Australian Government
AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

Money laundering and terrorism financing (ML/TF) risk assessment framework

Quick guide for lawyers

Businesses regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act) are at high risk of criminal exploitation.

Criminals may target the services you provide to move, hide or disguise illicit funds. This money can then be used to fund terrorism or support the spread of weapons of mass destruction.

Managing your money laundering, terrorism financing and proliferation financing risks (we refer to these as your ML/TF risks) is a main part of meeting your obligations under the Act. An ML/TF risk assessment is the first step in protecting your business. It helps you identify where you could be exposed and guides the policies, systems and controls you need to manage those risks.

ML/TF risk assessment framework

The core risk assessment approach has three stages:

STEP 1

Identify your inherent risk

Pinpoint areas of your business that could be exposed to ML/TF risk. At this stage, focus on any weaknesses.

STEP 2

Assess your inherent risk

Are these weaknesses open to exploitation? Assess the potential impact on your business if they are.

STEP 3

Evaluate and prioritise

Compare the risks you've assessed and decide which ones need attention.

After completing your risk assessment, your next steps are to:

- manage and mitigate identified risks through your anti-money laundering and counter-terrorism financing (AML/CTF) policies
- review and update your risk assessment to make sure it remains accurate and up to date.

Inherent risk: these are the risks you may reasonably face before you apply any policies, procedures, systems and controls to mitigate and manage them.

What to consider in your risk assessment

When you identify and assess your ML/TF risks, you must consider the following risk categories:

- services you provide
- customers you deal with
- channels you use to deliver services
- countries you deal with.

You must also consider information communicated by AUSTRAC about ML/TF risks associated with your services. These include our risk products, national risk assessments, sector guidance and any direct feedback we give you.

Developing your ML/TF risk assessment – lawyers

The examples in this quick guide can be used to help you develop an ML/TF risk assessment for your business.

STEP 1

Identify your inherent risks

Legal practices face unique challenges. These examples show the sector's common weaknesses and risk factors. This isn't an exhaustive list.

Services

You should consider whether the services you provide have built-in ML/TF risks.

- **Unusually complicated arrangements** – contracts or agreements that are more complicated than necessary, without a clear business reason.
- **Rushed timeframes** – pressure to complete settlements or transactions (such as transfers, acquisitions or other legal arrangements) faster than usual or outside of normal timeframes.
- **Unusual payments** – customers using unusual payment methods or offering to pay fees that seem out of proportion to the services requested.

Customers

Some customer types may present higher ML/TF risks.

- **Evasive or secretive behaviour** – avoids answering questions or provides vague, inconsistent or incomplete information.
- **Unexplained sources of wealth** – lifestyle or transactions that don't align with known business and personal information.
- **Complex legal structures** – business structures or relationships that make it difficult to identify the true beneficial owner.
- **Connection to high-risk jurisdictions** – customer funds originating from countries with poor AML/CTF regimes.
- **Customers dealing in dual-use goods** – customers involved in the production, transfer or payment for military or dual-use goods and technology listed on the Defence and Strategic Goods List, especially to or from sanctioned or high-risk regimes.

Delivery channels

Below are examples of risk factors linked to the delivery channels your business may use.

- **Use of third parties or intermediaries** – instructions come through a third party or intermediary, with minimal or no direct contact with the customer, possibly to conceal ownership.
- **Remote engagement** – avoids in-person meetings or telephone conversations, increasing anonymity, and reducing the ability to assess customer behaviour.
- **Unregulated payment methods** – proposes using only cash or cryptocurrency to fund a transaction, making the source of settlement funds difficult to trace.

Countries

Assess this risk by listing all the countries your business deals with when providing designated services. This includes the country:

- of residence for individual customers
- where corporate customers or legal arrangements are registered or formed.

You should assess and apply a risk rating for each listed country. We expect you to apply a **high-risk rating** for any country that is on the Financial Action Task Force (FATF) grey or blacklist or is subject to Australian sanctions.

STEP 2

Assess your inherent risk

For each risk you identify, consider the following based on the size and complexity of your business.

Medium-complexity businesses:

If your business is medium complexity, you could consider how likely it is that the vulnerability could be exploited, and the potential impact if it were.

You could use the **example risk matrix** to guide your rating:

Likelihood/impact	Minor	Moderate	Major
Very likely	Medium	High	High
Likely	Low	Medium	High
Not likely	Low	Low	Medium

Example: if a risk is 'likely' and the impact would be considered 'moderate', the overall rating would be 'medium'.

You may also use a **table like this** to record and justify your risk ratings:

Risk factor	Description	Likelihood	Rationale of likelihood	Impact	Rationale of impact	Inherent risk rating

Smaller, low-complexity businesses:

If your business is small and low complexity, you could assess inherent risk by just focusing on the potential impact if the vulnerability were exploited.

STEP 3

Evaluate and prioritise

Compare the risks you've assessed and decide which need the most attention. This will help you:

- rank risks in order of risk rating
- focus your attention and resources where they're most needed.

Important: High-risk areas should be addressed first.

After your assessment

Once you've identified your ML/TF risks, you must develop and maintain AML/CTF policies, procedures, systems and controls to manage and mitigate them. These should be proportionate – with stronger measures for higher risks and simpler measures for lower risks – and clearly set out how you'll manage them in practice.

Example of controls for lawyers:

- Enhanced customer due diligence on high-risk customers.
- Verification of beneficial ownership in complex structures.
- Monitoring trust accounts for unusual payment patterns.
- Ongoing customer due diligence for long-term customers.
- Stronger scrutiny of third-party withdrawals or deposits into and from trust accounts.
- Training staff to identify red flags.
- Monitoring customers for potential proliferation financing (PF) risks. For example, involvement in arms, munitions or dual-use goods listed on the Defence and Strategic Goods List.
- Screening and monitoring customers against the Department of Foreign Affairs and Trade (DFAT) Consolidated List.
- Embargoes on all business with citizens from countries of proliferation concern.

These are **examples only**. You must design AML/CTF policies that are tailored to your business's size, services and ML/TF risk profile.

Proliferation financing

You must assess your PF risk as part of your ML/TF risk assessment. The results inform whether you're required to develop and maintain specific AML/CTF policies to address PF risk.

Your PF risk	AML/CTF policies for PF risk
Low risk	Specific policies to address PF risks aren't required if your AML/CTF policies adequately manage this risk.
Medium risk	Develop and maintain AML/CTF policies to manage and mitigate PF risk.
High risk	

Your risk may be lower if you:

- only operate in Australia
- don't provide services to customers located in, or connected to, high-risk jurisdictions
- don't move money, sensitive goods or dual-use technologies overseas
- don't offer services relevant to PF.