financial loss >5% of annual firm revenue	Severe disruption affecting the firm's ability to operate effectively	Significant loss of clients or inability to maintain key relationships

In the above table, each risk category is assigned a risk weighting expressed as a percentage to determine the overall impact rating.

In the table below, each risk rating is assigned a score which is then used to calculate the average score for a particular risk (as demonstrated in the example below).

Table 3.7. Example risk event

Risk event					
An individual client requests the practice to hold funds in escrow pending completion of a transaction with no apparent economic purpose.					
Regulatory/legal risk	Reputational risk	Financial risk	Operational risk	Client relationship risk	Average score
Severe (5)	Severe (5)	Minor (2)	Significant (3)	Significant (3)	3.6
Overall rating			Significant		

The impact rating can be expressed through risk bands (as in the example above), where each risk rating is expressed as a range and the average then falls within that range (e.g. the range for significant is between (3) and (4)).

Alternatively, practices could round to the nearest whole number. In this example that would be (4), which would determine an impact rating of ‘major’.

Overall inherent risk

Once a likelihood and impact assessment has been completed, this is then used to determine the overall inherent risk using a risk matrix.

Below is an example of an inherent risk matrix practices could use to evaluate inherent risk using a likelihood and impact assessment.

Table 3.8. Example inherent risk matrix

Inherent Risk		Likelihood				
		Improbable	Unlikely	Likely	Very likely	Almost certain
Impact	Severe	Low	Medium	High	High	High
	Major	Low	Medium	High	High	High
	Significant	Low	Medium	Medium	High	High
	Minor	Low	Low	Medium	Medium	Medium
	Insignificant	Low	Low	Low	Medium	Medium

Residual risk and control effectiveness assessments

Provisional residual risk

At the time of initial implementation, legal practices are unlikely to have sufficient evidence to reliably assess residual risk. This evidence includes items such as formal documentation of the control and how it is implemented; and control effectiveness testing results.

Therefore, we suggest that you consider an assessment of your provisional residual risk and that this residual risk is **provisionally assessed as the same as inherent risk** across all risk factors. This reflects that, while some controls may exist, they are not yet embedded or evidenced through operational data, quality assurance or control testing.

After conducting the individual risk assessments and allocating a provisional residual risk score (where appropriate), practices of medium or high complexity may also consider conducting an assessment of the control environment and how it manages and mitigates

the risks faced. This could be done by identifying and documenting the controls, assessing the control design and operating effectiveness and then determining the residual risk.


Design effectiveness is a measure of how a control is designed with reference the relevant obligations and risks it is seeking to mitigate. Operating effectiveness is a measure of how the control is operating in practice - for example, whether staff are performing CDD in accordance with the AML/CTF program requirements.

The effectiveness informs and aids medium and large practices in determining the residual risk after controls are applied. Working backwards, if the residual risk level is accepted then the risk factor and its associated inherent risk can be accepted, as it falls within practice’s risk appetite. Medium practices can use this to fill out the Starter Kit Risk Assessment appetite acceptance column in the ‘Inherent risk’ table and the risk appetite acceptance and avoidance columns in the ‘Risk factor’ table. The ‘avoid’ column is the controls you apply in order to accept that risk.



Image 1.1. AUSTRAC Legal Profession Starter Kit – Risk assessment (page 11)

Designated services: Risk factors



This table supports Step 2 in Part 1 of the [Customise the program starter kit guide](#).
Refer to the [customise guide](#) for full instructions on completing the table.

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite – would you accept this risk?	If NO, how will you avoid this risk?
High value transactions	Legal professionals can facilitate or assist with high-value transactions across a range of business areas, including mergers and acquisitions or obtaining complex financing. They're also involved in legal aspects of large asset purchases, investments, and financial markets.	Legal professionals often facilitate high value transactions on behalf of their clients, making them attractive for laundering significant amounts of illicit funds without drawing attention from law enforcement. Some transactions can occur very quickly, including those in commercial matters. This speed of transactions, along with their high value, can allow criminals to move significant amounts of illicit funds in a single transaction.	Medium	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Unusual physical transactions	Any physical currency transactions (for example in AS notes and coins or a foreign currency equivalent) that's unusual in the circumstances. Whether a physical currency transaction is unusual will often depend on: <ul style="list-style-type: none"> its size and complexity if it has an apparent economic or lawful purpose 	Physical currency is anonymous and hard to trace, making it difficult to verify the source of funds. In Australia, it's one of the most restrained, forfeited or frozen asset types in criminal asset confiscation matters. It's exploited for its accessibility, widespread acceptance and availability. Its use also requires minimal skills, knowledge and expertise.	High	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Practices of high complexity will be expected by AUSTRAC to have considered their residual ML/TF risk. Our suggestion is that, even after controls are applied, your residual risk rating will remain the same as your inherent risk for at least the first 12 months or until you have sufficient evidence to assess the effectiveness of the controls.

The residual risk table included in the Risk Assessment is for you to consider and fill out should you deem it appropriate/scalable to your practice. Please be aware that the examples included here are only to give you an idea of the types of controls your practice may wish to apply. Please consider the table and examples in the context of your business and consider which risk rating would be most appropriate to your practice.

Practices of high complexity can build this assessment table into any risk registers they may maintain or develop a new risk register by documenting the risk, its inherent rating and how the residual risk rating was determined. This means including information regarding each of the following:

- inherent risk
- controls in place
- control effectiveness (e.g. effective, partially effective, not effective)
- testing/evidence
- residual risk rating (low/medium/high)
- rationale (for the risk rating).

Where practices of high complexity do not have a risk register or are building a new one, further considerations can be made as to what to include in the register as identifiers or further information outside of the risk rating phase (described above). Items you could consider inserting into the register include, but may not be limited to:

- risk ID - unique identifier for each risk
- risk factors (client, service, jurisdiction, delivery method, with reference to the nature size and complexity of the business)
- key risks and vulnerabilities (risk name): short description of the risk or vulnerability
- practice-specific risk: describes the actual risk the practice is exposed to and why
- likelihood (of the risk occurring)
- impact (of the risk occurring)
- overall risk: low, medium, high, based on the risk methodology
- rationale for the overall risk rating
- controls in place.

“We suggest that you consider an assessment of your provisional residual risk and that this residual risk is provisionally assessed as the same as inherent risk across all risk factors.”

We also suggest that practices of medium or high complexity consider triggers for reviewing and updating the risk assessment (see section 26D of the AML/CTF Act and rule 5-1 of the AML/CTF Rules). Significant changes and trigger sources may include:

- mergers and acquisitions and lateral hires of new practices
- the practice’s use of data, technology and systems and how this can impact the level of ML/TF risk presented, including assessing how issues with data quality and cleanliness can impact the ML/TF risks faced by organisations
- significant changes in global politics, like the Russian invasion of Ukraine, which can create new risks, including the swift implementation of sanctions or shifts in how international funds are moved and stored (such as capital flight).

Throughout the risk assessment, we suggest that practices of medium and high complexity also consider how they use AML-relevant data they already hold about their customers, products, designated services, channels and countries to provide a better understanding of the ML/TF risk profile of its business. This approach aligns with AUSTRAC’s expectation that reporting entities use information obtained through ongoing CDD to review and, where appropriate, update customer ML/TF risk assessments on a relationship-wide basis, rather than a matter-by-matter review. For example, some practices may periodically analyse client data from the preceding 12 months to identify whether there have been changes in country exposure, client typologies or service offerings. This may prompt consideration of whether the firm’s AML/CTF risk assessment, country risk and/or customer risk ratings remain appropriate, rather than requiring automatic reassessment for every new matter.

Risk profiles

Having a profile of each risk type will likely yield data that will assist practices to arrive at an accurate understanding of their inherent risk over the last 12 months, upon which they can rely to update their ML/TF risk assessment.

We understand and acknowledge that more accurate assessments will come with time, as data relating to ML/TF risks will be more relevant, substantive and accessible the more practices are running programs and collecting such data.

Designated service risk

We suggest that you identify all matters which involve the provision of each designated service at section 6, table 6, of the AML/CTF Act. To assist, you may wish to refer to our example template at page 57 of this Guide. As practices of medium or high complexity undertake significant and more complex work, and certain professional services are more prone to be exposed to medium/high inherent risk factors and ML/TF risk typologies than other designated services, this will provide a picture of where the most exposed areas of the practices are, particularly given that practices of medium or high complexity will often have departments for a given type or group of designated services.

As an example, designated service item 3, which involves directly handling client funds (physical or virtual), may be higher risk, as it is exposed to the following factors with high inherent risk:

- unusual physical transactions
- unusual virtual asset transactions.

As such, if a practice provides a high proportion of designated services that are high risk, their designated service risk is likely to be high.

Client risk

Page 66 of this Guide contains an example template to assist medium and large practices to assess client risk. Clients are broken down into total number for each client type and then how many of those clients within each client type have two medium risk factors and how many have a high risk factor.

Where a practice has a higher proportion of clients within a client type that is not an individual or sole trader (e.g. a number of government bodies or overseas clients), this may translate to a higher risk level, as there may be more domestic and foreign PEP considerations (which are both medium and high inherent risk) than a practice that does not provide services to government bodies (such as a small regional law practice). Where it is a practice of medium complexity that has a large / majority domestic individual / sole trader or simple corporate structure clients, the low inherent risk rating may be more prominent, because it does not involve international aspects and complex legal structures that could conceal or obscure ownership.

Channel risk

To assist medium and large practices assess channel risk, page 74 of this Guide contains an example template which breaks down designated services per service delivery channel. This is intended to provide practices with insight into their potential exposure to fraudulent identities.

Where a practice of medium or high complexity provides a larger proportion of designated services through channels which require more controls to

reduce, mitigate or manage risk, we suggest that a medium or high inherent risk rating may be the more likely outcome. For example, if there are no mitigating factors, risk will likely remain high where the law practice communicates advice through online conference platforms (WebEx, Google Meet) rather than in person, as there are always online security vulnerabilities which do not arise if the meeting is in person.

Jurisdiction risk

To assist in assessing jurisdiction risk, page 76 of this Guide contains a suggested template which breaks down the countries dealt with by the number of designated services involving the country and the number of clients within that country.

Given practices of medium or high complexity are more likely to deal with clients that are based overseas, understanding whether there are any services provided to low/medium/high risk countries, and how many services are provided, allows the practice to identify, in conjunction with resources like the Basel AML Index, the jurisdictional risk the practice has been exposed to in the last 12 months.

For example, knowing and documenting that 300 of 1,500 (20%) designated services and 150 out of 1,000 (15%) clients serviced in the last 12 months involved clients from China (a high-risk country per the Basel AML Index) would give a legal practice reliable insight into its inherent jurisdictional risk level.

Certain jurisdictions will also pose higher sanctions risks. Currently DPRK, Russia, Iran and Myanmar are high risk due to the breadth of sanctions and the imposition of sanctions on their financial sectors (e.g. major banks).

For practices operating across multiple international jurisdictions (more likely larger practices) it may be worth first considering how you will structure your practice's Enterprise-Wide Risk Assessment (**EWRA**). Depending on the practice, how many jurisdictions it operates in, how many clients are based inside/outside of Australia and where specifically the practice's offices and/or clients are located, the EWRA may be sectioned off in more of a business unit structure. For example, you may break it up:

- by servicing team - separate assessment for area the service is provided - for example, residential conveyancing/commercial conveyancing/trust services et cetera
- by department - separate assessment for team function - for example, compliance, finance, administration, human resources
- by country - one for Australia and one for every other country the practice has a permanent establishment in.

As the individual business units will deliver more valuable and relevant risk data, this provides larger practices with the ability to more accurately measure

and understand with more granularity the ML/TF risks in both a business unit and larger EWRA context.

Risk assessment examples

Large practices: suggested risk assessment structure

As noted previously, the AUSTRAC Starter Kits are not suitable for practices of high complexity. In place of the structure set out in the Starter Kits, and in line with the considerations of the analysis required (as detailed in above sections), the following are two examples of structures (both of which should be adapted to suit the practice) that may be used for the ML/TF risk assessment.

Example 1

1. **Introduction**
 - a. Summary
 - b. Purpose (reference to the Act)
 - c. Risk assessment approach
 - d. Risk methodology
 - e. ML/TF/PF - high-level description
 - f. Practice's risk appetite
2. **Risk assessment analysis**
 - a. Nature, size and complexity
 - b. Service
 - c. Clients
 - d. Jurisdiction
 - e. Delivery method

Note: In this section, risks can be presented (directly from the risk register) in a simple two-column table (Risk / Risk rating) under each factor (noting any overlap), including key insights backed up with the results of data analysis (graphs where relevant). A risk rating is given with a detailed rationale for each risk factor.

3. **Overall risk assessment**
 - a. Risk assessment table setting out each risk factor and its risk rating
 - b. Practice's overall risk rating (which may differ from the national risk assessment)
 - c. Rationale is provided explaining the overall risk rating, keeping the risk assessment current
 - d. Full risk register
4. **Appendices (including, but not limited to):**
 - a. Definitions of ML/TF/PF
 - b. Red flags - indicators of unusual or criminal behaviour
 - c. Sector risk assessment table (if there will be one in Australia)
 - d. Guidance material (risk assessment sources)
 - e. Glossary
 - f. Version control table

Example 2

1. Version control
2. Overview/summary
 - a. ML/TF risk assessment sources (similar to Starter Kits but also including [Reform guidance - Step 2: Identify and assess your risks: risk assessment \(Reform\)](#) and suspicious indicators (from AUSTRAC))
 - b. Purpose of the Act - section 5
 - c. Overview of ML/TF risks
 - What is ML
 - What is TF
 - What is PF
 - What is exploitation
3. Purpose
 - a. Obligations
 - ML/TF risk assessment approach - this is written; tailored to firm’s nature, size and complexity; and based on the firm’s inherent ML/TF risks, by having regard to ML/TF risk categories (see section 26C(3)(a)-(d) of the AML/CTF Act and ML/TF risk matters (section 26C(3)(e)-(f)) (these also include risk factors in Starter Kits as appropriate))
 - Conducting the firm’s ML/TF risk assessment - follow [step 2 of AUSTRAC Risk Assessment guidance](#) for examples on how to:
 - i. identify the firms inherent ML/TF risks
 - ii. assess/score these risks to understand the scale of each risk by the likelihood and impact of each risk
 - iii. evaluate these risks by taking a risk-based approach and prioritising where appropriate AML/CTF controls that are proportionate to mitigate and/or manage these risks and, if needed, update the firm’s client risk rating methodology
 - iv. review the firm’s ML/TF risk assessment for effectiveness to ensure the firm’s inherent ML/TF risks continue to be appropriately managed and/or mitigated
 - ML/TF risk categories - listing each (section 26C(3)(a)-(d) of the AML/CTF Act)
 - ML/TF risk matters - listing each (section 26C(3)(e)-(f) of the AML/CTF Act)
 - b. ML/TF Risk Assessment application - whether it applies to all or parts of the practice
 - c. Client risk rating (**CRR**) system - how this applies to the client and the associated level of controls and level of CDD that applies for each level of risk (e.g. low = simplified CDD, medium = standard CDD, high = standard CDD + enhanced CDD) and the process to risk rate - that is, mentioning a client CRR is separate from the firm’s rating process and is on a case-by-case basis, based on the client’s ML/TF risk categories and ML/TF risk matters (standard and/or enhanced CDD triggers e.g. low risk client with a foreign PEP escalates to high-risk, or a client with a low risk client type, country, delivery channel and designated service = low risk). For example, an initial CRR can be rated to obtain an initial level of CDD to apply to the client and, once all ‘Know Your Client’ (**KYC**) information has been obtained and screening completed, if the risk is different, the practice can apply a different risk level and request any further KYC information. If the risk remains unchanged then the initial CRR may remain in the final CRR system
4. Inherent legal sector ML/TF risks (from Starter Kit Risk Assessment) - could also link to the [Current National Terrorism Threat Level](#)
5. Practice’s overall ML/TF risk - this is a summary of the practice’s ML/TF risk category scores providing an overall risk rating and may include a couple of paragraphs explaining the key facts that inform the overall rating from all categories. These may be listed in a table based on their overall category and overall average scores - for example, see the table below

Table 3.9. Example of practice’s overall ML/TF risk

ML/TF risk category	ML/TF category risk rating	ML/TF category score
Designated services	Medium	13
Clients	Low-medium	9
Countries	Low-medium	9
Service delivery channels	Low	5
Overall ML/TF 5 level risk rating	Low-medium	9
Overall ML/TF 3 level risk rating	Low	

6. Risk assessment methodology
 - a. Identification of inherent ML/TF risks
 - data used to identify these risks - for example, internal firm personnel and client, country and designated services data and trust account information
 - AUSTRAC data - for example, suspicious indicators relevant to the legal sector as per the National Risk Assessment
 - b. Assessment of inherent ML/TF risks
 - likelihood and impact ML/TF risk assessment methodology
 - i. explain the likelihood and impact method, scales and matrix, used as per AUSTRAC step 2 and in this Guide
 - ii. explain how an inherent ML/TF risk rating is determined - for example, likelihood x impact = inherent ML/TF risk score and rating (e.g. a 9 may = low or a 25 may = high risk)
 - c. Evaluation of inherent ML/TF risks
 - explain how the inherent risk rating relates to AML/CTF controls, table example below
7. Nature, size and complexity of the firm
 - a. Nature - comment on practice's nature, including practice groups and what designated services they provide if possible
 - b. Size and complexity - comment on practice's size and complexity in relation to ML/TF risk categories
8. Practice's ML/TF risk categories assessment (for each category, mention overall risk score and rating; and any relevant statistics that support this rating), refer each category to your practice's DS ML/TF risk assessment. This can be maintained in a spreadsheet and linked to keep the document length simple and include the following:
 - a. Designated services
 - b. Clients
 - c. Service delivery channels
 - d. Countries - take all clients or a subset (e.g. you can use data from the last financial year) and apply the jurisdiction list rating to each client with a designated service and work out the percentage of designated service clients being low to high on a 5 and/or 3 risk scale to determine the overall firm rating for this category
 - e. Country risk methodology - you may wish to use the AUSTRAC Starter Kits approach or customise your own and detail the methodology and sources here or in your policies document
9. ML/TF risk indicators - list out as per AUSTRAC Starter Kits and suspicious indicators as relevant for the firm
10. Glossary

Table 3.10 Example responses to inherent risk ratings

Inherent risk rating	Firm risk response
High	Apply appropriate AML/CTF policies as a high priority, with enhanced measures, including additional controls to mitigate this risk.
Medium	Apply appropriate AML/CTF policies with standard measures, to effectively manage and/or mitigate this risk.
Low	Apply appropriate AML/CTF policies, with simplified measures, to manage this risk.

Policy

Where a legal practice has been assessed to be a practice of medium complexity (e.g. using our suggested self-assessment tool), you may wish to assess whether the policy document within the Starter Kits is appropriate for your business and identify any changes you need to make or, in the case of a large practice, items you might want incorporate into your own AML/CTF program.

The policy document consists of 3 parts:

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

Each part contains elements that may be adapted to a practice of medium complexity after completing the self-assessment tool.

Part 1: Personnel

The 'Personnel' section of the AUSTRAC-issued policy details the requirements for legal practices to fill and appoint key roles and conduct suitable personnel due diligence on those involved in AML/CTF activities, as well as providing those personnel with appropriate training.

Practices of high complexity are, of course, not required to consider the specific requirements for single practitioner practices, as these practices are exclusively small and have one person in charge of all AML/CTF activities and complying with the obligations as set out in the AML/CTF Act and AML/CTF Rules.

However, we suggest practices of medium or high complexity consider the requirements and suitability of different personnel to fulfil the roles of:

- governing body
- senior manager
- AMLCO
- any other personnel who will meet its AML/CTF obligations, such as the solicitor who has day-to-day responsibility for liaising with the client or managing the matter. However, we suggest that, for practices of medium and high complexity, AML/CTF personnel due diligence is only required for staff who have an AML role as defined in our [Implementation Guide: for sole practitioners and small practices](#) - that is, persons in the legal practice who have AML/CTF duties or that discharge AML/CTF obligations. For example, while a receptionist at a medium or large firm may have occasional contact with clients, if they are not provided with an AML/CTF role (e.g. responsibility for collecting and verifying information for initial CDD), AML/CTF personnel due diligence is not requirement for their

role. Similarly, a solicitor who assists in the running of a matter involving a designated service but is not given AML/CTF duties can also be excluded, despite the fact that they may become aware of the potential need to conduct enhanced CDD or escalate a matter to the AMLCO or AMLCO team to determine if a suspicious matter obligation has arisen. However, we suggest that personnel who are reasonably expected to have an AML/CTF role (e.g. conducting enhanced due diligence checks, such as making inquiries into a client's source of funds or source of wealth (**SoW**)) should be included in AML/CTF personnel due diligence checks and processes. Other roles that are likely to have AML/CTF duties include:

- human resources (**HR**) personnel who conduct employee due diligence (beyond merely confirming that a practising certificate is held, e.g. police checks)
- support staff who screen clients
- staff that undertake KYC and assess ML/TF risk
- finance personnel for transaction reporting and monitoring
- the partner responsible for determining whether an obligation to undertake enhanced CDD or make a Suspicious Matter Report (**SMR**).

We suggest that personnel due diligence procedures and training policies are carried out in accordance with the Starter Kits policy but disregarding sections regarding single practitioner practices or where the AML/CTF compliance officer is the governing body.

As identified above, given practices of medium or high complexity will likely have a wider array of personnel engaged to perform AML/CTF-related functions, AUSTRAC is likely to expect that such practices can show that:

- there has been deliberate consideration of who does what in the AML/CTF program
- core AML/CTF concepts are delivered to all relevant staff
- enhanced or specialised training is provided where staff have greater risk exposure or control responsibilities.

While training needs should be assessed on a role-by-role basis, you may wish to group roles with similar AML/CTF risk profiles and functional responsibilities into cohorts for training purposes, with additional or enhanced training applied to higher risk or specialist roles as appropriate.

Table 4.1. Example of training cohorts

Training cohort	Typical roles included	Training focus
Cohort 1 - All staff (baseline)	All employees, contractors, secondees	AML/CTF fundamentals, recognising red flags, obligation to escalate concerns
Cohort 2 - Client-facing intake roles	Reception, client services, paralegals, junior lawyers	CDD basics, identifying suspicious behaviour, information collection requirements
Cohort 3 - Matter owners / deal leads	Partners, senior lawyers, engagement leads	Risk assessment, source of funds/wealth, matter-level escalation, ongoing monitoring
Cohort 4 - AML/CTF operational support	AML analysts, risk/compliance team	Detailed AML/CTF Rules, enhanced due diligence, SMR thresholds, record-keeping
Cohort 5 - Senior management and principals	Board, partners, practice leaders	Governance obligations, risk appetite, breach implications, AUSTRAC expectations
Cohort 6 - AML/CTF compliance officer	Nominated AML/CTF compliance officer	End-to-end regime, reporting, training oversight, AUSTRAC engagement

To assist, you may wish to consider the training template included in our [Implementation Guide: for sole practitioners and small practices](#).

Part 2: Clients

In our view, the policies set out in Part 2 of the AUSTRAC Starter Kits may be used by practices of medium and high complexity if they consider the policies to be appropriate for their use.

All practices are required to report to AUSTRAC under certain circumstances, with some potentially non-applicable, depending on business practices:

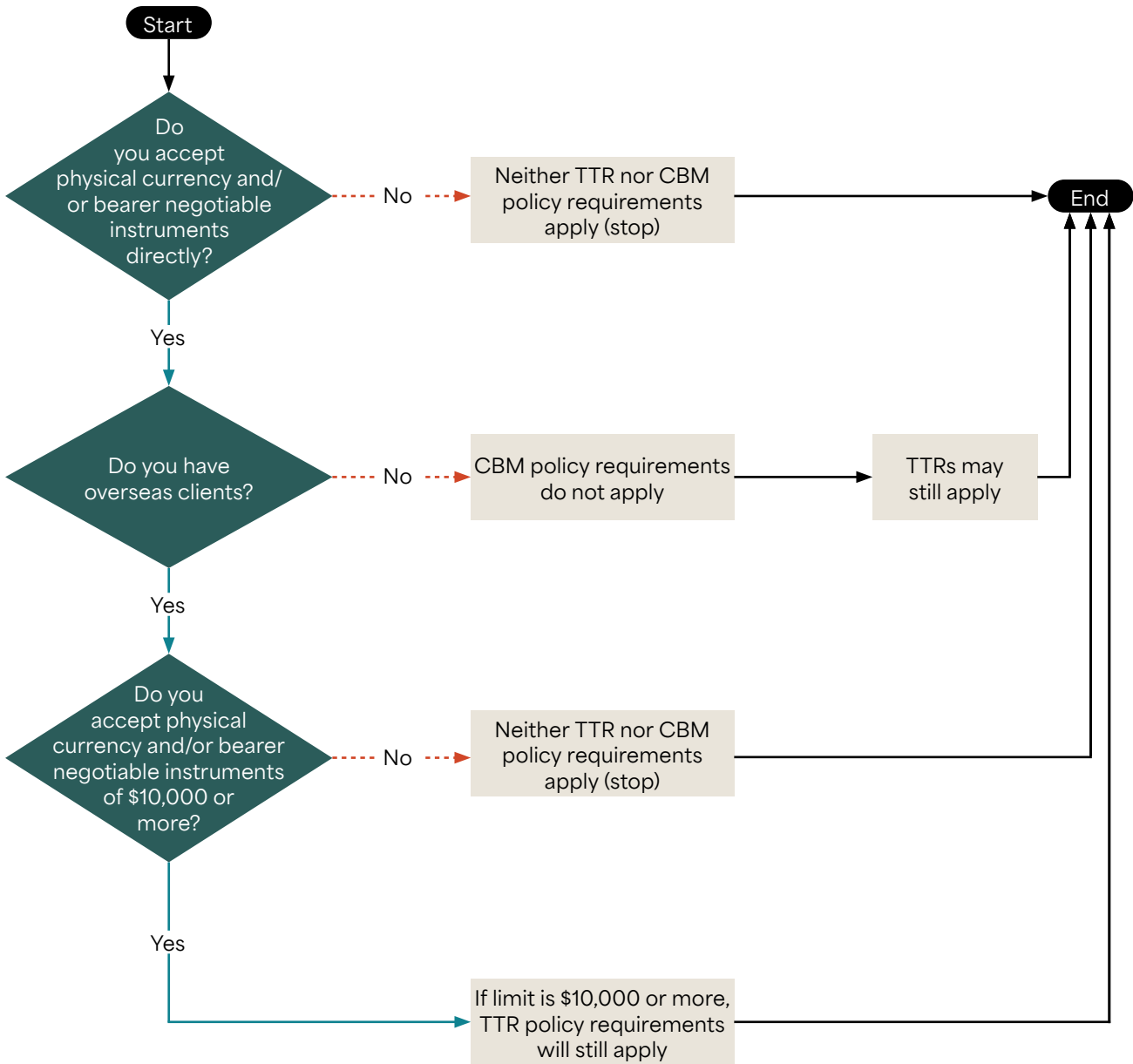
- Threshold transactions: any physical currency transaction valued at \$10,000 or more
- Cross-border movements: cross-border movement of physical currency and/or bearer negotiable instruments, valued at \$10,000 or more. Note: 'bearer negotiable instruments' refers to the physical movement of cash-like instruments. The obligation to report cross-border movements does not extend to ordinary electronic funds transfers, settlement payments or routine trust account transactions conducted through the regulated banking system. In practice, most legal practices are unlikely to encounter bearer negotiable instruments in the course of providing legal services, and the reporting obligation will typically

only arise in limited and unusual circumstances involving physical instruments.

As practices of medium or high complexity are more likely to have clients that are overseas than small practices, additional considerations may arise whether your practice allows for these transactions to take place. If so, you could consider the following questions (in order):

- Do you accept physical currency and/or bearer negotiable instruments directly?
 - If no, both Threshold Transaction Reports (**TTR**) and Cross Border Movements (**CBM**) policy requirements do not apply (and there is no need to proceed further with other questions).
 - If yes, TTR and/or CBM policy requirements may still apply.
- Do you have overseas clients?
 - If no, CBM policy requirements do not apply; TTR may still apply.
 - If yes, do you accept physical currency and/or bearer negotiable instruments of \$10,000 or more?
 - If no, both TTR and CBM policy requirements do not apply.
 - If yes and limit is \$10,000 or more, TTR policy requirements will apply.

Image 2.1. Example TTR and CBM risk management



For ease, please refer to the diagram above for a suggested approach to managing TTR and CBM risk, depending on your practice’s risk appetite regarding them.

Where one of / both TTR or CBM reporting requirements do not apply to your practice, this should be reflected in your AML/CTF program accordingly.

We consider that usual trust accounting rules, controls and procedures apply in the above circumstances. If you have any trust accounting related inquiries, you can direct them to trust@lawsociety.com.au.

Part 3: Maintaining your AML/CTF program

In our view, the policy relating to maintaining your AML/CTF program as provided in the Starter Kits is largely applicable without amendment. However, we suggest that you amend your maintenance policies if you identify that one or more AUSTRAC reporting requirements (e.g. CBM, TTR, as described above) are inapplicable or irrelevant to your practice. In such case, consider noting specifically in your policy that the related effectiveness tests and controls in relation to TTR and CBM are not applicable.

Processes

Generally speaking, there are a number of key areas where practices of medium or high complexity may wish to adapt the Starter Kit processes to their businesses. Where Starter Kit processes are adopted, there are likely to be additional considerations to make to their AML/CTF processes, which we suggest are both documented and put into practice.

These areas are:

- client risk and client due diligence (including transition of pre-commencement clients)
- reporting
- AUSTRAC communication
- enrolment
- escalation of particular matters to the AML/CTF compliance officer.

For example, practices of medium complexity may wish to update the process documents to specifically refer to the following systems/platforms/controls relevant to them. These may include:

- the client relationship management (**CRM**) or practice management software you utilise
- e-verification providers
- third-party search vendors
- screening platforms
- where digital files are stored
- standard operating procedures for onboarding and reporting.

Practices of medium or high complexity may wish to adopt and adapt their own process documents with the same considerations, in the context of their larger scale operations.

Consider ensuring that your process documents appropriately reflect considerations of the ML/TF risks identified in your risk assessment; and how you mitigate and manage those risks and the processes you undertake to deal with the risks and your clients' risk factors. You may wish to include specific considerations for:

- identification documents, including any practice specific alternatives
- beneficial owners
- industry examples in the 'inherent risk' and 'country risk' sections – that is, what you, as a practice of medium or high complexity, consider as relevant industry examples to adopt or adapt into your process for looking at inherent risk and your country risk

- typical document sets for your real client base – that is, what specific document/s would your practice expect to see on file (specific form of ID, certain formal engagement documents et cetera).

Reflect your practice's practice mix and client base

We suggest that your process document appropriately reflects:

- the types of services you provide – for example, whether you handle regular conveyancing, corporate work, high-risk industries, or overseas clients
- the types of entities you service – for example, whether you engage with trusts, self-managed superannuation funds, partnership structures or charities
- the types of clients you serve – for example, whether you often act for foreign individuals or entities (which changes sanctions, country risk and beneficial ownership requirements).

AUSTRAC enrolment process

Enrol with AUSTRAC

Practices of medium or high complexity can approach initial AUSTRAC enrolment in a more structured, coordinated and forward-looking way than small practices, reflecting their larger and more complex operations (broader service offerings, larger personnel base and more complex client and transaction profiles).

Rather than treating enrolment as a one-off administrative task, we understand that larger practices abroad typically integrate enrolment into their broader AML/CTF governance framework, ensuring that designated services are accurately mapped; responsible roles are clearly defined; and enrolment data aligns with risk assessments, onboarding workflows and internal systems from the outset.

With increased resources, it may be beneficial for your practice to apply stronger internal controls around accuracy, approvals and record-keeping. For example, your practice may benefit from:

- involving compliance specialists, senior management and risk committees in confirming the scope of designated services

- ensuring AUSTRAC records are complete and consistent
- embedding enrolment obligations into ongoing compliance calendars and system controls.

This reduces the risk of under-enrolment, misclassification of services and governance gaps as the practice grows or diversifies.

In the establishment of enrolment controls, we suggest that these controls consider triggers and ownership for updating enrolment as the practice grows or changes.

Update AUSTRAC enrolment details

If your practice is a partnership, you are only required to provide details regarding a partner who is an individual (or is a member of a group of individuals who have) primary responsibility for the governance and executive decisions of the partnership.³

We suggest, therefore, that, if your practice does not provide details of every partner of the practice, you document reasons for limiting the selection to a smaller group - for example, in a file note that identifies a group of senior management partners for the purpose of enrolment with AUSTRAC.

Nonetheless, we recognise that providing the required details of each relevant partner involves a significant level of operational burden, even where AUSTRAC has provided some leniency on time. We understand that AUSTRAC's expectations are for medium and large practices to proactively manage enrolment information to appropriately reflect your strong governance and internal controls.

Your practice may benefit from incorporating existing AML/CTF activities into the partner review process and update of any personal information. For example:

1. Add a slide to the partner induction pack and annual ethics/AML/CTF training that explains what types of changes matter for AUSTRAC enrolment. This could also include a link to the internal notification form for any change in details for compliance to report. As part of this, training could be completed on an annual basis across the practice (rather than on the anniversary of employment), so that all information is able to be updated in one instance each year.
2. Set automated six-monthly reminders for the compliance team to review enrolment details, and pair this with risk review cycles required under the practice's AML/CTF program.

Client risk rating and ongoing customer due diligence process

Applying an ML/TF risk rating

In developing and documenting the process for how your practice plans to record an ML/TF risk rating to a client during onboarding (i.e. after reviewing the initial CDD (ICDD) form), we suggest:

- practices of medium or high complexity should consider leveraging an existing practice management software and CRM platform and third-party provider, and
- if your CRM does not already have this capability, consider selecting a CRM that allows you to store multiple notes for both initial and future documents for facilitation of future reviews of risk rating, which are required by statutory triggers,⁴ but also at a minimum on an appropriate, risk-based periodic basis (e.g. high-risk, one year; medium-risk, three years; low-risk, five years et cetera).

For practices of medium or high complexity, ICDD is expected to be conducted at the commencement of the overall client business relationship only, rather than the start of each matter. This is the case even where the client requests multiple designated services. Although individual matters may resemble occasional transactions, they are typically undertaken within an established and ongoing client relationship and monitoring applied on a relationship-wide basis, taking into account the nature and pattern of matters over time.

Applying risk-based ongoing customer due diligence

For ongoing CDD and review of their risk rating during your practice relationship with the client, consider detailing in your procedures one or more of the following, as appropriate:

- Where clients are not handled face-to-face, monitor their behaviour - this will mean reviewing the notes stored in CRM or online/over-the-phone interactions.
- For escalation trigger and actions processes, including the completion of a form, consider building this functionality into your CRM or sourcing to a provider with an electronic form capability functionality.
- Ongoing monitoring may be performed by back-office staff / executive assistants / finance staff, not just the lawyer involved in the matter. If you do this, these staff will need to be trained appropriately, and training material should be adjusted accordingly.

³ *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* (Cth) r 3-3(5)(a).

⁴ *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 30(2); *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025* (Cth) r 6-35.

- For practices of medium and/or high complexity, which are more likely to have longer term relationships with clients, where they act on more than one matter (even where it is low risk) and are more likely to have higher risk clients, it may be worth consistently measuring your level of ML/TF risk, so that ongoing monitoring is appropriately applied and revised where necessary.

Pre-commencement clients

We understand that medium and large practices are likely to have large numbers of clients prior to 31 March 2026, which may be considered as 'pre-commencement clients'. In many cases, these will be longstanding clients with multiple historical matters, often serviced across different practice groups, and for whom the practice holds varying degrees of existing client knowledge.

In our view, section 36 of the AML/CTF Act permits a matter that is currently on foot to proceed without interruption (e.g. to continue to run without requiring ICDD to be carried out mid-matter). This may include litigation, advisory or transactional matters that commenced prior to 31 March 2026 and continue on or after commencement, provided the scope of the engagement has not materially changed.

However, depending on the circumstances, we consider that it is open to practices of medium or high complexity to consider how they handle pre-existing clients who provide instructions for a new designated service, commencing on or after 1 July 2026. This issue is most likely to arise where a pre-existing client engages the practice for a new matter that falls within the designated services regime for the first time or where the new matter introduces new features not previously present in the client relationship.

Generally, it will be a decision for your practice as to whether you consider it more appropriate to either:

- 'front-load' your AML/CTF controls - that is, conduct ICDD for all existing clients that approach your practice with instructions for a new matter involving designated services on or post 1 July 2026. This approach may be adopted, for example, where the new matter involves different jurisdictions, ownership or control structures, sources of wealth or funds, or other features that materially differ from the client's prior engagements. In these circumstances, you may consider using delayed ICDD (see section 29 of the AML/CTF Act) where appropriate,⁵ or

- utilise section 36(4) of the AML/CTF Act for pre-existing clients who request a new service post 1 July 2026 - that is, where a pre-existing client provides instructions for a new designated service post 1 July 2026, your practice deems that client as a 'pre-commencement customer' under section 36 of the AML/CTF Act and merely conducts sufficient checks to determine that there is no significant change to that client's (or their matter's) risk profile. This may include confirming, for example, that there are no changes to beneficial ownership or control, no new third-party payment arrangements and no new high-risk jurisdictions; and that the nature and purpose of the new matter is consistent with the client's known activities.

Example of handling a pre-commencement client

Where a client has received, or is receiving, a designated service from a practice prior to 1 July 2026 and continues to request the same designated service post 1 July 2026, the practice may consider conducting a client and matter risk assessment to determine if there have been significant changes in their nature or purpose of the business relationship which might result in their customer risk rating as medium or high or triggering an SMR obligation. These significant changes may include a new designated service being requested, a change in country jurisdiction, unusual client behaviour or unusual transactions or behaviours.

Where the risk rating has been determined as 'medium' or 'high,' the practice may decide that ICDD is required before opening the matter and commencing to provide the designated service (unless delayed ICDD applies). However, where the rating is determined as 'low', the practice may elect to open the matter and commence working on providing the designated service.

Each practice's approach to pre-commencement clients will likely vary, depending on their practice's ML/TF risk profile, as well as their resourcing and capacity.

Regardless of which approach your practice elects to adopt, we suggest that you document that approach in your AML/CTF policy, noting the circumstances in which ICDD must be completed. We further suggest that the approach you select is informed by your practice's risk assessment.

⁵ See *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 29.

Using delayed initial customer due diligence

We suggest that, in your AML/CTF policy, you consider (and document) the circumstances in which your practice will delay conducting ICDD as per section 29 of the AML/CTF Act. For example, it may only be appropriate to utilise delayed ICDD where the client is of low ML/TF/PF risk,⁶ the designated service must commence urgently and there is no suspicion of ML/TF/PF. In applying section 29, we suggest that, in considering whether the designated service is 'essential to avoid interrupting the ordinary course of business', you consider your practice's business, and not the client. However, we note that, as the provision of legal services is predominantly underpinned by the existence of a fiduciary relationship rather than a transactional relationship, the client's business will often, if not always, impact the legal practice's ordinary course of business.

Initial client due diligence where the practice is part of a reporting group

For practices of medium or high complexity with international clients - where a practice within a reporting group proposes to provide a designated service to a client (and a service was previously provided by that same practice or another practice within the reporting group) through a permanent establishment in a foreign country, the practice may consider ICDD obligations to be satisfied if any of the following criteria are satisfied:

- The foreign country gives effect to the FATF recommendations on CDD and record-keeping.
- The foreign entity was not required to establish the relevant matter due to a low assessed risk of ML, TF or PF.
- The matter was established in accordance with those laws.

AUSTRAC's expectations for what this means in practice are as follows:

- You may transition different customer classes at different times, but each class must only be subject to one ICDD approach at a time.
- You must apply the new ongoing CDD obligations to all customers from 31 March 2026.
- Any operational overlap should be temporary, documented and controlled.
- All other obligations under the AML/CTF Act continue to apply.

To comply with these expectations and given the quantum of pre-commencement clients medium and larger sized practices will have when entering the AML/CTF regime, we suggest that practices consider the following steps:

- Note any required updates to existing policies/procedures, including a CRM system or other platforms used in the current due diligence.
- Construct a remediation plan, including resources required to execute.
- Make a record of clients which had insufficient CDD applied to them.
- Construct a timeline which will allow these clients to be transitioned over to have CDD correctly applied in line with new legislative requirements.
- Integrate updates into the CRM and onboarding policies.
- Implement new policies which meet the standard to all new onboarded clients.

Statutory declaration process

The standard statutory declaration process outlined in the Starter Kits provides guidance that may be applied to essentially all legal practice sizes if considered appropriate in the absence of an alternative process. However, statutory declarations are not in themselves a requirement in the AML/CTF Act or Rules.

For practices of medium or high complexity, when establishing a process for determining circumstances that may affect a person's suitability for a relevant role, the practice may incorporate or leverage existing internal HR capabilities and/or document management platforms for necessary record-keeping.

We understand that, in many cases, medium, and more likely large, practices will be relying on the fact that most individuals undertaking AML functions will have a current legal practising certificate which must be renewed annually. Should this be the case, we suggest that practices include in the documented process that the practising certificate is used in place of a statutory declaration, and it serves as sufficient evidence of the candidate's suitability to perform the relevant role. You may wish to recognise in your documented process that, in order to renew a New South Wales practising certificate, solicitors must disclose to the Law Society of New South Wales the relevant regulator; any matter that may be relevant in determining whether they are a fit and proper person to hold an Australian practising certificate, including if they have become subject to disciplinary proceedings; if they are the subject of an unresolved complaint; or if they have been removed from the roll of any Australian jurisdiction or foreign roll of lawyers.⁷

⁶ Consider section 29(d) of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

⁷ When applying for the grant or renewal of a practising certificate in New South Wales, applicants must address each of the matters referred to in r 13 of the *Legal Profession General Rules 2015* (NSW).

Verify the nature and purpose of the practice process

Practices of medium or high complexity may have more relationships and information to verify and subsequently monitor, as a result of having:

- a larger client base (in number and in size)
- more complex clients (e.g. multi-jurisdictional, complex ownership structures et cetera).

With practices that service these larger and/or more complex clients, considerations for this process could include:

- Verifying KYC information against more complex sources - for example, foreign company registers and databases that are not necessarily readily accessible for small practices. This can include the adoption/utilisation of e-verification providers.
- In line with reliable and independent documentation requirements, include steps relating to verifying translations of foreign documents (e.g. certificates of incorporation, trust agreements) where necessary.

Source of funds and source of wealth check process

Source of funds

Practices of medium or high complexity may have more (in number and in complexity) clients with more intricate wealth structures and potentially confusing and/or larger sources of funding to establish and verify, which makes CDD more labour intensive.

Medium or larger entities are dealing with larger scale matters that are the subject of any legal advice or relationship, including larger sources and structure of funding - for example, significant mergers and acquisitions and capital markets transactions, major projects, large or complex property developments and cross-border work.

Medium and larger practices could consider, depending on the nature of the identified funds, whether multiple rounds or sources of certification are required. These can be completed using tools such as:

- bank data analysis platforms that allow clients to share verified banking information directly and automatically highlight the origin and flow of funds
- tools that help map beneficial ownership.

Practices of medium or high complexity may also consider incorporating document-authenticity solutions, such as validation of financial statements, bank documents or identity materials used to support assertions about the source of funds.

Source of wealth

Medium or larger entities often source their capital and wealth from multiple sources when starting up. Over

time, these sources can grow significantly in number/value, requiring more work effort to verify them. This could involve investor groups, equity practices, multiple smaller practices and individual investors.

Consistent with AUSTRAC's guidance, practices of medium or high complexity should apply a risk-based approach to SoW assessments, scaling the nature and depth of verification to the specific ML/TF risk presented by the client and the matter. Enhanced or more structured verification should not be applied by default but considered only where risk indicators are present or where readily available information is insufficient to reasonably support the stated SoW.

In practice, many large or more complex clients, such as listed entities, regulated institutions or entities owned or controlled by governments, often present lower SoW risk due to the availability of transparent, reliable and independently verifiable public information. In these cases, reliance on publicly available financial reporting, regulatory disclosures or government sources may be sufficient, without the need for additional certification or specialised verification tools.

Where higher SoW risk is identified - for example, due to complex private ownership structures, opaque jurisdictions or unusually high-value transactions - some medium and larger practices may choose to use proportionate, targeted measures to support their assessment. This may include consolidating existing financial information into a consistent record or using supplementary intelligence to sense-check whether the client's stated wealth profile is broadly consistent with known public or commercial information.

Combined with internal governance measures such as escalation or partner approval for higher risk matters, this approach supports SoW assessments that are reasonable, defensible and aligned with a risk-based framework, without imposing unnecessary complexity where risk is demonstrably low.

Sanctions check processes

Personnel carrying out a sanctions check

Practices of medium or high complexity in general are much more likely to use a screening software provider rather than looking at the Department of Foreign Affairs and Trade Consolidated List. To enhance the sanctions screening process, these practices should consider:

- an automated sanctions screening platform for comprehensive, up-to-date checks
- continuous or periodic re-screening for long-running matters or higher risk clients
- centralised AML workflow systems to ensure consistent documentation of screening completed, including printouts of results, review notes and audit trails
- defined escalation procedures for potential sanctions matches.

Responding to a positive sanctions check

By virtue of having more complex and more international clients, the higher likelihood for sanctions to return a positive match is a point of note for medium and large practices.

As such, we suggest adopting a detailed and thorough sanctions check process. While the Starter Kits cover how to deal with positive matches in a high-level manner, practices of medium or high complexity may want to consider additional or more detailed steps in the process, such as one or more of the following:

- running secondary and tertiary verification using additional sanctions screening platforms to confirm the match
- adopting more formal governance mechanisms to adjudicate the match - for example, risk committees, senior partner approval or internal legal counsel for high-risk decisions
- developing a more comprehensive audit trail.

From there, legal practices could consider maintaining the same requirements as detailed in the Starter Kits, including notifying the Australian Sanctions Office and Australian Federal Police, or determining the requirement on a practice-by-practice basis.

Politically exposed person checks

Initial searches

In general, practices of medium or high complexity may benefit from adopting PEP screening software provider or databases for PEP screening, beyond just online keyword searches.

Given the level of complexity of clients, corporate structure and implications of multiple related parties, medium and large practices could also consider incorporating into their PEP check processes one or more of the following, as appropriate:

- multi-jurisdiction data to identify PEPs in foreign political systems where manual searching may be difficult
- PEP screening of all beneficial owners, directors, trustees, authorised signatories, family members and related parties using systems capable of handling:
 - multiple name spellings, transliterations and alias detection
 - foreign-language name matching
 - geographic risk weighting
- multiple screening platforms for cross-validation between datasets
- a detailed internal PEP-review register so the AML compliance team sees consistent risk classification
- structured review processes for 'possible matches', with secondary checks by compliance officers using more advanced investigative tools

- adverse-media monitoring that continuously scans global media for emerging political involvement or controversies.

When using screening software, practices should be aware that different providers may use different definitions to determine whether a customer is a PEP, and these may not fully align to regulatory requirements within Australia.

Verifying disclosed politically exposed persons

Particularly for practices with multiple offices, where there is a positive match or undisclosed status, you could consider one or more of the following, as appropriate:

- Apply matter-level controls (e.g. automatically pausing onboarding or freezing trust account activity pending review).
- Document whether a PEP classification triggers cross-border regulatory reporting obligations, including cross-border movement reports.
- Ensure decision-making is independent from fee-earners and follows a structured governance process.

Documenting and retaining politically exposed person results

Where a client is determined to be a PEP, medium and large practices can leverage the relevant CRM and document management systems and incorporate, where appropriate:

- version-controlled audit trails
- automated retention schedules aligned with legal/regulatory requirements, so that record-keeping obligations are met
- periodic internal audits of PEP checks so the central AML compliance team can ensure practice-wide consistency
- linked PEP records to ongoing monitoring so that changes in PEP status automatically update the client record.

Adverse media check processes

Much like PEP and sanctions screening searches, practices of medium or high complexity may consider it appropriate to utilise a screening software provider or database, rather than just internet searches for adverse media.

Further, practices of medium or high complexity, with their capabilities and resources, can consider incorporating one or more of the following measures into their processes, as appropriate:

- access to foreign-language media, translations and international news archives to capture risks across multiple jurisdictions

- integration of search results with sanctions, PEP and law enforcement databases for a holistic risk profile
- batch screening of multiple individuals at once (e.g. all beneficial owners, directors, trustees and authorised signatories)
- de-duplication and identity-resolution tools, reducing the risk of false matches with individuals of similar names
- internal compliance review, where specialists assess seriousness, credibility and whether allegations relate to the correct person
- cross-checking findings with corporate-registry tools (Orbis, Sayari) to verify links to implicated entities or high-risk sectors
- detailed relevance assessments, including whether the alleged conduct was profit-generating or linked to ML/TF typologies
- escalation pathways to risk committees, AMLCO or legal counsel for significant allegations
- automated documentation and audit trails via centralised CRM and document management systems.

Beneficial ownership processes

For practices of medium or high complexity, determining the beneficial ownership of clients is increasingly complicated and important the more complex/bigger the client is. Dealing with clients that may have a structure stretching across multiple jurisdictions with varying ML/TF and sanctions risk levels, and entity types within their structure, increases the lengths to which practices may be required to go to, to collect and/or verify information regarding their client.

Additional measures which can be considered by practices of medium or high complexity could include one or more of the following, as appropriate:

- for clients with large corporate structures, using corporate-intelligence platforms to verify the existence of all intermediaries in the structure
- applying risk analytics that highlight offshore entities, nominee directors/shareholders, opaque trust arrangements, private funds or special purpose vehicles (SPVs) and rapid changes in ownership
- when preparing ownership charts for offshore clients, requiring certified or externally validated ownership charts; and applying automated risk tools to flag high-risk jurisdictions, shell structures and nominee entities
- using analytical tools to detect unusual control chains or concentrations of power.

Dealing with a large number of entities within the client's structure may lead you to collect a high volume of information, documents and data, including from foreign or multiple certifiers, and this material may not be as reliable. Additional identification document collection may be pertinent as well, so you are not just relying on documents supplied. As a practice of medium or high complexity, you could consider investing additional efforts in obtaining reliable documentation yourself, including one or more of the following, as appropriate:

- retrieving official registry extracts directly from global databases, including for foreign companies (and, depending on the jurisdiction, trusts and partnerships) where possible to supplement client-supplied documents
- using automated workflows to ensure documents are current, complete and matched against authoritative sources
- using document fraud tools such as Persona or Resistant AI to authenticate corporate records and certificates
- conduct cross-jurisdiction verification, matching documents to independent foreign registries where possible
- applying compliance team review for inconsistencies, unusual amendments or non-standard structures.

Determining beneficial ownership within the criteria of AML/CTF legislation, including ownership percentage and existence of voting rights, could be carried out using resources, including one or more of the following, as appropriate:

- Use automated calculation tools to compute aggregated ownership across multiple layers.
- Validate calculations with corporate-registry data to ensure accuracy.
- Apply 'look-through' functionality for complex fund or trust structures where percentages are indirect.
- Deploy legal and compliance analysts to interpret:
 - control through voting agreements
 - de facto or shadow directors
 - protector roles in trusts
 - veto or casting-vote rights.

Where no ultimate beneficial owner can be identified, medium and large practices may consider adding steps into the process to resolve this, including:

- using detailed, structured workflows to document all steps and automatically escalate to compliance
- retaining a full audit trail to show all reasonable steps were taken, as required by AML/CTF Rules, rule 6-8, being:
 - the reporting entity has taken all reasonable steps to establish the identity of any beneficial owners of the customer but has been unable to do so, and
 - the reporting entity has recorded the steps taken and any difficulties encountered in attempting to establish the identity of any beneficial owners, and
 - the reporting entity has collected information about the identity of the individual who is the chief executive officer (or equivalent) of the customer, and
 - the reporting entity has verified, using reliable and independent data, such of that information as is appropriate to the ML/TF risk of the customer.

As a result of practice-collected documents, in addition to those supplied by the clients and their associated entities, you may also wish to consider ensuring your document management system has the necessary storage capabilities to keep detailed audit logs for easy inspection.

Annual report to the governing body process

Practices of medium or high complexity, which are likely to have larger governance structures, may be sourcing reportable information for their annual report to the governing body across teams/offices (possibly including overseas offices/affiliates). As such, additional/increased governance measures could be considered in the preparation and review of the report, including one or more of the following, as appropriate:

- more frequent check-in on report preparation where multiple departments or offices are involved
- earlier reminder set for preparation as opposed to a smaller practice
- review by multiple people (e.g. lead partner in each department/office) before AMLCO presents to the governing body
- implementation of dual-signoff (e.g. head of risk and managing partner) for greater governance rigour
- use of digital signatures and automated version control for auditability.

Reporting on results of the proposed action already implemented/taken is likely important for the governing body to form a view on the applicability across the entire practice or wherever appropriate.

Documenting this oversight will be of increased importance in more complex environments or corporate structures. Summarising key AML/CTF activities and events, training activities and SMRs/TTRs can leverage data analytics - for example, to:

- support recommendations (e.g. resourcing needs, staffing levels, transaction-monitoring capacity)
- present dashboards showing trends in ML/TF risk, system performance, training completion and reporting activity or obligation breach frequency, breaking items down by different elements (team/office/jurisdiction et cetera)
- identify high emerging global risks and regulatory updates relevant to larger, cross-border client bases
- show results from internal audit, specialist AML testing teams or external consultants.

Practices of medium or high complexity are likely to have an increased need to focus on linking overall effectiveness to the practice's ML/TF risk profile with its growth trajectory, as obligations and business goals are more complex. As such, the accuracy, completeness and credibility of these reports are critically important. We suggest, therefore, that these reports leverage the processes as described above.

Independent evaluation process

There are elements that may be beneficial for medium and large practices to consider when preparing for an independent evaluation, starting at the commissioning process. When considering who to appoint to review, you may wish to consider:

- sourcing and engaging an evaluator with specialist AML/CTF expertise that specifically includes cross-border experience or sector-specific knowledge
- undertaking enhanced independent assessment checks of the entity (or, if choosing to evaluate in-house, the team) conducting the review. You may wish to consider likelihood and consequences of any exposure to client legal privileged information.

Practices of medium or high complexity may also benefit from having more thorough testing of technology systems and controls, interviews or workshops, with multiple levels of personnel involved in AML/CTF activities. Consider providing yourself with the option to undertake these additional due diligence measures when you enter into any engagement discussions or formal agreements.

The review and remediation process will likely be wider scoped than that of a small practice. You may therefore wish to consider having remediation teams (IT security, CDD, compliance, HR et cetera), project managers, additional data sources and workflow software (potentially those with subscriptions) to develop and action your remediation plans.

You may also wish to test the effectiveness of the implemented updates, through using either internal audit or compliance testing teams or centralised AML teams. In doing so, you may consider applying data-driven validation, such as sampling onboarding cases, reviewing SMR timeliness or confirming that risk assessments reflect updated country/PEP/sanctions settings and, where necessary, re-engaging evaluators for supplementary testing.

Following the outcome of an independent evaluation, you may wish to issue practice-wide communications on new or updated policies which are not limited to new training requirements. As such, your practice may benefit from the ability to store all evaluation documentation in a secure, centralised repository with role-based access. Further, you may wish to consider sharing closing summaries with relevant leaders and practice groups to reinforce lessons learned.

Escalating matters to the AMLCO process

Additional note: AUSTRAC has made accommodations for medium or large practices, where an action, process or form does not mention a timeframe, to have extended 'as soon as practicable' times.

Escalation and trigger actions

For practices of medium or high complexity, we suggest that escalation and trigger actions focus on developing detailed processes that are clearly defined and work efficiently, notwithstanding the increased complexity as practices get larger - for example:

- **Broader and more granular escalation triggers:** Define escalation triggers beyond obvious red flags to include patterns, trends and cumulative risk indicators across matters, clients or practice groups.
- **Automated escalation flags:** Use AML systems to automatically flag escalation triggers (e.g. high-risk countries, PEP status, adverse media, unusual payment patterns) rather than relying solely on fee-earner judgement.
- **Tiered escalation pathways:** Introduce multiple escalation levels (e.g. matter team → compliance → AML committee → senior management) proportionate to risk severity.
- **Specialist compliance review:** Use route escalations to trained AML/CTF specialists or risk teams for independent assessment, reducing reliance on individual partners.
- **Clear decision ownership:** Define who can:
 - pause onboarding or transactions
 - require enhanced CDD
 - approve continuation of a matter
 - determine SMR/Unusual Activity Report (UAR) reporting obligations.

- **Matter-control mechanisms:** Enable practical controls such as:
 - temporary matter freezes
 - restrictions on trust-account use
 - conditional continuation subject to additional evidence.
- **Cross-matter visibility:** Centralise escalations so patterns across multiple matters or offices are visible, particularly for repeat clients or intermediaries.
- **Formal documentation standards:** Require escalation records to capture:
 - trigger identified
 - risk assessment undertaken
 - decision made and rationale
 - reporting outcome (if any).
- **Integration with reporting obligations:** Link escalation workflows directly to SMR/UAR decision-making and AUSTRAC reporting processes.
- **Governance oversight:** Provide periodic escalation summaries to senior management or risk committees to identify systemic issues or control gaps.
- **Consistent practice-wide application:** Embed escalation rules into workflows and training to ensure consistent handling across practice groups and offices.
- **Feedback and continuous improvement:** Use escalation data to refine risk assessments, update controls, and inform training priorities.

Forms

Where a practice of medium complexity considers it suitable to adapt the Starter Kit Risk Assessment, policy and/or processes to fit their size, complexity and operational activity, we suggest also ensuring that the forms within the Starter Kits are revised to reflect the changes made to its various components.

Where a practice of high complexity creates its own AML/CTF program (risk assessment, policies and processes), if considered appropriate, the forms within the Starter Kits may be leveraged and adapted to align to the policy and processes set out in their AML/CTF program.



Additional guidance

Reporting groups

Where two or more entities are connected, they may be considered to be a reporting group. Being a reporting group enables practices to share aspects of their AML/CTF framework and compliance arrangements, such as having a shared AML/CTF program.

Notwithstanding your broader business structure, if you do not want to be considered as part of a reporting group, you may need to opt out,⁸ and document that decision and process within your internal governance documents and procedures.

If you determine that it is appropriate for you to be part of a reporting group, you will need to determine the control structure of different businesses within your group. There must be a control structure where one or more persons within a group are controlled by another, in order for there to be a business group. A business group becomes a reporting group where one or more persons in the group provide designated services.

Although there are advantages to forming reporting groups, the legislation also imposes additional obligations on reporting groups, particularly relating to the lead entity. Reporting groups can also have implications for other businesses in the control structure that do not otherwise provide designated services.

It is recommended that practices seek legal advice to understand whether a reporting group is appropriate for their business.

Item 3 designated services

There is additional complexity provided by section 6, table 6, item 3, in which certain services may be provided to a customer who is not a 'client' in the traditional sense of client-solicitor relationship, such as in developer sales, commercial sales and dispute settlement funds without a court order.

The Law Society of New South Wales considers that, for these purposes, clients and customers are synonymous; therefore, where a person is not a client of a firm, they should not be treated as a customer for AML/CTF purposes.

⁸ See *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 (Cth)*, Part 2

Director Identification Numbers

Under rule 6-2(2)(i) of the AML/CTF Rules, where the customer is a body corporate, partnership or unincorporated association, entities are required to collect, for KYC purposes, 'the full name, and if applicable director identification number, of the individual, or each member of the group of individuals, with primary responsibility for the governance and executive decisions of the customer'. The purpose of this information is to establish, on reasonable grounds, the identity of the customer, as required by section 28(6)(a) of the AML/CTF Act.⁹

We are aware that some practices are applying a risk-based approach to their interpretation of this provision and require Director Identification Numbers (**DINs**) only where it is reasonable to do so based on their own risk assessment. For example, some practices require DINs only where the director is the ultimate beneficial owner and where the risk profile of the corporate warrants such collection (such as when it is not listed on the Australian Stock Exchange).

Rule 6-7 of the AML/CTF Rules provides that, where it has been established that the customer is a listed public company and is subject to public disclosure requirements, the reporting entity is taken to have established on reasonable grounds the identity of any beneficial owners of the customer.

Below are some examples to illustrate of how some practices are incorporating rule 6-7 of the AML/CTF Rules to their risk-based approach to the requirement at rule 6-2(2)(i) of the AML/CTF Rules:

- Where the client is low risk and is a listed public company or subsidiary, some practices are not collecting DINs.
- Where the client is low risk, and a private company with:
 - only one ultimate beneficial owner captured as the sole director or its managing director, only the DIN for this person is collected
 - five directors, with no individual owning 25% of more of the business, and a CEO who holds a directorship, only the DIN for the CEO is collected
 - three directors, one individual who is not a director owning 100%, and a CEO who is not a director, no DINs are collected.

- Where the client is medium risk, and a private company with:
 - seven directors, of which two are the board chair and vice chair and one is the CEO, the DINs for these three directors are collected.

The above examples show that whether a DIN is collected can be determined on a case-by-case basis, with regard to legislative requirements, the client's risk profile and the role(s) that the beneficial owner(s) hold.

Below are examples of how the practice may document its risk-based approach to DINs in its AML/CTF program:

- For low-risk customers, DINs are collected on those with key executive control or responsibility, where such persons are directors. Typically, these persons are C-suite (i.e. CEO, CFO, COO or equivalent). The rationale for this is:
 - C-suite represents the primary individuals with day-to-day operational control
 - this provides sufficient visibility of senior management who make executive decisions for low-risk relationships without being overly burdensome.
- For medium-risk or low-risk clients with complex structures, DINs are collected not only from executive management but also from key persons on the board, where they are directors. Examples include the chairperson, vice-chairperson or equivalent. The rationale for this is:
 - as risk or complexity increases, governance oversight becomes more relevant
 - the board chair reflects strategic control and governance influence above and beyond management.
- For high-risk customers, DINs are collected from executive management and all board members. The rationale for this is that full transparency is required of governance and control structures, commensurate with the customer's elevated risk profile.

If you adopt a risk-based approach to the requirement at rule 6-2(2)(i) of the AML/CTF Rules, we suggest that you document this approach, with reasons, in your AML/CTF policy and ensure it is aligned with your practice's risk assessment.

⁹ See *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 (Cth) r 6-2*; *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) s 28*.

Annexure - Risk Assessment Guide

How to use this risk assessment guide	41
Risk assessment	42
Risk ratings overview	42
Money laundering: Inherent risk, practice inherent risk, provisional residual/residual risk	44
Terrorism financing: Inherent risk, practice inherent risk, provisional residual/residual risk	48
Proliferation financing: Inherent risk, practice inherent risk, provisional residual/residual risk	50
Designated services: Inherent risk	52
Designated services: Profile	57
Designated services: Risk factors	58
Designated services: New and emerging technologies	63
Clients: Inherent risk	64
Clients: Profile	66
Clients: Risk factors	67
Delivery channels: Inherent risks	73
Delivery channels: Profile	74
Delivery channels: Risk factors	75
Countries: Risk assessment	76
Countries: Profile	76
Common money laundering and terrorism financing methods	77
Indicators of unusual or criminal behaviour	83
Client behaviour	83
Client profile	83
Unusual transactions and behaviours	85
Foreign jurisdiction indicators	88
Terrorism financing indicators	88
Proliferation financing indicators	88
Risk assessment sources	89

How to use this risk assessment guide

In preparing this template risk assessment guide, as we have done in preparing our [AML/CTF Implementation Guide: for sole practitioners and small practices](#), we have used the AML/CTF Program Legal Profession Program Starter Kit and Conveyancing Program Starter Kit (**Starter Kits**) prepared by AUSTRAC as a foundation, representing, as they do, AUSTRAC's view of what satisfactory compliance looks like. As such, this risk assessment heavily draws from the AUSTRAC Risk Assessments in the Starter Kits.

It is critical that each practice's risk assessment is tailored to reflect their business. While we have created a combined risk assessment for practices that provide both designated professional services and real property services, law practices that do not provide real property services should not use the sections we have included that are specific to conveyancing.

Each practice must consider whether the components and assumptions made in this risk assessment adequately reflect the size, nature and complexity of their business. It may require little amendment for those practices which, based on their suitability assessment, can largely rely on the AUSTRAC Starter Kits for compliance generally. However, this risk assessment guide may well be increasingly less appropriate to use as the size and complexity of the practice increases.

Suggestions on what a practice of high complexity may wish to consider as part of its risk assessment can be found in our AML/CTF Implementation Guide: for medium and large practices.

Please see our suitability assessment and the 'Terminology' section of this AML/CTF Implementation Guide: for medium and large practices for how we determine whether a practice should be considered small, medium or high complexity for the purposes of anti-money laundering and counter-terrorism financing (**AML/CTF**) compliance.

This risk assessment includes some additional elements and adjustments to the Starter Kits Risk Assessments - namely:

- practice-centric inherent risk
- provisional residual/residual risk
- templates to facilitate data collection to better understand money laundering (**ML**) and terrorism financing (**TF**) risk as it pertains to your practice.

These additional elements are inserted throughout this risk assessment and are provided by way of example for you to consider when developing your risk assessment to ensure that it appropriately reflects the size, nature and complexity of your practice.

Risk assessment

Your practice needs to have a ML, TF and proliferation financing (PF) risk assessment (together, **ML/TF risk assessment**).

A risk assessment will help your practice to identify and assess the ML/TF risks about the:

- services you provide
- clients and jurisdictions you deal with
- delivery channels you use to provide services.

These inform how you develop other processes in your AML/CTF program by ensuring that controls are proportionate to the level of risk you identify.

Under this system, a client will have either a:

- **high risk rating** - where at least **one high ML/TF risk factor** is present or the information you have otherwise warrants this rating - for example, indicators from this risk assessment suggest a client is not who they claim to be
- **medium risk rating** - where there are at least **two medium ML/TF risk factors** present or the information you have otherwise warrants this rating (moderate vulnerabilities to ML/TF present)
- **low risk rating** - a high or medium ML/TF risk rating is not warranted under the tests above.

You will also need to update your risk assessment to reflect changes in ML/TF risk (refer to 'Maintain our AML/CTF program policy' in the Starter Kits).

Risk ratings overview

The ratings and descriptions given below are used throughout this risk assessment. These ratings and description are taken from AUSTRAC's Risk Assessment in its Starter Kits, which we suggest remain applicable to practices of medium and high complexity.

Rating	Description
High	<p>Represents significant potential ML/TF impact, major damage or effect. Potentially involves serious ML, TF or proliferation activity. Requires strong and proactive controls. Controls include:</p> <ul style="list-style-type: none"> • enhanced customer due diligence (CDD) • gathering more information about the client at onboarding (simplified CDD cannot be used) • ongoing monitoring • more frequent periodic reviews (every year).
Medium	<p>Represents moderate potential ML/TF impact with a potential for adverse outcomes if controls do not appropriately manage and mitigate the risk. Controls include:</p> <ul style="list-style-type: none"> • gathering more information about the client at onboarding (simplified CDD cannot be used) • ongoing monitoring • periodic reviews every two years.
Low	<p>Represents minor or negligible potential ML/TF impact, with limited inherent exposure which can be easily contained. Can be managed effectively through standard policies, including simplified CDD on onboarding, monitoring and periodic reviews every three years.</p>

AUSTRAC has determined these ratings by considering different risk factors which may make your practice vulnerable to exploitation, meaning how easily criminals could exploit your designated services to launder money, finance terrorist acts or obtain weapons of mass destruction.

To do this, AUSTRAC has considered whether your designated service(s):

- could be exploited to conceal the identity or source of wealth or source of funds of a person
- could be easily accessed and used
- could allow value to be raised, moved or stored
- are known to be exploited by criminals.

To create its risk assessment, AUSTRAC expects the practice to understand the inherent risks and other risk factors associated with providing designated services.

This risk assessment replicates the list of inherent risks and risk factors known to be relevant to sectors which provide professional and conveyancing services as found in the Risk Assessments in the Starter Kits.

Inherent risk

An inherent ML/TF risk rating is an assessment of the level of ML, TF and PF risk that exists before any controls or mitigants are applied.

The rating identifies what the level of risk would be if no AML/CTF controls were in place and is used as the baseline against which the effectiveness of controls is assessed to determine the residual ML/TF risk.

The inherent risk boxes on the following pages, are identical to the inherent risk rows in the Starter Kits. We consider that, for small practices and practices of medium complexity that are able to adapt the Starter Kits (see our [suitability assessment tool](#)), the inherent risk table does not require amendment.

Law practice inherent risk

While the Starter Kits provide a good starting point to assess a practice's inherent ML/TF risk, further factors relevant to the practice should be considered.

We have included a law practice-centric inherent risk table in this risk assessment for you to consider.

Residual risk and provisional residual risk

A residual ML/TF risk rating is the level of ML and TF risk that remains after AML/CTF controls and mitigations are applied.

It reflects how effective an organisation is at reducing the inherent risk and represents the actual risk the organisation is exposed to on an ongoing basis.

At the time of initial implementation, legal practices are unlikely to have sufficient evidence to reliably assess residual risk.

We suggest, therefore, that you consider an assessment of your provisional residual risk and that this is the same as the practice inherent risk rating across all risk factors. This reflects that, while some controls may exist, they are not yet embedded or evidenced through operational data, quality assurance or control testing.


Once the AML/CTF program, including key controls, is embedded and operating effectively, this risk assessment can be updated to reassess residual risk against the inherent risks identified, based on demonstrated control effectiveness. Once reassessed, this should be renamed and evaluated as your practice's **residual risk**.

Eventually, practices of medium and high complexity will be expected by AUSTRAC to have considered their residual ML/TF risk, rather than their provisional residual risk. Our suggestion is that, even after controls are applied, your residual risk rating either will remain the same as your inherent risk rating or can be lowered.

We have included a provisional residual risk table in this risk assessment for you to consider. These provisional risks should be considered temporary until you have reassessed whether your controls and operating procedures are effective. After this reassessment (say, after 12 months), this risk assessment template should refer to 'residual risks' instead of 'provisional residual risks'.

Please be aware that the included examples are only to give you an idea of the types of controls your practice may wish to apply. Please consider the table and examples in the context of your business and consider which risk rating would be most appropriate to your practice.

Money laundering: Inherent risk, practice inherent risk, provisional residual/residual risk



The 2024 ML national risk assessment assesses ML vulnerabilities for conveyancers, legal professionals, and trust and company service providers. As the vulnerabilities for both groups apply to the designated services in this risk assessment, inherent risks for both groups have been provided here.

Australia’s 2024 ML national risk assessment assesses:

- legal professionals as posing a high and stable vulnerability to ML
- trust and company service providers as posing a medium and stable vulnerability to ML.

It is expected that:

- legal professionals will continue to pose a high vulnerability to ML, providing access to a range of critical products, services and structures desired by criminals
- trust and company service providers will continue to pose a medium vulnerability to ML because their services and expertise are desired by criminals.

Conveyancing

Australia is one of the most attractive real estate markets globally. Australia’s 2024 ML national risk assessment assessed real estate as having a very high and stable ML vulnerability. Criminals can exploit real estate at all stages of the ML cycle.

It is expected that real estate will continue to pose a high ML vulnerability driven largely by the market’s stability and high value.

Between July 2020 and June 2023, law enforcement authorities seized over \$62 million in real estate as part of proceeds of crime investigations. Notably, the sector also attracts significant foreign criminal investments looking to legitimise illicit funds.

Inherent risk rating

Risk rating	Rationale
High	Real estate is highly vulnerable to exploitation by criminals when laundering money obtained from serious crimes. This means that conveyancers are vulnerable to exploitation by criminals who need help purchasing or selling properties with the proceeds of crime.

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert ‘High’, ‘Medium’ or ‘Low’ depending on your assessment outcome.	<p><i>You may wish to consider the following qualitative metrics to evaluate your practice’s inherent risk. Ensure the reasoning is adequately tailored to your circumstances.</i></p> <p>High: The practice provides conveyancing services involving complex or high-value property transactions, non-resident or corporate purchasers, trusts or layered ownership structures – particularly where transactions involve cross-border elements, use of third-party funding or arrangements that confer financial control – and where the effectiveness of AML/CTF controls has not yet been demonstrated.</p> <p>Medium: Conveyancing services are provided in a conventional and controlled manner (e.g. domestic residential transactions), but AML/CTF controls are newly implemented or not yet evidenced, creating uncertainty around the consistent identification of beneficial ownership, source-of-funds and third-party risk indicators.</p> <p>Low: Conveyancing exposure is limited and tightly constrained, transactions are low-complexity and domestic, clients are well understood, and strong gatekeeping and verification controls demonstrably operate across client onboarding and transaction execution.</p>

Provisional residual/residual risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</p> <p>High: Despite effective controls, the inherent risk profile of the services remains elevated and cannot be sufficiently reduced through mitigation alone; and the effectiveness of AML/CTF controls has not yet been demonstrated.</p> <p>Medium: Controls are operating effectively and consistently, but the nature of services still presents an irreducible level of ML exposure.</p> <p>Low: Strong, mature controls materially reduce exposure arising from funds handling, transactions and structuring, leaving only limited residual vulnerability.</p>

Legal professionals

The involvement of legal professionals as facilitators for ML is recognised both domestically and internationally as an enduring vulnerability. Australian Government agencies report the exploitation of legal professionals as a key component of the criminal practice model.

Legal professionals conduct a range of services that can be used to benefit criminals in the ML process, including:

- operating trust and other accounts to deposit, hold and disburse client funds
- facilitating real estate, business and asset transactions, including purchase, sale, transfer of ownership and financing arrangements
- establishing and administering complex domestic and offshore legal structures.

Secondary reporting by Australian banks demonstrates that legal professionals handle large volumes of cash and facilitate a large volume of incoming and outgoing international funds transfers. This increases vulnerability to ML by both complicit and non-complicit legal professionals. Vulnerability is increased further when a client uses a third party to help obscure beneficial ownership.

Inherent risk rating

Risk rating	Rationale
High	The legal sector is highly vulnerable to exploitation by criminals seeking advice on ways to launder money and services which may make it easier to do so.

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>You may wish to consider the following qualitative metrics to evaluate your practice's inherent risk. Ensure the reasoning is adequately tailored to your circumstances.</p> <p>High: The practice assist clients in the planning or execution of the creation or restructuring a body corporate or legal arrangement. Establishing and administering complex domestic and offshore legal structures, particularly where complexity, cross-border elements or financial control is present - and where control effectiveness is not yet demonstrated.</p> <p>Medium: Medium provisional residual risk is appropriate where the planning or execution of the creation or restructuring of a body corporate or legal arrangement are provided in a controlled, conventional way, but controls are still new / not yet evidenced, creating uncertainty about consistent identification of complex ownership and source-of-funds risks.</p> <p>Low: ML/TF/PF exposure is minimal and tightly constrained; and the practice's activities are limited to low-risk entity maintenance with strong gatekeeping.</p>

Provisional residual/residual risk rating

Risk rating	Rationale
<p>Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.</p>	<p><i>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</i></p> <p>High: Despite effective controls, the inherent risk profile of the services remains elevated and cannot be sufficiently reduced through mitigation alone; and the effectiveness of AML/CTF controls has not yet been demonstrated.</p> <p>Medium: Controls are operating effectively and consistently, but the nature of services still presents an irreducible level of ML exposure.</p> <p>Low: Strong, mature controls materially reduce exposure arising from funds handling, transactions and structuring, leaving only limited residual vulnerability.</p>

Trust and company service providers

Trust and company services providers (TCSPs) are often exploited by criminals due to their expertise in wealth protection and the administration of trust and company structures. Whether they are complicit or not, they create further distance between a criminal and their illicit proceeds.

Although companies can generally be set up without a TCSP, the creation of more complex legal structures, including trusts, often requires the expertise of TCSPs. These structures are highly attractive to criminals, as they:

- make it hard to determine beneficial ownership
- conceal the origin and purpose of financial transactions
- move significant volumes of funds domestically and offshore.

As more sophisticated criminals consistently exploit these mechanisms, TCSPs remain vulnerable to enabling ML.

Many of the established methodologies used to conceal wealth, circumvent financial obligations and ultimately launder money are enhanced by a TCSP. Key methodologies include:

- establishing corporate structures in jurisdictions with lax regulatory and legislative frameworks, including secrecy jurisdictions
- creating complex chains of companies across multiple jurisdictions
- appointing dummy directors and shareholders
- acting as trustees on behalf of a client
- providing loans secured by client funds.

Inherent risk rating

Risk rating	Rationale
<p>Medium</p>	<p>Trust and company service providers are vulnerable to ML due to the services they provide and their attractiveness to criminals.</p>

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<i>You may wish to consider the following qualitative metrics to evaluate your practice's inherent risk. Ensure the reasoning is adequately tailored to your circumstances.</i>
	High: The practice provides TCSP services that enable entity/trust structuring and administration, particularly where complexity, cross-border elements or financial control is present – and where control effectiveness is not yet demonstrated.
	Medium: TCSP services are provided in a controlled, conventional way, but controls are still new / not yet evidenced, creating uncertainty about consistent identification of complex ownership and source-of-funds risks.
	Low: TCSP exposure is minimal and tightly constrained; and the practice's activities are limited to low-risk entity maintenance with strong gatekeeping.

Provisional residual/residual risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<i>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</i>
	High: Despite effective controls, the inherent risk profile of the services remains elevated and cannot be sufficiently reduced through mitigation alone; and the effectiveness of AML/CTF controls has not yet been demonstrated.
	Medium: Controls are operating effectively and consistently, but the nature of services still presents an irreducible level of ML exposure.
	Low: Strong, mature controls materially reduce exposure arising from funds handling, transactions and structuring, leaving only limited residual vulnerability.

Terrorism financing: Inherent risk, practice inherent risk, provisional residual/residual risk

Conveyancing

The real estate sector is more commonly used to launder money rather than fund terrorism. The 2024 TF national risk assessment does not describe any vulnerabilities specifically associated with real estate and TF.

There is a lack of available information from international sources to suggest specific vulnerabilities faced by sectors which deal with real estate.

Inherent risk rating

Risk rating	Rationale
Low	The use of real estate to facilitate TF is believed to be limited.

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>You may wish to consider the following qualitative metrics to evaluate your practice's inherent risk. Ensure the reasoning is adequately tailored to your circumstances.</p> <p>High: The charity / non-profit organisation (NPO) exposure creates heightened TF vulnerability, and control effectiveness cannot yet be demonstrated.</p> <p>Medium: Charity/NPO work presents recognised TF risk drivers, but the extent of exposure is moderated; and controls are expected to be effective once embedded.</p> <p>Low: Charity/NPO exposure is clearly limited to low-risk, domestic activities; and the absence of control evidence is unlikely to materially increase TF exposure.</p>

Provisional residual/residual risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</p> <p>High: The nature of the NPO/charity work creates persistent TF exposure that remains elevated even after controls due to operating footprint, funding channels, counterparties or governance risk.</p> <p>Medium: The firm provides charity/NPO services with some TF risk drivers, such as crossborder links or higher risk operating environments, but controls effectively reduce likelihood while leaving some unavoidable exposure.</p> <p>Low: NPO/charity work is limited to low-risk domestic organisations with transparent governance and funding; and the practice has strong controls that reduce TF exposure to minimal levels.</p>

Legal professionals

Legal professionals are more commonly used to launder money rather than fund terrorism. However, those services related to trust and company formation and the handling of client funds are internationally recognised as being attractive to those seeking to distance themselves from fundraising towards terrorism.

Most TF cases involve simple unsophisticated methods such as low-value client-to-client transfers. More complex cases - for example, those involving efforts to obscure beneficial ownership using legitimate or shell companies or third-country transfers - are rare. In these instances, it is often difficult to definitively link the transaction to TF.

Legal professionals may be involved in either:

- setting up charities or other NPOs
- providing other services to the charity.

Registered charities and legitimate NPOs provide an attractive channel for TF. This is because donations can be solicited from many individuals, witting and unwitting, and diverted for illicit purposes.

Inherent risk rating

Risk rating	Rationale
Low	The use of legal professionals to facilitate TF is uncommon but can occur when assisting exploited NPOs or providing trust and company services.

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>You may wish to consider the following qualitative metrics to evaluate your practice's inherent risk. Ensure the reasoning is adequately tailored to your circumstances.</p> <p>High: The practice's conveyancing work presents heightened TF vulnerability, including transactions involving higher risk jurisdictions, non-resident or unknown counterparties, use of intermediaries or third-party funding, or unusual transactional complexity – and where the effectiveness of TF-relevant controls has not yet been demonstrated.</p> <p>Medium: Conveyancing services present recognised TF risk drivers (e.g. occasional exposure to foreign purchasers, trusts or complex funding arrangements), but the extent of exposure is moderated, and controls are expected to be effective once fully embedded and operating consistently.</p> <p>Low: Conveyancing exposure is clearly limited to low-risk, domestic property transactions, client and funding profiles are well understood, and the absence of fully evidenced controls is unlikely to materially increase the practice's exposure to TF risk.</p>

Provisional residual/residual risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</p> <p>High: The practice's conveyancing activities continue to present heightened TF vulnerability after controls are applied – including ongoing exposure to higher risk jurisdictions, nonresident or opaque counterparties, complex ownership structures, or atypical funding arrangements – and where implemented controls do not sufficiently mitigate TF risk in practice.</p> <p>Medium: Conveyancing services involve recognised TF risk drivers, but these are partially mitigated through operationally effective controls, resulting in some residual exposure that is not considered material or systemic.</p> <p>Low: Conveyancing activities are limited to low-risk, domestic transactions, client and funding arrangements are transparent and well understood, and operating controls demonstrably reduce TF risk to a low and manageable level.</p>

Proliferation financing: Inherent risk, practice inherent risk, provisional residual/residual risk

Conveyancing

The 2024 PF national risk assessment provides little evidence of real estate playing a role in facilitating PF. International reports show that real estate can be used in PF, although evidence of sector-wide vulnerability is limited.

Known international cases involve construction, property development and the sale or leasing of commercial or residential properties.

Inherent risk rating

Risk rating	Rationale
Low	Limited evidence exists suggesting real estate is being used in PF.

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p><i>You may wish to consider the following qualitative metrics to evaluate your practice's inherent risk. Ensure the reasoning is adequately tailored to your circumstances.</i></p> <p>High: The practice's conveyancing work gives rise to heightened PF vulnerability, including transactions involving higher risk or sanctioned jurisdictions, opaque or nonresident purchasers, complex ownership or trust structures, or the use of intermediaries or third-party funding – and where the effectiveness of PF-relevant controls (including sanctions screening and beneficial ownership verification) has not yet been demonstrated.</p> <p>Medium: Conveyancing services present recognised PF risk drivers (such as occasional foreign purchasers, trusts or links to higher risk jurisdictions), but the extent of exposure is moderated; and controls are expected to be effective once fully implemented and operating consistently.</p>

Practice inherent risk rating (continued)

Risk rating	Rationale
	Low: Appropriate only where conveyancing exposure is clearly limited to low-risk, domestic transactions, client and funding arrangements are straightforward and transparent, and the lack of fully evidenced controls is unlikely to materially increase the practice's exposure to PF risk.

Provisional residual/residual risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p><i>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</i></p> <p>High: The practice's conveyancing activities continue to present elevated PF vulnerability after controls are applied – including exposure to higher risk jurisdictions subject to sanctions or export controls; use of complex ownership or trust structures, opaque purchasers or funding sources; or involvement of intermediaries – and where operating controls do not sufficiently mitigate the risk of misuse of property transactions to support proliferation-related activity.</p> <p>Medium: Conveyancing services involve recognised PF risk drivers (e.g. occasional transactions linked to foreign entities, trusts, or higher risk jurisdictions), but these risks are largely mitigated through effective sanctions screening, beneficial ownership checks and transaction oversight, leaving some residual exposure that is not considered serious or systemic.</p> <p>Low: Conveyancing activities are limited to low-risk, domestic transactions, counterparties and funding sources are transparent and well understood, sanctions and PF-relevant controls operate effectively, and residual PF risk is reduced to a low and manageable level.</p>

Legal professionals

The 2024 PF national risk assessment found that criminals seeking to finance the proliferation of weapons of mass destruction exploit legal professionals the same way as money launderers. They do this by using legal professionals to:

- establish complex corporate structures, such as shell and front companies
- create banking arrangements to evade sanctions and generate revenue for proliferation activities.

While the extent of criminal exploitation for these purposes is likely low, legal professionals remain exposed to the risk of being taken advantage of by criminals for PF.

Inherent risk rating

Risk rating	Rationale
Medium	Legal professionals are vulnerable to exploitation by criminals engaging in proliferation activities when helping create corporate structures which distance them from illicit funds.

The Law Society of NSW has added the below additional types of risk for practices of medium complexity to consider and adapt as appropriate.

Practice inherent risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p><i>You may wish to consider the following qualitative metrics to evaluate your practice's inherent risk. Ensure the reasoning is adequately tailored to your circumstances:</i></p> <p>High: Legal professionals regularly assist in creating or administering complex or offshore corporate structures that could be used to distance proliferators from funds, assets or procurement activity; and control effectiveness is not yet demonstrated.</p> <p>Medium: The legal professional assists with entity formation or structuring that introduces some separation between clients and funds, but complexity and jurisdictional exposure are limited, and controls are still new / not yet evidenced, creating uncertainty.</p>

Practice inherent risk rating (continued)

Risk rating	Rationale
	Low: The legal professional's involvement in corporate structuring is minimal, domestic and transparent, with little opportunity to distance clients from funds or ownership, and the absence of control evidence is unlikely to materially increase TF exposure.

Provisional residual/residual risk rating

Risk rating	Rationale
Please insert 'High', 'Medium' or 'Low' depending on your assessment outcome.	<p>We suggest including an overview of the controls that justify any variation reduction or rationale for keeping the inherent risk rating for residual risk. To do this, you may wish to evaluate your provisional residual risk or residual risk using the following example qualitative metrics:</p> <p>High: Legal professional's involvement in corporate structuring is limited, transparent and domestic; and controls demonstrably mitigate the risk of structures being misused to distance clients from illicit activity.</p> <p>Medium: Legal professional assists with corporate structuring that introduces some separation between individuals and assets or funds, but controls reduce the likelihood of misuse to an acceptable level.</p> <p>Low: Legal professional's involvement in corporate structuring is limited, transparent and domestic; and controls demonstrably mitigate the risk of structures being misused to distance clients from illicit activity.</p>

Designated services: Inherent risk



This table supports Step 1 in Part 1 of the Customise the program starter kit guide. Refer to the Customise guide for full instructions to assist you in completing your table.

Designated service	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide this service?
<p>Conveyancing services</p> <p>Helping a person with planning or executing a transaction to buy, sell or transfer real estate - this includes acting on someone's behalf.</p> <p>(Item 1, table 6 of the AML/CTF Act)</p>	<p>Conveyancing involves helping in the planning or execution of the sale, purchase or transfer of real estate.</p> <p>The conveyancer, settlement agent or property solicitor typically undertakes work to plan, execute or give effect to the transfer of real estate from one person to another.</p>	<p>Conveyancing services are vulnerable to exploitation, as they can be used by criminals to transfer property titles to individuals or entities who would not attract the attention of law enforcement.</p> <p>Criminals may use conveyancers to:</p> <ul style="list-style-type: none"> • help legitimise a property transaction involving criminal proceeds • seek advice on creating distance between the criminal and their property. 	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

Designated service	Description	Vulnerabilities to ML/TF risk	Risk appetite – would you provide this service?
<p>Other professional services</p> <p>Assisting a person in the planning or execution of a transaction to buy, sell or transfer a body corporate or legal arrangement - this includes acting on their behalf in a transaction.</p> <p>This only applies where the sale, purchase or transfer relates to a controlling interest in the body corporate or legal arrangement.</p> <p>(Item 2, table 6 of the AML/CTF Act)</p>	<p>Legal professionals are routinely asked to help with transactions to buy, sell or transfer a body corporate or legal arrangement. This typically involves:</p> <ul style="list-style-type: none"> • preparing and reviewing contracts • conducting due diligence • obtaining relevant government approvals • preparing financial settlements or documents. <p>This does not include transactions following, or resulting from, an order of a court or tribunal.</p> <p>A body corporate can include a person, association or group of persons incorporated into a corporation.</p> <p>A legal arrangement can include a structured agreement or setup recognised by law. It often involves trusts, contracts or similar frameworks that define rights, duties or relationships between parties.</p>	<p>Criminals can exploit both body corporates, such as companies; and legal arrangements, such as trusts. This can include:</p> <ul style="list-style-type: none"> • using complex ownership structures or rapid ownership transfers to obscure ownership • as vehicles to conceal beneficiaries and source of funds • to assist in integrating illicit funds into the legitimate economy (e.g. laundering of proceeds of crime through a cash-intensive business) • to move proceeds of crime overseas. 	<input type="checkbox"/> Yes <input type="checkbox"/> No
<p>Other professional services</p> <p>Receiving, holding, controlling or managing a person's money, accounts, securities or securities accounts, virtual assets or other property as part of assisting the person in the planning or execution of a transaction.</p> <p>This includes acting for or on behalf of a person in a transaction.</p> <p>(Item 3, table 6 of the AML/CTF Act)</p>	<p>This may include:</p> <ul style="list-style-type: none"> • managing sale proceeds or purchase funds for a client on escrow • money or property being held by a legal professional prior to being settled as trust property on the creation of an express trust • having authority to make payments over a client's bank or securities account on behalf of the client, including under a power of attorney. <p>Legal professionals operating trust accounts in the absence of any other designated services are not covered.</p>	<p>Criminals can exploit legal professionals in several ways, including to:</p> <ul style="list-style-type: none"> • hide behind their legal professional by using them to manage illegally gained funds for purchases and expenses on their behalf • integrate illegal funds into the legitimate economy • store value from criminal proceeds • obscure the origin of the money, accounts and assets through a complex transaction. 	<input type="checkbox"/> Yes <input type="checkbox"/> No

Designated service	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide this service?
<p>Other professional services</p> <p>Assisting in organising, planning or executing a transaction for equity or debt financing relating to a body corporate or legal arrangement.</p> <p>This includes acting on the person’s behalf in a transaction.</p> <p>(Item 4, table 6 of the AML/CTF Act)</p>	<p>Helping with equity or debt financing can typically include:</p> <ul style="list-style-type: none"> • supporting a business to raise capital or debt through various methods, such as initial public offerings, venture capital, share purchase plans, debt financing, bonds, asset financing, loans and debentures • services directly advancing a transaction to secure equity and debt financing for the company relating to negotiating, structuring and executing a financing deal or the drafting of debt or equity finance documents. 	<p>Criminals can exploit legal professionals for equity and debt financing in several ways, including using them to:</p> <ul style="list-style-type: none"> • manage illegally gained funds • purchase equity in a business • assist in complex debt financing applications (often commingling them with legitimately sourced funds to pay back the debt) • manipulate the value of shares to quickly launder money • create loan-back schemes to launder money. 	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Other professional services</p> <p>Selling or transferring a shelf company.</p> <p>(Item 5, table 6 of the AML/CTF Act)</p>	<p>This involves establishing, selling or transferring a previously established shelf company.</p>	<p>Criminals often prefer purchasing shelf companies as opposed to forming new companies, particularly where the registration date is earlier than when it was used for any purpose (legitimate or illegitimate).</p> <p>Shelf companies are commonly used by criminals in the same way as ‘shell companies’, which are companies with no real assets or business operations. However, shelf companies registered in the past may seem more legitimate than a newly formed company when trying to open a bank account or send proceeds of crime overseas.</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

Designated service	Description	Vulnerabilities to ML/TF risk	Risk appetite – would you provide this service?
<p>Other professional services</p> <p>Assisting in planning or executing in the creation or restructuring of a body corporate or legal arrangement.</p> <p>This includes acting on the person's behalf.</p> <p>(Item 6, table 6 of the AML/CTF Act)</p>	<p>This routinely involves:</p> <ul style="list-style-type: none"> • supporting merger and acquisitions by drafting, reviewing and negotiating preparatory documents, including partnership agreements, company constitutions, trust deeds or documents • registering applications and forms with the Australian Securities and Investments Commission (ASIC) – for example, to register a company or a business name • obtaining Foreign Investment Review Board approvals and Australian Stock Exchange and ASIC waivers. 	<p>Criminals can exploit both body corporates and legal arrangements in several ways, including:</p> <ul style="list-style-type: none"> • by using complex ownership structures to obscure ownership • as vehicles to conceal beneficiaries and source of funds • to integrate illegal funds into the legitimate economy • by using loan-back schemes to launder money. 	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Other professional services</p> <p>Acting as a director or secretary of a company, a power of attorney of a body corporate or legal arrangement, a partner in a partnership, a trustee of an express trust, or any other functionally equivalent position on behalf of a person.</p> <p>This includes arranging for another person to act in these roles.</p> <p>(Item 7, table 6 of the AML/CTF Act)</p>	<p>This typically includes:</p> <ul style="list-style-type: none"> • drafting documents • identifying or introducing people to act in the type of role specified • performing tasks to make the relevant appointments or authorisations on behalf of a client. <p>This does not include persons acting in either a:</p> <ul style="list-style-type: none"> • fiduciary capacity because of an order of a court or tribunal • trustee of a regulated debtor's estate due to bankruptcy. 	<p>Criminals can exploit legal professionals acting on behalf of a person in several ways, including to:</p> <ul style="list-style-type: none"> • obscure control behind those acting on their behalf • integrate illegal funds into the economy by moving the funds through additional entities to obscure the origin. 	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

Designated service	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide this service?
<p>Other professional services</p> <p>Acting as a nominee shareholder of a body corporate or legal arrangement on behalf of a person. This includes arranging for another person to act in these roles.</p> <p>(Item 8, table 6 of the AML/CTF Act)</p>	<p>This typically includes:</p> <ul style="list-style-type: none"> • drafting or amending documents to authorise a 'nominee shareholder' • identifying or introducing a person to act as a 'nominee shareholder' on behalf of a nominator. 	<p>Criminals can exploit legal professionals acting as a nominee shareholder in several ways, including to:</p> <ul style="list-style-type: none"> • obscure ownership behind the nominees • integrate illegal funds into the economy by moving the funds through additional entities to obscure the origin. 	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Other professional services</p> <p>Providing a registered office address or principal place of business address of a body corporate or legal arrangement.</p> <p>(Item 9 of table 6 of the AML/CTF Act)</p>	<p>This is typically when a practice provides a body corporate with a registered office address or principal place of business address instead of the address the person operates their business from.</p>	<p>Criminals can use this service to appear legitimate and make it seem like the business is operating in a different location from where it is located. This allows them to distance themselves from illicit activities, making it difficult to identify beneficial ownership.</p> <p>The service can facilitate the use of complex legal structures with ties to overseas jurisdictions. This could help criminals launder illicit funds to high-risk countries for ML/TF use.</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

The Law Society of NSW has created the below template which you may wish to use to collect relevant data to assist in forming your practice's risk profile.

Designated services: Profile

During the last [12] months the following designated services have been provided to clients.

Designated service	Number of matters that involved the provision of this designated service
Item 1, table 6 of the AML/CTF Act: Helping a person with planning or executing a transaction to buy, sell or transfer real estate. This includes acting on someone's behalf.	
Item 2, table 6 of the AML/CTF Act: Assisting a person in the planning or execution of a transaction to buy, sell or transfer a body corporate or legal arrangement.	
Item 3, table 6 of the AML/CTF Act: Receiving, holding, controlling or managing a person's money, accounts, securities or securities accounts, virtual assets, or other property as part of assisting the person in the planning or execution of a transaction.	
Item 4, table 6 of the AML/CTF Act: Assisting in organising, planning or executing a transaction for equity or debt financing relating to a body corporate or legal arrangement.	
Item 5, table 6 of the AML/CTF Act: Selling or transferring a shelf company.	
Item 6, table 6 of the AML/CTF Act: Assisting in planning or executing of the creation or restructuring of a body corporate or legal arrangement.	
Item 7, table 6 of the AML/CTF Act: Acting as a director or secretary of a company or as a power of attorney of a body corporate or legal arrangement.	
Item 8, table 6 of the AML/CTF Act: Acting as a nominee shareholder of a body corporate or legal arrangement on behalf of a person.	
Item 9, table 6 of the AML/CTF Act: Providing a registered office address or principal place of business address of a body corporate or legal arrangement.	

Designated services: Risk factors



This table supports Step 2 in Part 1 of the Customise the program starter kit guide.
 Refer to the Customise guide for full instructions to assist you in completing your table.

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Conveyancing services</p> <p>High-value and unfinanced transactions</p>	<p>Sales or purchases of property which:</p> <ul style="list-style-type: none"> involve transaction(s) valued at \$1.5 million or more, and do not involve any mortgage or other loan from a lending institution (such as a bank or non-bank lender). 	<p>High-value real estate markets are attractive to people seeking to launder illicit funds gained from criminal activity, as they can launder more funds in one transaction. This has been seen by law enforcement with the number of high-value properties seized in proceeds of crime investigations.</p> <p>Where the average transaction in a market is higher, criminals can place greater amounts of illicit funds in a property without drawing attention.</p> <p>Lenders perform in-depth due diligence on clients and properties before providing funds as part of a mortgage. Where a property is bought without a mortgage, there is a significant difference in the amount of scrutiny on the buyer.</p>	<p>Medium</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Conveyancing services</p> <p>High-value physical currency transactions</p>	<p>Property that is purchased using high-value physical currency transaction(s) (e.g. in Australian dollar notes and coins or a foreign currency equivalent) valued at \$50,000 or more.</p>	<p>Physical currency is anonymous and hard to trace, making it difficult to verify the source of funds. In Australia, it is one of the most restrained, forfeited or frozen asset types in criminal asset confiscation matters. It is exploited for its accessibility, widespread acceptance and availability. Its use also requires minimal skills, knowledge and expertise.</p> <p>Criminals looking to purchase real estate with large amounts of cash may give the cash to a conveyancer or deposit it into their statutory trust account directly.</p>	High	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	
<p>Conveyancing services</p> <p>Virtual assets</p>	<p>Any payment or sale involving a virtual asset (e.g. digital currencies such as Bitcoin or Ethereum).</p> <p>Virtual asset payments are highly unusual in the real estate sector, but some sellers do accept virtual assets as payment.</p>	<p>Criminals are attracted to virtual assets because they:</p> <ul style="list-style-type: none"> • offer speed and global reach - transactions are almost instant and irreversible, making it challenging to detect and stop illicit use • allow movement of value with low visibility of the identity of the individual who owns or controls it. <p>After someone exchanges fiat currency (this is government-issued currency, such as Australian dollars) for virtual assets, their payments completely bypass oversight from financial institutions.</p>	High	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Conveyancing services</p> <p>Unusual service requests</p>	<p>Any request for designated services which:</p> <ul style="list-style-type: none"> • has no apparent economic or legal purpose • would involve unusually complex or large transactions • would involve an unusual pattern of transactions. 	<p>Clients who seek unusual services from your practice are more likely to seek services to disguise or facilitate ML/TF or criminal activity. Criminals often act and transact in ways which may appear illogical or uneconomical to other people - for example, where a client asks for the title of the residential property they are purchasing to be held by an unusually complex corporate structure.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	
<p>Other professional services</p> <p>High-value transactions</p>	<p>Legal professionals can facilitate or assist with high-value transactions across a range of business areas, including mergers and acquisitions or obtaining complex financing.</p> <p>They are also involved in legal aspects of large asset purchases, investments and financial markets.</p>	<p>Legal professionals often facilitate high-value transactions on behalf of their clients, making them attractive for laundering significant amounts of illicit funds without drawing attention from law enforcement.</p> <p>Some transactions can occur very quickly, including those in commercial matters. This speed of transactions, along with their high value, can allow criminals to move significant amounts of illicit funds in a single transaction.</p>	<p>Medium</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Other professional services</p> <p>Unusual physical transactions</p>	<p>Any physical currency transactions (e.g. in Australian currency notes and coins or a foreign currency equivalent) that are unusual in the circumstances.</p> <p>Whether a physical currency transaction is unusual will often depend on:</p> <ul style="list-style-type: none"> its size and complexity whether it has an apparent economic or lawful purpose whether it is consistent with what you know about the client and their industry. 	<p>Physical currency is anonymous and hard to trace, making it difficult to verify the source of funds. In Australia, it is one of the most restrained, forfeited or frozen asset types in criminal asset confiscation matters. It is exploited for its accessibility, widespread acceptance and availability. Its use also requires minimal skills, knowledge and expertise.</p> <p>Criminals may give the cash directly to your practice or deposit it into your statutory trust account directly.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	
<p>Other professional services</p> <p>Unusual virtual asset transactions</p>	<p>Any transaction involving a virtual asset (e.g. digital currencies such as Bitcoin or Ethereum).</p> <p>Whether a virtual asset transaction is unusual will often depend on:</p> <ul style="list-style-type: none"> whether the use of virtual assets is common in the circumstances whether there is any apparent economic or lawful purpose for using virtual assets over fiat currency (this is government-issued currency, such as Australian dollars) whether it is consistent with what you know about the client and their industry. 	<p>Criminals are attracted to virtual assets because they:</p> <ul style="list-style-type: none"> offer speed and global reach - transactions are almost instant and irreversible, making it challenging to detect and stop illicit use allow movement of value with low visibility of the identity of the individual who owns or controls it. <p>After someone exchanges fiat currency for virtual assets, their payments completely bypass oversight from financial institutions.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Other professional services</p> <p>Effective anonymity</p>	<p>Legal professionals can help their clients create legal structures which make it hard to determine who owns or controls their property or money. This often involves creating layers of companies, trusts and other entities between the individual and the property or money they are trying to hide.</p> <p>Note that there are many legitimate uses of complex legal structures. Whether this is unusual depends on whether the requested services could be used for an illegitimate purpose.</p> <p>If you can clearly identify all individuals who control and benefit from the trust, this reduces and/or removes anonymity.</p>	<p>Complex legal structures and arrangements are attractive to criminals, as they can provide anonymity and legitimacy when seeking to obscure their activities.</p> <p>Where a person's ownership and control structure is highly complex or unusual, it can be very difficult to analyse each layer and identify the beneficial owners. This makes the beneficial ownership 'effectively anonymous'.</p> <p>Although there are legitimate reasons to use complex ownership and control structures, these structures are often used by criminals to distance themselves from transactions and activity which may attract attention from law enforcement.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	
<p>Unusual service requests</p>	<p>Any request for designated services which:</p> <ul style="list-style-type: none"> • has no apparent economic or legal purpose • would involve unusually complex or large transactions • would involve an unusual pattern of transactions. 	<p>Clients who seek unusual services from your practice are more likely to be seeking services to disguise or facilitate ML/TF or criminal activity. Criminals often act and transact in ways which may appear illogical or uneconomical to other people - for example, where a client is willing to pay significantly higher fees if the service is done quickly.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Designated services: New and emerging technologies



This table supports Step 1 in Part 1 of the Customise the program starter kit guide.

Refer to the Customise guide for full instructions to assist you in completing your table.

New and emerging technologies may affect the ML/TF risks associated with services you provide to clients and the channels you use when providing services. Some examples of technologies which may be vulnerable to exploitation by clients are provided below.

Kind of technology	Description	Why it creates ML/TF vulnerabilities
Artificial intelligence (AI)	<p>Legal professionals are often required to conduct a high volume of enquiries using various software programs and technological options, including AI. Additionally, virtual assistants and chatbots powered by AI are also being used to engage first-time clients.</p> <p>AI and machine learning are being adopted by practices to:</p> <ul style="list-style-type: none"> • enhance data analysis and decision-making • automate repetitive work through robotic process automation. <p>AI and machine learning can be used specifically relating to their AML/CTF processes. For example:</p> <ul style="list-style-type: none"> • Encrypted apps and AI work management platforms are being increasingly used by practices to deal with and communicate with their clients. • Digital identity solutions can be used by practices to remotely identify and verify clients during onboarding. These solutions use AI to perform micro-expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis. 	<p>Leveraging emerging technologies, criminals can hide their identities using techniques such as:</p> <ul style="list-style-type: none"> • impersonating phone numbers and email addresses (spoofing) • using deepfake images and videos to impersonate another person through digital channels.

Clients: Inherent risk



This table supports Step 1 in Part 1 of the Customise the program starter kit guide.
Refer to the Customise guide for full instructions to assist you in completing your table.

Kinds of client	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these clients?
<p>Individuals and sole traders</p>	<p>An individual client, other than a sole trader, is a human being with legal capacity to enter into contracts and conduct transactions.</p> <p>A sole trader is an individual client who owns and operates a business alone, with no legal separation between the owner and the business. Like individuals, sole traders have the legal capacity to enter into contracts and conduct transactions.</p>	<p>The risk level varies based on personal, transactional and contextual factors.</p> <p>Individual clients can have risk factors that increase their ML/TF risk. This includes:</p> <ul style="list-style-type: none"> • their personal background and occupation • their business activities • their source of funds • their financial behaviour • any potential connections to high-risk activities or jurisdictions. 	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>Bodies corporate</p>	<p>A body corporate is a style of legal structure with a separate legal identity from their owners or members. A body corporate is recognised by law as having its own rights and obligations.</p> <p>The most common forms of companies are:</p> <ul style="list-style-type: none"> • private companies (Proprietary Limited) • public companies (Limited) • unlisted public companies (Limited) • owner’s strata corporations • cooperatives • incorporated partnerships. 	<p>Bodies corporate may be attractive to money launderers, as they are easy to set up or purchase with limited knowledge, skills or expertise. They also provide criminals with the capacity to launder high volumes of funds without the activity being directly linked to their own identity.</p> <p>Australian authorities report that bodies corporate are often exploited alongside other types of entities to create complex and opaque legal and group structures.</p> <p>The absence of public information about the beneficial owners of companies can make it difficult to verify if you are indirectly engaging with a criminal entity. It often requires manual analysis and information gathering.</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>

Kinds of client	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these clients?
Partnerships	<p>A partnership refers to where two or more individuals or other legal entities share ownership. A partnership is not a separate legal entity from its owners.</p> <p>The most common forms of partnerships are:</p> <ul style="list-style-type: none"> • general partnerships (simpler) • limited partnerships (more complex). 	<p>The level of risk will vary based on a range of factors.</p> <p>Partnership clients can have risk factors that increase the ML/TF risk, including the:</p> <ul style="list-style-type: none"> • backgrounds of the partners • nature of their business activities • ownership and control structure • geographic location of the partners • source of partnership funds. 	<input type="checkbox"/> Yes <input type="checkbox"/> No
Trusts	<p>A trust refers to a legal arrangement where one or more trustees hold and manage assets for the benefit of one or more beneficiaries.</p> <p>A trustee may be an individual or a legal entity (such as a company).</p> <p>The most common forms of trusts are:</p> <ul style="list-style-type: none"> • discretionary trusts (often used for family trusts) • unit trusts (often used by investment firms) • testamentary trusts (often created as part of an estate). 	<p>Trusts are attractive vehicles for ML, as they separate the legal owner of the assets (the trustee) from the beneficiary. This helps hide the beneficiary's interests. Trusts may also use a shell company with dummy directors as trustee to make it harder to identify who is controlling the trust.</p> <p>Australian authorities say trusts are frequently used with companies to form complicated, unclear legal structures.</p> <p>Lack of transparency for trusts in Australia hinders the detection of criminal use, making it harder to identify and seize illicit assets.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
Associations	<p>An association refers to a group of individuals who come together for a common purpose without forming a corporation or similar legal entity. Unless it is registered as an incorporated association, the association itself does not have legal rights or obligations.</p> <p>Associations may be incorporated or unincorporated.</p>	<p>Associations can have risk factors that increase the ML/TF risk, including the:</p> <ul style="list-style-type: none"> • backgrounds of the members • nature of the association's activities • incorporation status • control and governance structure • geographic location • source and use of association funds. <p>Unincorporated associations do not have the legal right to own property. Other kinds of clients may sell, buy or transfer property on behalf of an unincorporated association.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No

Kinds of client	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these clients?
Government bodies	A government body refers to a legal entity that is established and recognised by a government to perform specific functions and duties. It has a separate legal identity from its members or employees. A government body is recognised by law as having rights and obligations.	<p>While government entities are typically subject to strong oversight and internal controls, they can still be exploited indirectly or become vulnerable under certain conditions.</p> <p>Government body clients can have risk factors that increase their ML/TF risk - for example:</p> <ul style="list-style-type: none"> • nature of their activities • geographic location • amount of bribery and corruption present • associations with high-risk jurisdictions. 	<input type="checkbox"/> Yes <input type="checkbox"/> No

The Law Society of NSW has created the below template which you may wish to use to collect relevant data to assist in forming your practice’s risk profile.

Clients: Profile

The following clients have been provided designated services over the last [12] months.

Kind of client	Total number of clients	Total number of clients with two medium risk factors	Total number of clients with a high risk factor
Individuals and sole traders			
Bodies corporate			
Partnerships			
Trusts			
Associations			
Government bodies			

Clients: Risk factors



This table supports Step 2 in Part 1 of the Customise the program starter kit guide.

Refer to the Customise guide for full instructions to assist you in completing your table.

It is important to note that the following risk factors will arise if they are present in any person involved in the designated service, including:

- the client of the designated service
- any representative of the client
- any person on whose behalf a client is receiving a service (e.g. a beneficiary of a trust)
- any beneficial owner of the client.

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
Individuals that you suspect have committed profit-generating offences	<p>An individual may be involved in crime and use criminal proceeds to buy property.</p> <p>Not all criminal offences generate ML/TF risks. Offences that can be used to generate illicit profits include, but are not limited to:</p> <ul style="list-style-type: none"> • ML • TF • fraud and other financial crimes • tax evasion • corruption • drug trafficking • people smuggling. 	<p>Criminals who have profited from serious crimes are highly likely to try to obtain professional assistance when laundering their illicit funds. They are likely to continue doing so until their behaviour is detected.</p>	High	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Politically exposed persons (PEPs) (domestic)</p>	<p>Domestic PEPs are individuals who hold, or have held, senior roles in an Australian government body. This includes their family members and close associates, even if those people have not held such roles themselves.</p> <p>To establish if a former PEP may still present ML/TF risk, you should consider factors such as:</p> <ul style="list-style-type: none"> • whether the person still has influence over government decisions • how much time has elapsed since the person was a PEP • whether the person is still prominent and politically connected. 	<p>PEPs often have a public profile and may be vulnerable to corruption and bribery.</p> <p>For example, they may be able to influence any of the following:</p> <ul style="list-style-type: none"> • government spending and budgets • procurement processes • development approvals and grants. 	<p>Medium</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>PEPs (international organisations)</p>	<p>International organisation PEPs are individuals who hold, or have held, senior roles in an international organisation. This also includes their family members and close associates, even if those people have not held such roles themselves.</p> <p>To establish if a former PEP may still present ML/TF risk, you should consider factors such as:</p> <ul style="list-style-type: none"> • whether the person still has influence over international organisation decisions • how much time has elapsed since the person was a PEP • whether the person is still prominent and internationally connected. 	<p>PEPs often have a public profile and may be vulnerable to corruption and bribery.</p>	<p>Medium</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>PEPs (foreign)</p>	<p>Foreign PEPs are individuals who hold, or have held, senior roles in a foreign country’s government. This includes their family members and close associates, even if those people have not held such roles themselves.</p> <p>To establish whether a former PEP may still present ML/TF risk, you should consider factors such as:</p> <ul style="list-style-type: none"> • whether the person still has influence over government decisions • how much time has elapsed since the person was a PEP • whether the person is still prominent and politically connected. 	<p>PEPs often have a public profile and may be vulnerable to corruption and bribery.</p> <p>Foreign PEPs involved in corrupt activity frequently travel outside their jurisdiction to avoid domestic law enforcement. They may seek to move illegally generated funds offshore to avoid confiscation.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
<p>Client’s legal structures creating effective anonymity</p>	<p>Where a person’s ownership and control structure is highly complex or unusual, it can be difficult to analyse each layer and identify the beneficial owners. This makes the beneficial ownership ‘effectively anonymous’.</p> <p>Although there are legitimate reasons to use complex ownership and control structures, these structures are often used by criminals to distance themselves from transactions and activity which may attract attention from law enforcement.</p> <p>Importantly, beneficial owners of legal structures are not effectively anonymous if you can gather reliable documents which show individuals with ownership or control. For example, although information about trusts is not usually publicly available, getting the trust deed may show that the trustee and beneficiaries are related individuals.</p>	<p>Given the lack of measures to provide information about beneficial ownership of companies and trusts in Australia, the use of complex legal structures remains a major challenge for law enforcement.</p> <p>This vulnerability is of particular concern, as the use of Australian companies and financial infrastructure to evade sanctions is a key PF threat.</p>	<p>High</p>	<p><input type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>	

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
Third party (for individuals)	<p>An individual third party is an individual who acts through a third party or intermediary, such as a local representative.</p> <p>Note: This risk does not apply if the third party is a reporting entity enrolled with AUSTRAC or the client is not an individual (such as a company).</p>	<p>Using a third party or intermediary makes it difficult to:</p> <ul style="list-style-type: none"> know who the client is know what information the third party receives verify the source of funds. <p>Law enforcement confiscation of property and other assets purchased with proceeds of crime is challenging when third parties are used to conceal ownership.</p>	Medium	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Clients with significant unexplained wealth	<p>A client with significant unexplained wealth is an individual who has wealth far greater than their known legal income or assets and is unable to provide a reasonable explanation for the source of their wealth.</p>	<p>Unexplained wealth is a strong indicator of ML. It is a common offence type used in ML prosecutions and criminal asset confiscation cases.</p>	High	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Charities and NPOs	<p>Registered charities and legitimate NPOs provide an attractive channel for TF, as donations can be solicited from many individuals, witting and unwitting, and diverted for illicit purposes. Most observed cases relate to outgoing funds to support violent extremism or designated terrorist groups overseas.</p>	<p>As charities and NPOs are not reporting entities under the AML/CTF Act, detection of suspicious financial activity is therefore reliant on other reporting entities who provide services to NPOs.</p>	Medium	<input type="checkbox"/> Yes <input type="checkbox"/> No	
Low-complexity clients	<p>A low-complexity client is a client who presents with low complexity - for example, a domestic individual or a low-complexity legal structure with no other underlying high-risk factors.</p>	<p>There is low inherent risk associated with these parties in the absence of other risk factors. Low inherent risk does not mean no risk.</p>	Low	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Delivery channels: Inherent risks



This table supports Step 1 in Part 1 of the Customise the program starter kit guide.

Refer to the Customise guide for full instructions to assist you in completing your table.

Channel type	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide services using these delivery channels?
In person	The client is engaged or provided access to a service through direct, face-to-face interactions.	Risk factors include: <ul style="list-style-type: none"> exploitation through personal relationships and manipulation ability to detect fake or stolen IDs in person. 	<input type="checkbox"/> Yes <input type="checkbox"/> No
Email	The client is engaged or provided access to a service through emails.	Risk factors include: <ul style="list-style-type: none"> higher risk of fraud and scams due to fake or stolen IDs challenges in identifying suspicious behaviour or inconsistencies email address spoofing lack of encryption for document transfer reliance on third-party technologies. 	<input type="checkbox"/> Yes <input type="checkbox"/> No
Telephone	The client is engaged or provided access to a service through the telephone (including calls and text messages).	Risk factors include: <ul style="list-style-type: none"> challenges in identifying suspicious behaviour or inconsistencies phone number spoofing and voice manipulation. 	<input type="checkbox"/> Yes <input type="checkbox"/> No
Video conferencing programs	The client is engaged or provided access to a service through video conferencing programs.	Risk factors include: <ul style="list-style-type: none"> higher risk of fraud and scams due to fake or stolen IDs challenges in identifying suspicious behaviour or inconsistencies potential use of AI reliance on third-party technologies. 	<input type="checkbox"/> Yes <input type="checkbox"/> No
Online platforms	The client is engaged or provided access to a service through an online platform, including your website, a payment platform or other third-party apps.	Depending on the platform's purpose, functionality and regulatory oversight, digital channels are increasingly used to facilitate, conceal or coordinate illicit financial activity. Risk factors include: <ul style="list-style-type: none"> criminals depositing illegal funds with limited visibility higher risk of fraud and scams due to fake or stolen IDs challenges in identifying suspicious behaviour or inconsistencies reliance on third-party technologies. 	<input type="checkbox"/> Yes <input type="checkbox"/> No

The Law Society of NSW has created the below template which you may wish to use to collect relevant data to assist in forming your practice's risk profile.

Delivery channels: Profile

Over the last [12] the following channels have been used to provide designated services to clients.

Kind of channel	Total number of designated services provided using a channel
In person	
Email	
Telephone	
Video conferencing programs	
Online platforms	


Delivery channels: Risk factors



This table supports Step 2 in Part 1 of the Customise the program starter kit guide. Refer to the Customise guide for full instructions to assist you in completing your table.

Risk factor	Description of risk	Why it creates ML/TF vulnerability	Inherent risk rating	Risk appetite - would you accept this risk?	If NO, how will you avoid this risk?
Suspected false and fraudulent identities	<p>Criminals can use false identities to obtain services from practices without disclosing their real identity to them.</p> <p>False identities can involve using fake identification documents, lying on documentation about personal details, or using technology to impersonate another person.</p>	<p>Using a false identity allows criminals to get services which may have otherwise been out of reach. They can use a false identity to avoid detection by those practices and affect the practice's ability to correctly assess ML/TF risk.</p> <p>Leveraging emerging technologies, criminals can more easily hide their identities than ever before. Using techniques such as spoofing (impersonating phone numbers and email addresses) or using deepfake images and videos, criminals can take advantage of remote and digital channels more easily than ever before.</p> <p>You should consider how their delivery channels may allow for false identities and how you will detect if your client and other related parties are who they claim to be.</p>	High	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Countries: Risk assessment



This table supports Step 3 in Part 1 of the Customise the program starter kit guide. Refer to the Customise guide for full instructions to assist you in completing your table.

Country	Basel AML risk rating	Listed in high-risk country list?	Final country risk rating	Risk appetite - would you onboard these clients?	If NO, how will you avoid this risk?
Australia	Low	<input type="checkbox"/> Yes <input type="checkbox"/> No	Low	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	Choose an item.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

The Law Society of NSW has created the below template which you may wish to use to collect relevant data to assist in forming your practice’s risk profile.

Countries: Profile

Over the last [12] months, we have dealt with the following countries when providing designated services to clients.

Country	Final risk rating [H/M/L]	Total number of designated services involving country	Total number of clients located in country
Australia			
[Add Country]			

Common money laundering and terrorism financing methods



Common ML/TF methods are publicly known trends in how criminals launder money and finance terrorism or the proliferation of weapons of mass destruction. Identifying trends and patterns in criminal behaviours will help you to:

- understand the nature of existing and emerging ML/TF threats
- detect where criminals may try to use these methods when attempting to exploit your services.

The table below shows typical industry-specific ML/TF methods for you to look out for. Note that your practice may encounter other methods used by criminals which are not listed here.

Use this information as a reference during your daily monitoring and when reviewing client activity. If you are not sure if something is suspicious, escalate it so the AML/CTF compliance officer can make the assessment and determine next steps.

Method	Description	How it creates ML/TF risk	Possible red flags/ indicators
Conveyancing services Use of non-financial professionals	Professionals, such as lawyers and accountants, are often used by people to represent their interests in particular situations. This may be through mechanisms such as a power of attorney, empowering someone to obtain services and make decisions as if they were the person themselves.	Legitimate services offered by professionals such as lawyers and accountants can also be used by criminals to help mask their identity and the origin of their criminal profits, whether or not the professional is aware of the criminal's intentions. For example, a buyer may hire a solicitor to manage all interactions with a seller's conveyancer, making it difficult for the conveyancer to understand who their client is.	<ul style="list-style-type: none"> • Client uses a third-party without a logical reason. • Person on the contract of sale is different from the individual dealing with the conveyancer.
Conveyancing services Trust accounts	Conveyancers are required to hold funds received from buyers in a statutory trust account, as opposed to an ordinary practice bank account. When a buyer or real estate agent transfers a deposit to the conveyancer, they will hold it in their trust account until they are instructed to send those funds to the seller.	Criminals can misuse trust accounts to move illicit money while hiding its origin from the beneficiary. For example, when a conveyancer transfers funds from the sale to a seller, the seller's bank will not have visibility of the original source of that deposit. Criminal proceeds can also be commingled with legitimate client funds, making it difficult for law enforcement to detect suspicious activity.	<ul style="list-style-type: none"> • Client asks conveyancer to hold a deposit in trust longer than required, then issues an unusual instruction for disbursement. • Client deposits cash for property deposit, then withdraws and requests refund by cheque or electronic transfer.

Method	Description	How it creates ML/TF risk	Possible red flags/ indicators
Conveyancing services Shell companies	Shell companies are companies which have no real assets or any legitimate operations. They may hold a bank account and be registered as providing certain services; however, the company will rarely show any indications of a legitimate business.	Domestic and foreign shell companies commonly feature in Australian ML investigations. They are used to create a layer between suspicious transactions and the criminals. Shell companies often use dummy directors or shareholders on official records – that is, directors who have no actual involvement with the company’s activities. These individuals are used to conceal beneficial ownership and complicate the identification and disruption of ML.	<ul style="list-style-type: none"> • Company has little or no apparent business activity. • Company uses dummy directors or shareholders.
Conveyancing services Offshore companies	Companies and other legal entities or arrangements may be formed in one country but only ever used in others. These companies are particularly suspicious when they are based in countries which lack oversight or allow secrecy for beneficial owners – countries often known as tax havens.	Using offshore companies makes it harder for reporting entities to identify where beneficial owners are located, and where funds ultimately originate from or will ultimately be received. For example, where a person in a high-risk jurisdiction sends funds to an account held by a shell company in a tax haven country prior to a transfer to Australia, the Australian party would not have visibility of the true source.	<ul style="list-style-type: none"> • Client in Australia is purchasing property using an offshore company. • Client is a domestic entity owned by an offshore company in a tax haven or secrecy jurisdiction.
Conveyancing services Overvaluation or undervaluation	Where criminals work with other parties to misrepresent a property’s price on official documents, allowing illicit funds to be legitimised through the transaction. This would not include situations where a property sells for above market value due to public demand – for example, where bidding at an auction increases the purchase price well above the price guide.	For undervaluation, the sale contract would record a price lower than market value. The buyer pays the difference to the seller with illicit cash. For overvaluation, the property would be purchased at an inflated price so that the buyer can secure the largest possible loan, which can then be repaid using illicit funds.	<ul style="list-style-type: none"> • Property sold well above or below market price. • Unusual valuation of atypical properties, such as hotels or resorts.

Method	Description	How it creates ML/TF risk	Possible red flags/ indicators
Conveyancing services Quick reselling	<p>Property is bought and resold quickly in a way that is unusual, often at an inflated price without any physical changes to the property.</p> <p>There may be normal situations where this may occur - for example, where market conditions allow buyers to make profits after a short period of time.</p>	<p>Criminals may create multiple transactions between related parties that create distance between the origin of funds and their ultimate destination, being invested in real estate.</p>	<ul style="list-style-type: none"> Client resells a property shortly after purchase for no logical reason. There are repeated transactions involving the same buyer or seller.
Other professional services Misuse of client accounts (including trust accounts)	<p>Client accounts can be used to transfer funds without providing an underlying designated service.</p> <p>This can include unknown transactions made by the client or other professionals on their behalf.</p>	<p>Criminals can misuse trust accounts to move illicit money while hiding its origin from the beneficiary.</p> <p>Criminal proceeds can also be commingled with legitimate client funds, making it difficult for law enforcement to detect suspicious activity.</p>	<ul style="list-style-type: none"> There is no legitimate reason why the transfer is made through your trust account, rather than the client's personal bank account. Client uses trust account to purchase services or products that have no reasonable connection to services typically provided by your firm.
Other professional services Misuse of bodies corporate or legal arrangements	<p>Bodies corporate and legal arrangements can hide the ownership, purpose, activities and financing relating to criminal activity, serving as a source of income.</p>	<p>These uses make it more challenging to monitor and perform customer due diligence and verify the source of funds.</p>	<ul style="list-style-type: none"> Structure of body corporate or legal arrangements can effectively ensure anonymity of individuals who own, control or benefit from property or money. Structure is unnecessarily complex and the complexity cannot be explained by economic or legitimate reasons.

Method	Description	How it creates ML/TF risk	Possible red flags/ indicators
<p>Other professional services</p> <p>Use of specialised skills to use complexity to hide criminal activity</p>	<p>Specialised skills can be used to benefit criminal activity. The skills include the creation of company and trust formation, performing financial transactions and providing financial advice.</p>	<p>Skillsets held by professional service providers can be used to conceal and transfer criminal funds, obscuring ownership and criminal activity.</p> <p>The reputation and status of a legal practice creates an air of legitimacy that can be used to obscure the illicit use of services and skills.</p>	<ul style="list-style-type: none"> Client requests or uses unnecessarily complex business ownership structures, including nominee shareholders or bearer shares. Client asks to buy aged shelf companies, rather than set up new ones. Client requests the creation of a trust where it is unlikely to be appropriate or necessary.
<p>Other professional services</p> <p>Loan-back schemes</p>	<p>Loan-back schemes can be used by criminals to disguise illicit funds as legitimate loans. Criminals lend themselves money, often through property purchases or shares in investment funds. The 'loan' makes it appear that funds come from legitimate business activity.</p>	<p>Loan-back schemes can:</p> <ul style="list-style-type: none"> create the appearance of lawful funds hide the true identity of the parties disguise the real purpose of the transaction. <p>They make it difficult to identify and verify the source of funds of a transaction and the identity of ownership.</p>	<ul style="list-style-type: none"> Client is using their own company or associate to provide a loan. Funds are recycled through the same accounts. Loan terms are unusual or not at market rate. Client requests contracts for private loan agreements outside the financial system, with an unclear source of funds or wealth. Client is involved in business agreements or payments where the asset value is hidden or hard to determine.

Method	Description	How it creates ML/TF risk	Possible red flags/ indicators
Other professional services Unnecessary use of non-financial professionals	Professional services can be used to create structures to move illicit funds unnoticed. This includes other professionals being used as a nominee director, shareholder or trustee to disguise the client's true identity or involvement.	This increases the difficulty involved in verifying the client's true identify and finding and verifying the source of funds.	<ul style="list-style-type: none"> Client insists on using unnecessary non-financial professionals without clear need. Unnecessary non-financial professionals are involved in multiple complex transaction without a clear business reason.
Other professional services Shell companies	Shell companies are companies which have no real assets or any legitimate operations. They may hold a bank account and be registered as providing certain services; however, the company will rarely show any indications of being a legitimate business.	<p>Domestic and foreign shell companies commonly feature in Australian ML investigations. They are used to create a layer between suspicious transactions and the criminals.</p> <p>Shell companies often use dummy directors or shareholders on official records - that is, directors who have no actual involvement with the company's activities. These individuals are used to conceal beneficial ownership and complicate the identification and disruption of ML.</p>	<ul style="list-style-type: none"> Company has little or no apparent business activity. Company uses dummy directors or shareholders.
Other professional services Offshore companies and trusts	Companies and other legal entities or arrangements may be formed in one country but only ever used in others. These companies are particularly suspicious when they are based in countries which lack oversight or allow secrecy for beneficial owners - countries often known as tax havens.	<p>Using offshore companies makes it harder for reporting entities to identify where beneficial owners are located; and where funds ultimately originate from or will ultimate be received.</p> <p>For example, where a person in a high-risk jurisdiction sends funds to an account held by a shell company in a tax haven country prior to a transfer to Australia, the Australian party would not have visibility of the true source.</p>	<ul style="list-style-type: none"> Client in Australia is using an offshore company. Client is a domestic entity owned by an offshore company in a tax haven or secrecy jurisdiction.

Method	Description	How it creates ML/TF risk	Possible red flags/ indicators
Other professional services Overvaluation or undervaluation	The overvaluing, undervaluing or manipulation of the real value of an asset is a technique that consists of buying or selling assets at a price above or below its market value. This includes properties, body corporate and legal arrangements.	<p>For undervaluation, the sale contract would record a price lower than market value. The buyer pays the difference to the seller with illicit cash.</p> <p>For overvaluation, the asset would be purchased at an inflated price so that the buyer can secure the largest possible loan, which can then be repaid using illicit funds.</p>	<ul style="list-style-type: none"> Asset is sold well above or below market price. There are repeated transactions involving related parties.
Other professional services Structuring payments	A client can avoid reporting obligations or evade tax by restructuring payments. Structuring can also occur by using names of third parties to avoid the threshold reporting obligations.	Payment restructures can be used to avoid suspicion from regulatory bodies or evade tax.	<ul style="list-style-type: none"> Client makes frequent small transactions just under threshold reporting. Client uses multiple accounts (own or third party) to spread deposits.

Indicators of unusual or criminal behaviour

The tables below group common indicators of unusual or criminal behaviour based on the legal sector. Your practice may experience other indicators not listed.

Use this information as a reference during your ongoing monitoring and when reviewing client activity. If you are not sure if something is suspicious, escalate it so the AML/CTF compliance officer can make the assessment and determine next steps.

Learn more about [risk insights and indicators of suspicious activity for legal professionals](#).

Go to:

- [Client behaviour](#)
- [Client profile](#)
- [Unusual transactions and behaviours](#)
- [Foreign jurisdiction indicators](#)
- [Terrorism financing indicators](#)
- [Proliferation financing indicators](#)

Client behaviour

Theme	Indicators
The client provides unusual instructions or requests	<p>Conveyancing services</p> <p>The client or parties involved:</p> <ul style="list-style-type: none"> • push for transactions to be completed urgently, apply undue pressure or make last-minute changes to financing • give instructions on a property purchase or sale that are unusual or lack a clear financial purchase • request multiple changes after being asked for more information • begin purchasing a property without physically inspecting it • ask the conveyancer to hold funds in trust longer than required, then issue an unusual instruction for disbursement.
	<p>Other professional services</p> <p>The client or other parties involved:</p> <ul style="list-style-type: none"> • ask for limited or no interaction with regulatory agencies and show an understanding of reporting thresholds • are prepared to pay much higher fees than usual without clear reasons • make unusual requests with no clear economic reason • change instructions multiple times or in a short period of time without good reason • ask for shortcuts or speedy transactions, or other activities without a clear reason • want to take risks to reduce tax bills or are open to avoiding tax.

Theme	Indicators
The client exhibits unusual behaviours or avoids direct contact	<p>Conveyancing services</p> <p>The client or parties involved:</p> <ul style="list-style-type: none"> • appear nervous or are uncooperative during the CDD process • avoid face-to-face meetings without a clear reason • act in ways that do not match normal client behaviour • seem to follow instruction from someone else without naming that person • give limited ways to be contacted, such as through messaging apps, phone or email only. <p>Other professional services</p> <p>The client or other parties involved:</p> <ul style="list-style-type: none"> • request undue secrecy or are reluctant to provide further information or documentation when asked • request services with no face-to-face interaction • end the relationship quickly and unexpectedly • appear nervous or defensive when questioned • have multiple accounts in their name or the names of family members or corporate entities with no clear business or other purpose • are involved in transactions or account activities that are suspicious but refuse or are unable to answer questions related to those activities.
Third parties are unusually involved	<p>Conveyancing services</p> <p>The client or parties involved:</p> <ul style="list-style-type: none"> • appear to know and be working with the other parties to make a transaction look legitimate while stating they have no relationship • try to buy property in the name of a relative, minor or third party without a clear legal or financial reason • ask for sudden or unexplained changes in ownership, especially close to settlement • seek to transfer property without money changing hands or transfer ownership indirectly through another person, company or trust. <p>Other professional services</p> <p>The client or other parties involved:</p> <ul style="list-style-type: none"> • appear to be acting on somebody else's instructions but do not reveal that person's identity • appear to know and be working with the other parties to make a transaction look legitimate while stating they have no relationship.

Client profile

Theme	Indicators
The client's request appears inconsistent with their profile	<p>Conveyancing services</p> <p>The client:</p> <ul style="list-style-type: none"> • has wealth or assets that do not match their occupation or known income • operates a business with little or no trading activity • uses a business or entity to buy property in a way that does not match its profile (e.g. a charitable trust purchasing a luxury residential property). <p>Other professional services</p> <p>The client:</p> <ul style="list-style-type: none"> • has a lifestyle and/or transactions which are inconsistent with their known business and personal information • takes on work/employment that is outside their normal range of goods and services • has records that consistently show business sales losses, but they continue operating without a reasonable explanation • has no employees, which is unusual for their business type • is suspected of using personal accounts for business or vice-versa • recently established a series of new relationships with different financial entities • has changed professional advisers often without legitimate reasons or was refused service by other professional advisors.
The client provides unusual information during CDD	<p>Conveyancing services</p> <p>The client or parties involved:</p> <ul style="list-style-type: none"> • provide identity or other verification documents that appear fraudulent or cannot be authenticated • provide identity documents with inconsistencies or differences in details like their name, address, date of birth or phone number • have common identifiers that are used by multiple other people who do not appear to be related or are carrying out similar transactions • give only a post box address or pretend it is a residential or business address to hide their real address • refuse to identify their source of funds; or provide information that is false, misleading or substantially incorrect. <p>Other professional services</p> <p>The client or other parties involved:</p> <ul style="list-style-type: none"> • provide identity or other verification documents that appear fraudulent or cannot be authenticated • provide identity documents with inconsistencies or differences in details like their name, address, date of birth or phone number • have common identifiers that are used by multiple other people who do not appear to be related or are carrying out similar transactions • give only a post office box address or pretend it's a residential or business address to hide their real address • refuse to identify their source of funds; or provide information that is false, misleading or substantially incorrect.

Theme	Indicators
The client is subject to adverse information and potential criminal links	<p>The client, other parties involved or a person closely linked to the client has:</p> <ul style="list-style-type: none"> • been subject to negative media reports or other adverse information from a reliable source, connecting them to profit-generating criminal activity • ties to industries with known ML/TF risks, including those identified in Australia's national risk assessments.
The client is a PEP, from a high-risk country or subject to sanctions	<p>The client, other parties involved, or a person closely linked to the client:</p> <ul style="list-style-type: none"> • is a high-risk PEP or closely linked to one • comes from a high-risk country identified by credible sources as linked to corruption, organised crime, serious fraud or TF • is listed on the Department of Foreign Affairs and Trade Consolidated List.

Unusual transactions and behaviours

Theme	Indicators
Transactions between the client and your practice are unusual	<p>Conveyancing services</p> <p>The client or parties involved:</p> <ul style="list-style-type: none"> • deposit physical currency for a property, then withdraw and request a refund by cheque or electronic transfer • pay physical currency directly to the seller as a deposit or in a large single payment • request to pay you in physical currency or foreign currency without a valid reason (e.g. having no personal or professional link to the currency) • request to pay you using virtual assets (such as Bitcoin or Ethereum).
	<p>Other professional services</p> <p>The client or other parties involved:</p> <ul style="list-style-type: none"> • pay you by a method not in line with their profile • unnecessarily split or structure transactions to avoid identification or reporting thresholds for other financial services • abort activities or transactions after receiving funds, with a request to refund, or an unexplained request to send funds to a third party • provide confusing details about a transaction or know little about its purpose • use trust accounts for transactions that are more appropriately conducted from their bank account • use cryptocurrency or other virtual assets inconsistent with their client profile • make transactions in rounded sum values, not typical of what would be expected • make transactions consistent with a publicly known trend in criminal activity.

Theme	Indicators
Your client's property transactions are outside of normal patterns	<p>Conveyancing services</p> <p>The client or parties involved:</p> <ul style="list-style-type: none"> • buy or sell property in quick succession without a clear reason • request a service outside the conveyancer's normal area of practice, such as commercial instead of residential • pay far more or less than the expected market value • want an unnecessarily complex title transfer that increases costs or taxes • use promissory notes, bills of exchange, titles of credit or other negotiable instruments outside the financial system that can be settled in cash • pay part or all the property purchase price in physical cash • renovate and resell a recently purchased property without a clear or legitimate source of funds.
	<p>Other professional services</p> <p>The client or other parties involved:</p> <ul style="list-style-type: none"> • engage in transactions related to high-value assets with an unclear source of funds • make transactions involving a disproportionate amount of private funding or physical currency inconsistent with their socioeconomic profile • have transaction activity inconsistent with their apparent financial standing, usual activities or employment status (e.g. they may be a student, unemployed or on social assistance) • have transaction activity far exceeding the projected activity at the start of the relationship • conduct transactions inconsistent with what is expected from their declared business (e.g. no payroll payments) • make frequent overseas transfers inconsistent with their financial profile • receive payments from unrelated or unknown third parties without legitimate explanation • have accounts that appear to be used for pass-through activities (e.g. to receive and forward funds to others) • are involved in transactions or requests for financial services (e.g. loans) that do not make commercial sense, or with early settlement • have a sudden change in their financial profile, activity or transactions • have transactions with financial connections between individuals or entities that are not usually connected (e.g. a food importer dealing with an automobile parts exporter) • have a rapid turnover or transactions or activities (e.g. they may trade for a short time, close, then start up as a new company) • make large payments to subsidiaries or similarly control companies that are outside the normal course of business • use aliases or name variations from one transaction to another • conduct transaction(s) involving a suspected shell entity that appears to have no economic or logical reason to exist • have funds transferred in and out of an account on the same day or in a relatively short period of time without explanation • make or request wire transfers to or from multiple beneficiaries that are inconsistent with the expected use of their account type.

Theme	Indicators
Unusual third-party involvement in transactions with your practice	<p>The client or parties involved:</p> <ul style="list-style-type: none"> • direct sale proceeds to a third party or ask that costs or invoices be paid by someone else • bring in a third party to cover costs or repayments or to receive proceeds without a clear reason • in conveyancing transactions - use third parties to distance themselves from the transaction, such as when the person on the contract of sale is different from the individual dealing with the conveyancer.

Foreign jurisdiction indicators

Theme	Indicators
The client is linked to a high-risk foreign jurisdiction	<p>The client, or a person closely linked to the client:</p> <ul style="list-style-type: none"> • is based in or is residing in a high-risk jurisdiction • has a company owned or controlled by another company based in a high-risk jurisdiction • transfers funds to or from a country that has no clear connection to them • transfers funds to or from entities in high-risk countries.

Terrorism financing indicators

Theme	Indicators
The client has known links to activities with high TF risk	<p>The client, or a person closely linked to the client:</p> <ul style="list-style-type: none"> • is known to be involved or suspected of involvement with terrorist or TF related activities • is based in or linked to countries or regions identified by credible sources as providing funding or support for terrorist activities or that have <u>listed terrorist organisations</u> operating within them • appears in media or online as fundraising for causes which may be directly or indirectly linked to terrorism or violent extremism • is linked to unregistered NPOs or other unlicensed fundraising.

Proliferation financing indicators

Theme	Indicators
The client is linked to regions or other persons subject to high PF risk	<p>The client or parties involved:</p> <ul style="list-style-type: none"> • are linked to countries of proliferation or sanctions concern (e.g. the Democratic People's Republic of Korea or Iran). • share addresses, employment or other details with sanctioned individuals or organisations.
The client deals in goods subject to high PF risk	<p>The client or parties involved:</p> <ul style="list-style-type: none"> • deal in goods or technical controlled goods listed on the <u>Defence and Strategic Goods List</u>.

Risk assessment sources

The following sources have been used to produce the ratings for inherent risks, risk factors and ML/TF methods in the program starter kit for this AML/CTF program (as of 29 January 2026):

- [AUSTRAC - Money laundering in Australia national risk assessment 2024](#)
- [AUSTRAC - Terrorism financing in Australia national risk assessment 2024](#)
- [AUSTRAC - Proliferation financing in Australia national risk assessment 2022](#)
- [AUSTRAC - Risks and indicators of suspicious activity](#)
- [AUSTRAC - Reform guidance - Step 2: Identify and assess your risks: risk assessment \(Reform\)](#)
- [Australian Sanctions Office \(ASO\) - Advisory Notes \(ASO\)](#)
- International reporting on ML trends, including publications from the [Financial Action Task Force \(FATF\)](#), [Asia-Pacific Group on Money Laundering \(APG\)](#)
- financial transaction reporting to AUSTRAC
- financial, criminal and other intelligence holdings.



Record any other materials which you use to review and update this risk assessment as per the table below.

Author	Name of material	Date published	Location of material
<i>e.g. AUSTRAC</i>	<i>e.g. New national risk assessments</i>	<i>e.g. 1 January 2028</i>	<i>e.g. website URL</i>

Disclaimer

This Law Society of NSW AML/CTF Implementation Guide: for medium and large practices (**Guide**) is for general guidance purposes only and does not constitute legal, financial or other professional advice. This Guide is not intended to be relied upon as a substitute for professional advice. Users of the Guide must consider the particular circumstances and laws applicable to their situation.

While reasonable care has been taken in the preparation of this Guide, no representation or warranty (express or implied) is given as to the accuracy, reliability, currency or completeness of the information contained in it. Laws, regulations and guidance may change and the information in this Guide may not reflect the most current legal or regulatory developments.

To the maximum extent permitted by law, the Law Society of New South Wales and its officers, employees and agents disclaim all liability for any loss, damage, cost or expense (whether direct, indirect or consequential) arising out of or in connection with the use of, or reliance on, the information contained in this Guide.

Nothing in this Guide creates an advisory or other professional relationship between the Law Society of New South Wales and the user.

Copyright in this document is owned by Grant Thornton Australia Limited (**Grant Thornton**) and is used under licence. This document is produced and distributed under licence from Grant Thornton for the use of the Law Society of New South Wales, its members, and non-member legal practitioners. Except as permitted by the *Copyright Act 1968* (Cth), no part of this document may be reproduced, copied, stored, transmitted or otherwise dealt with without Grant Thornton's prior written permission. This document must not be sublicensed, assigned or otherwise transferred to any other person without Grant Thornton's prior written permission.



The Law Society
OF NEW SOUTH WALES

For the latest insights and developments
on AML/CTF, visit our dedicated AML/CTF Hub,
lawsociety.com.au/AMLCTFHub

The Law Society of New South Wales
170 Phillip Street, Sydney NSW 2000
ACN 000 000 699 ABN 98 696 304 966

T: +61 2 9926 0333 F: +61 2 9231 5809
E: CustomerService@lawsociety.com.au
W: lawsociety.com.au