Coolum Coastal Property

Risk Assessment Policy – Version 1 (22 June 2026).

Table of contents

Risk assessment

Your business needs to have a money laundering, terrorism financing and proliferation financing (we refer to these as ML/TF) risk assessment.

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

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

These inform how you develop other processes in your anti-money laundering and counter-terrorism financing (AML/CTF) program by ensuring that controls are proportionate to the level of risk you identify.

Under this system, a customer 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 customer isn't who they claim to be.
- **Medium risk rating** – where there are at least **2 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 isn't warranted under the tests above.

Risk ratings overview

These ratings and descriptions are used throughout the risk assessment.

Rating	Description
High	Represents significant potential ML/TF impact, major damage or effect. Potentially involving serious money laundering, terrorism or proliferation activity. Requires strong and proactive controls. Controls include: • enhanced customer due diligence (CDD) • gathering more information about the customer at onboarding (simplified CDD can’t be used) • ongoing monitoring • more frequent periodic reviews (every year).
Medium	Represents moderate potential ML/TF impact with a potential for adverse outcomes if controls do not appropriately manage and mitigate the risk. Controls include: • gathering more information about the customer at onboarding (simplified CDD can’t be used) • ongoing monitoring • periodic reviews every 2 years.
Low	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 3 years.

The ratings have been reached by considering different risk factors which may make your business vulnerable to exploitation. This is how easily criminals could exploit your designated services to launder money, finance terrorist acts or obtain weapons of mass destruction.

To do this, we've considered whether your designated services:

- 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 your risk assessment, you need to understand the inherent risks and other risk factors associated with providing your designated services.

Based on the sources listed below (see **Risk assessment sources**), we've provided a list of inherent risks and risk factors known to be relevant to sectors which work directly with real estate. The risk factors and ratings set out in the risk assessment have been used to develop the controls and processes which form the rest of the AML/CTF program.

Other elements of the program will draw directly on these risk factors to sort your customers into low, medium and high ML/TF risk categories. More thorough checks will apply to higher risk customers.

Money laundering: Inherent risk

Australia is one of the most attractive real estate markets globally. Australia's 2024 money laundering national risk assessment assessed:

- real estate as having a very high and stable vulnerability to money laundering. Criminals often exploit real estate as a core component of money laundering schemes
- real estate agents as posing a medium and stable vulnerability to money laundering, being exposed to potentially significant amounts of criminal proceeds.

It's expected that:

- real estate will continue to pose a high vulnerability to money laundering driven largely by the market's stability and high value
- real estate agents will continue to pose a medium vulnerability to money laundering driven by criminals' continued demand for Australian property.

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.

As the sale and purchase of real estate is a highly common way to launder money, real estate agents are inherently exposed to significant amounts of criminal proceeds when they hold deposits and other payments from customers.

Risk rating	Rationale
High	Real estate is highly vulnerable to exploitation by criminals when they are laundering money obtained through serious crimes, and this method is expected to continue for the foreseeable future.
Medium	Real estate agents can be taken advantage of by criminals when trying to purchase or sell real estate as part of a money laundering scheme.

Terrorism financing: Inherent risk

The real estate sector is more commonly used to launder money rather than fund terrorism. The 2024 terrorism financing national risk assessment doesn't describe any vulnerabilities specifically associated with real estate and terrorism financing.

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

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

Proliferation financing: Inherent risk

The 2024 proliferation financing (PF) national risk assessment provides little evidence of real estate playing a role in facilitating PF. Known international cases involve construction, property development and the sale or leasing of commercial or residential properties.

Risk rating	Rationale
Low	Limited evidence exists suggesting real estate being used in proliferation financing.

Designated services: Inherent risk

Designated service	Description	Vulnerabilities to ML/TF risk	Do you provide this service?
Brokering the sale, purchase or transfer of real estate on behalf of a customer. (Item 1, Table 5 of the AML/CTF Act)	Real estate brokering involves acting as an intermediary between buyers and sellers to complete property transactions. The real estate agent typically: • lists the property for sale, often through multiple listing sites and marketing channels • assesses potential buyers' financial capacity to buy the property • presents offers from buyers to the seller and negotiates terms such as price, contingencies, and settlement dates until an agreement is reached.	Real estate is a widely exploited asset type for money laundering in Australia. Criminals may use it to: • integrate illegal funds into the legitimate economy • store value from criminal proceeds. Criminals may purchase real estate by: • manipulating property value to quickly launder money • using complex ownership structures to conceal their involvement.	☒ Yes ☐ No

Designated services: Risk factors

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 and unfinanced transactions	Sales or purchases of property which: • involve transaction(s) valued at $1.5 million or more, and • don't involve any mortgage or other loan from a lending institution (such as a bank or non-bank lender).	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. Where the average transaction in a market is higher, criminals can place greater amounts of illicit funds in a property without drawing attention. Lenders perform in-depth due diligence on customers and properties before providing funds as part of a mortgage. Where a property is bought without a mortgage, there's a significant difference in scrutiny on the buyer.	**Medium**	☒ Yes ☐ No	
High value physical currency transactions	Property is purchased using high value physical currency transaction(s) (for example, in Australian dollar notes and coins or	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	**High**	☐ Yes ☒ No	**We'll ask the customer to make the payment via bank**

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?
	a foreign currency equivalent) valued at $50,000 or more.	asset types in criminal asset confiscation matters. It's exploited for its accessibility, widespread acceptance and availability. Its use also requires minimal skills, knowledge and expertise. Criminals looking to purchase real estate with large amounts of physical cash may give the cash to an agent or deposit it into the agency's statutory trust account directly.			**transfer. If they don't comply, we'll offboard the customer**
Virtual assets	Any payment or sale involving a virtual asset (for example, digital currencies such as Bitcoin or Ethereum). Virtual asset payments are highly unusual in the real estate sector, but some sellers do accept virtual assets as payment.	Criminals are attracted to virtual assets because they: • offer speed and global reach – transactions are almost instant and irreversible, making it challenging to detect and stop illicit use • allow movement of value with low visibility of the identity of the individual who owns or controls it. After someone exchanges fiat currency (this is government-issued currency, such as A$) for virtual assets, their		☐ Yes ☒ No	Refer to AML risk assessment team before engaging with customer.

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?
		payments completely bypass oversight from financial institutions.			
Unusual service requests	Any request for designated services which: • has no apparent economic or legal purpose • would involve unusually complex or large transactions • would involve an unusual pattern of transactions.	Customers who seek unusual services from your businesses 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 customer is willing to pay significantly more than market value for a property if the transaction is completed quickly.	High	☐ Yes ☒ No	Refer to AML risk assessment team before engaging with customer.

Designated services: New and emerging technologies

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

Kind of technology	Description	Why it creates ML/TF vulnerabilities
Artificial intelligence (AI)	Technology in the real estate sector provides secure digital infrastructure, integrated compliance tools and streamlined due diligence for property transactions. For example, virtual assistants and chatbots powered by AI are being used to engage new clients. Businesses are adopting artificial intelligence (AI) and machine learning to enhance data analysis, decision making and automate repetitive work.	AI represents a rising threat across the global economy and can easily be used for: • identity fabrication and impersonation • fake documents • laundering scam proceeds. Examples of how criminals can

	Businesses can use AI specifically for their AML/CTF processes. For example: • 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 with AI used to perform micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis.	hide their identities using AI include: • impersonating phone numbers and email addresses (spoofing) • using deepfake images and videos to impersonate another person through digital channels.
Real estate listing websites	Real estate websites and applications are the primary tools for searching and advertising properties, making them accessible to people at any time. These websites expand the possible audience for real estate listings to buyers across Australia and around the world.	Customers based in high ML/TF risk countries may be able to access listings online and use other professionals to attend property inspections and negotiations on their behalf.

Customers: Inherent risk

Kinds of customer	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these customers?
Individuals and sole traders	An individual customer, other than a sole trader, is a human being with legal capacity to enter into contracts and conduct transactions. A sole trader is an individual customer 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.	The risk level varies based on several personal, transactional and contextual factors. Individual customers can have risk factors that increase the ML/TF risk including their personal background, occupation or nature of business activities, source of funds, financial behaviour and any potential connections to high-risk activities or jurisdictions.	☒ Yes ☐ No
Bodies corporate	A body corporate is a type of legal structure with a separate legal identity from their owners or members. A body corporate is recognised by law as having	Bodies corporate may be attractive to money launderers as they're easy to set up or purchase with limited knowledge, skills or expertise. They also	☒ Yes ☐ No

Kinds of customer	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these customers?
	its own rights and obligations. The most common forms of companies are: • private companies (Proprietary Limited) • public companies (Limited) • unlisted public companies (Limited) • owner's strata corporations • cooperatives • incorporated partnerships	provide criminals with the capacity to launder high volumes of funds without the activity being directly linked to their own identity. Australian authorities report that bodies corporate are often exploited alongside other types of entities to create complex and opaque legal and group structures. The absence of public information about the beneficial owners of companies can make it difficult to verify if you're indirectly engaging with a criminal entity. It often requires manual analysis and information gathering.	
Partnerships	A partnership refers to where 2 or more individuals or other legal entities share ownership. A partnership isn't a separate legal entity from its owners. The most common forms of partnerships are: • general partnerships (simpler) • limited partnerships (more complex).	The level of risk will vary based on a range of factors. Partnership clients can have risk factors that increase the ML/TF risk including the: • backgrounds of the partners • nature of their business activities • ownership and control structure • geographic location of the partners • source of partnership funds.	☒ Yes ☐ No
Trusts	A trust refers to a legal arrangement where one or more trustees hold and manage assets for the benefit of one or more beneficiaries. A trustee may be an individual or a legal entity (such as a company).	Trusts are attractive vehicles for money laundering 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	☒ Yes ☐ No

Kinds of customer	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these customers?
	The most common forms of trusts are: • discretionary trusts (often used for family trusts) • unit trusts (often used by investment firms) • testamentary trusts (often created as part of an estate).	who's controlling the trust. Australian authorities say trusts are frequently used with companies to form complicated, unclear legal structures. Lack of transparency for trusts in Australia hinders the detection of criminal use, making it harder to identify and seize illicit assets	
Associations	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's registered as an incorporated association, the association itself does not have legal rights or obligations. Associations may be incorporated or unincorporated.	Associations can have risk factors that increase the ML/TF risk including the: • backgrounds of the members • nature of the association's activities • incorporation status • control and governance structure • geographic location • source and use of association funds. Unincorporated associations don't have the legal right to own property. Other kinds of customers may sell, buy or transfer real estate on behalf of an unincorporated association.	☒ Yes ☐ No
Government bodies	A government body refers to a legal entity that's established and recognised by a government to perform specific functions and duties. They have a separate legal identity from their members or employees. A government body is recognised by law as having rights and obligations.	While government entities are typically subject to strong oversight and internal controls, they can still be exploited indirectly or become vulnerable under certain conditions. Government body customers can have risk factors that increase their ML/TF risk including the: • nature of their activities • geographic location	☐ Yes ☒ No

Kinds of customer	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you deal with these customers?
		• amount of bribery and corruption present • associations with high-risk jurisdictions.	

Customers: Risk factors

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

- the customer of the designated service
- any representative of the customer
- any person on whose behalf a customer is receiving a service (for example, a beneficiary of a trust)
- any beneficial owner of the customer.

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	An individual may be involved in crime and use criminal proceeds to buy property. Not all criminal offences generate ML/TF risks. Offences that can be used to generate illicit profits include, but aren't limited to: • money laundering • terrorism financing • fraud and other financial crimes • tax evasion • corruption	Criminals who have profited from serious crimes are highly likely to try and launder their illicit funds through real estate purchases and sales. They're likely to continue doing so until their behaviour is detected.	**High**	☐ Yes ☒ No	Refer to AML risk assessment team before engaging with customer.

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?
	• drug trafficking • people smuggling.				
Politically exposed persons (PEPs) (domestic)	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 haven't held such roles themselves. To establish if a former PEP may still present ML/TF risk, you should consider factors such as: • if the person still has influence over government decisions • the time that has elapsed since the person was a PEP • if the person is still prominent and politically connected.	PEPs often have a public profile and may be vulnerable to corruption and bribery. For example, they may be able to influence any of the following: • government spending and budgets • procurement processes • development approvals and grants.	**Medium**	☐ Yes ☒ No	Refer to AML risk assessment team before engaging with customer.
PEPs (international organisations)	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 haven't	PEPs often have a public profile and may be vulnerable to corruption and bribery.	**Medium**	☐ Yes ☒ No	Refer to AML risk assessment team before engaging

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?
	held such roles themselves. To establish if a former PEP may still present ML/TF risk, you should consider factors, such as: • if the person still has influence over international organisation decisions • the time that has elapsed since the person was a PEP • if the person is still prominent and internationally connected.				with customer.
PEPs (foreign)	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 haven't held such roles themselves. To establish if a former PEP may still present ML/TF risk, you should consider factors such as: • if the person still has influence over	PEPs often have a public profile and may be vulnerable to corruption and bribery. 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.	High	☐ Yes ☒ No	Refer to AML risk assessment team before engaging with customer.

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?
	government decisions • the time that has elapsed since the person was a PEP • if the person is still prominent and politically connected.				
Legal structures creating effective anonymity	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'. 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. Importantly, beneficial owners of legal structures aren't effectively anonymous if you can gather reliable documents which	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. This vulnerability is of particular concern as the use of Australian companies and financial infrastructure to evade sanctions is a key proliferation funding threat.		☐ Yes ☒ No	Refer to AML risk assessment team before engaging with customer.

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?
	show individuals with ownership or control. For example, although information about trusts isn't usually publicly available, getting the trust deed may show that the trustee and beneficiaries are related individuals.				
Third party (for individuals)	An individual acts through a third party or intermediary, such as a local representative. Note: this risk doesn't apply if the third party is a reporting entity enrolled with AUSTRAC or the customer is not an individual (such as a company).	Using a third party or intermediary makes it difficult to: • know who the customer is • know what information the third party receives • verify the source of funds. Law enforcement confiscation of real estate purchased with proceeds of crime is challenging when third parties are used to conceal property ownership.	**Medium**	☒ Yes ☐ No	
Customers with significant unexplained wealth	A customer has wealth far greater than their known legal income or assets and is unable to provide a reasonable explanation for the source of their	Unexplained wealth is a strong indicator of money laundering. It's a common offence type used in money laundering prosecutions and criminal asset		☐ Yes ☒ No	Refer to AML risk assessment team before engaging

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?
	wealth.	confiscation cases.			with customer.
Charities and non-profit organisations (NPOs)	Registered charities and legitimate NPOs provide an attractive channel for terrorism financing 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.	As charities and non-profit organisations (NPOs) aren't reporting entities under the AML/CTF Act, detection of suspicious financial activity is therefore reliant on other reporting entities who provide services to NPOs.	**Medium**	☒ Yes ☐ No	
Low complexity customers	A customer presents with low complexity. For example, a domestic individual or a low complexity legal structure with no other underlying high-risk factors.	There's low inherent risk associated with these parties in the absence of other risk factors. Low inherent risk does not mean no risk.	**Low**	☒ Yes ☐ No	

Delivery channels: Inherent risks

Channel type	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide services using these delivery channels?

Channel type	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide services using these delivery channels?
In person	The customer is engaged or provided access to a service through direct, face-to-face interactions.	Risk factors include: • Exploitation through personal relationships and manipulation. • Ability to detect fake or stolen IDs in person.	☒ Yes ☐ No
Email	The customer is engaged or provided access to a service through emails.	Risk factors include: • 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.	☒ Yes ☐ No
Telephone	The customer is engaged or provided access to a service through the telephone (including calls and text messages).	Risk factors include: • Challenges in identifying suspicious behaviour or inconsistencies. • Phone number spoofing and voice manipulation.	☒ Yes ☐ No
Video conferencing programs	The customer is engaged or provided access to a service through video conferencing programs.	Risk factors include: • 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.	☐ Yes ☒ No
Online platforms	The customer is engaged or provided access to a service through an online platform. Including	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	☐ Yes ☒ No

Channel type	Description	Vulnerabilities to ML/TF risk	Risk appetite - would you provide services using these delivery channels?
	your website, a payment platform, or other third-party apps.	include: • 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.	

Delivery channels: Risk factors

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	Criminals can use false identities to obtain services from businesses without disclosing their real identity to them. False identities can involve using fake identification documents, lying on documentation about personal details, or using technology to impersonate another person.	Using a false identity allows criminals to get services which may have otherwise been out of reach, avoiding detection by those businesses and affecting their ability to correctly assess ML/TF risk. 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	**High**	☐ Yes ☒ No	**Refer to AML risk assessment team before engaging with customer.**

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?
		channels more easily than ever before. You should consider how your delivery channels may allow for false identities and how you will detect if your customer and other related parties are who they claim to be.			

Countries: Risk assessment

Country	Basel AML risk rating	Listed in high-risk country list?	Final country risk rating	Risk appetite – would you deal with these customers?
Australia	**Low**	☐ Yes ☒ No	**Low**	☒ Yes ☐ No
New Zealand	**Low**	☐ Yes ☒ No	**Low**	☒ Yes ☐ No
Sweden	**Low**	☐ Yes ☒ No	**Low**	☒ Yes ☐ No
France	**Low**	☐ Yes ☒ No	**Low**	☒ Yes ☐ No
Finland	**Low**	☐ Yes ☒ No	**Low**	☒ Yes ☐ No