



Australian Government

AUSTRAC

FIGHTING
FINANCIAL
CRIME
TOGETHER



PUBS AND CLUBS WITH GAMING MACHINES

REGULATORY GUIDE

Last updated **September 2026**

Contact us

Initial contact point

Enquiries about AUSTRAC, the legislation we administer or other information may be directed to AUSTRAC Central, available Monday to Friday, 8.30am to 5.00pm (Australian Eastern Standard Time).

Phone: 1300 021 037 (local call cost within Australia)

Email: contact@austrac.gov.au

Translating and interpreting assistance

AUSTRAC provides free access to a translation and interpreting service to assist people from diverse backgrounds to understand and meet their obligations to AUSTRAC.

AUSTRAC uses TIS National, an interpreting service provided by the Department of Home Affairs, for people who do not speak English, and English speakers who need to communicate with them.

To access the translation service, call during our Contact Centre operating hours on 131 450 and ask for 'AUSTRAC' on 1300 021 037. There is no charge for this service.

Deaf and speech-impaired callers

Callers who are deaf or have a hearing or speech impairment can contact AUSTRAC through the National Relay Service.

TTY (teletypewriter) or computer with modem users phone 133 677 and ask for 1300 021 037.

Speak and listen (speech-to-speech relay) users phone 1300 555 727 and ask for 1300 021 037.

Copyright

The Commonwealth owns the copyright in all material produced by this agency.

All material presented in this publication is provided under Creative Commons Attribution 4.0 International licence, with the exception of:

- the AUSTRAC logo
- content supplied by third parties.

The details of the relevant licence conditions are available on the Creative Commons website, as is the full legal code for the CC BY 4.0 license.

You may not reproduce or use this material in any way that suggests AUSTRAC or the Commonwealth endorses you or any of your services or products.



Attribution

Material obtained from this publication is to be attributed to:

© AUSTRAC for the Commonwealth of Australia 2026.

About regulatory guides

Regulatory guides provide detailed information about the anti-money laundering and counter-terrorism financing (AML/CTF) compliance requirements for the provision of designated services regulated by AUSTRAC. They include case studies that can be used to inform your understanding of your AML/CTF obligations.

What this regulatory guide is about

This guide has been developed for pubs and clubs that are licensed to operate electronic gaming machines (EGMs), including multi-terminal gaming machines (MTGMs).

This guide is designed to be used by AML/CTF compliance officers and senior managers working in the pubs and clubs sector. Use this guide to gain a thorough understanding of your AML/CTF obligations.



This guide should be considered in the context of your respective state and territory laws as part of your overall management of the risks of operating gaming machines at your venue.

This guidance doesn't constitute legal advice relevant to your business's specific needs and AML/CTF obligations.

There are 2 sections in this guide. The first section provides an overview of money laundering, terrorism financing, proliferation financing and the impacts of these for pubs and clubs. The second section provides practical guidance on how to meet your AML/CTF obligations.

The guide has been further divided into chapters addressing key topics, with each chapter including links to additional AUSTRAC guidance and other resources that will assist you.

Understanding the language we use

This guide uses specific language to indicate if something is an AML/CTF obligation, an expectation, or if it's a suggestion based on good practice.

When we use the phrase 'you must' in our guidance, that means it's either:

- a legal or regulatory obligation for your business
- an action we consider necessary in all circumstances to meet your obligations.

When we use the phrase 'we expect', this is an action that's likely necessary to comply with your obligations, but we remain open to other ways you can demonstrate compliance.

Other phrases, such as 'you may' or 'you could', are a suggestion based on good practice. You can choose to follow these suggestions or take a different approach that will work better for your business.

There's also a glossary at the back of this document that explains key terms.

Contents

Section 1: Anti-money laundering and counter-terrorism financing	5
What are money laundering, terrorism financing and proliferation financing?	5
Money laundering	5
Dealing in the proceeds of crime	5
Terrorism financing	5
Proliferation financing	6
The harms associated with these crimes	6
Australia's anti-money laundering and counter-terrorism financing laws	6
About AUSTRAC and who we regulate	7
Who is regulated by AUSTRAC?	7
How criminals try to exploit pubs and clubs	8
Obligations for pubs and clubs with electronic gaming machines	9
What happens if you don't meet your obligations?	10
Enforcement actions	10
Section 2: How to comply with your obligations	11
Enrolment and keeping your details up to date	11
Keeping your enrolment details up to date	11
Reporting groups	12
Your AML/CTF program	13
AML/CTF program obligations	13
Step 1: establish your governance framework	14
Step 2: identify and assess your risks	18
Step 3: mitigate and manage your risks – AML/CTF policies	24
Step 4: review and update your AML/CTF program	26
Step 5: conduct an independent evaluation	48
Record keeping	50
Record keeping for pubs and clubs with 15 or fewer EGM entitlements	51
Outsourcing	51
Section 3: Glossary	53
Need something else?	58

Section 1: Anti-money laundering and counter-terrorism financing

What are money laundering, terrorism financing and proliferation financing?

Money laundering

Money laundering is the process by which criminals take illicit funds from activities such as drug trafficking, illegal firearms sales, human trafficking, theft, tax evasion and other illegal activities and attempt to make the illicit funds appear legitimate.

Money laundering generally involves 3 stages:

1. Placement of the illicit funds into the financial system.
2. Layering of those illicit funds through multiple transactions and accounts to obscure their origin.
3. Integrating those illicit funds into the financial system where they appear legitimate.

Dealing in the proceeds of crime

In addition to the process of laundering funds, pubs and clubs are exposed to the risk of individuals spending funds from criminal activity for EGM play.

Dealing in the proceeds of crime is a criminal offence and venues should consider this as part of their risk assessment and transaction monitoring programs.

Terrorism financing

Terrorists need money to operate, for travel, equipment, shelter, food, supplies or services, training and to purchase weapons. Funds for terrorists can come from a range of legitimate and illegitimate sources and can be linked to organised criminal groups.

Acts of terrorism can be funded by relatively small amounts. It's estimated that the 2005 London bus bombings cost the equivalent of only a few thousand Australian dollars to carry out.

Terrorism financing generally involves 3 stages:

1. Raising funds, which can be through donations, self-funding or criminal activity.
2. Transferring the funds to a terrorist network, organisation or group.
3. Using the funds, for example to purchase weapons, cover living expenses for a terrorist group or make payments to their leaders.

Proliferation financing

Proliferation financing enables the spread of weapons of mass destruction. It's when a person makes available an asset, provides a financial service or conducts a financial transaction that's intended to facilitate the proliferation of weapons of mass destruction.

It helps provide the assets, services and transactions needed to obtain nuclear, chemical or biological weapons or materials related to these weapons.

The harms associated with these crimes

Money laundering, terrorism financing and proliferation financing are global problems that have direct social and economic impacts on Australia.

Criminals rely on money laundering to spend illicit funds, and to fund more illegal activities. The profits from their crimes can fund activities like tax evasion and fraud to human trafficking and modern slavery. Money laundering can:

- affect the price of goods
- deter foreign investors
- impede economic growth.

It also diminishes the tax revenue collected by governments and damages the credibility of our financial system and economy.

When terrorism financing contributes directly to an attack, the impact and harm are immediate, visible and severe. Terrorism financing can also create broader political and social damage, including community dispute and a loss of trust in government and public institutions.

Proliferation financing can have significant security and economic implications for Australia. Breaches of sanctions raise concerns about the integrity and effectiveness of Australia's counter-proliferation financing framework.

Australia's anti-money laundering and counter-terrorism financing laws

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the Act) aims to combat money laundering, terrorism financing and proliferation financing in Australia.

The Act places obligations on certain businesses known as 'reporting entities' to report transactions and suspicious activities to AUSTRAC and take steps to prevent their business from being used by criminals.

Each reporting entity must determine how it will meet its obligations, based on the level of money laundering, terrorism financing and proliferation financing risk (we refer to this as ML/TF risk) faced, as well as having regard to the nature, size and complexity of their business. This is because it's the reporting entity that's best placed to know the ML/TF risks associated with their:

- customers
- products
- operating structures
- business environment.

About AUSTRAC and who we regulate

AUSTRAC is Australia's AML/CTF regulator and financial intelligence unit. We're the Australian Government agency responsible for detecting, deterring and disrupting criminal abuse of the financial system.

AUSTRAC's purpose is to build resilience in the financial system and use financial intelligence and regulation to disrupt money laundering, terrorism financing, proliferation financing and other serious crimes. AUSTRAC works closely with businesses like yours, industry partners, law enforcement and other regulators to help fight financial crime.

AUSTRAC is responsible for:

- regulating reporting entities to ensure they comply with their obligations under the Act
- collecting and analysing the financial data reported by reporting entities
- disseminating financial intelligence for investigation to law enforcement, national security, revenue and regulatory agencies, as well as international counterparts.

The financial intelligence and reports generated by AUSTRAC are vital for Australia's national security and law enforcement.

Who is regulated by AUSTRAC?

AUSTRAC regulates businesses that provide certain 'designated services' listed in the Act. These designated services have been identified as posing a risk for money laundering, terrorism financing and proliferation financing.

This includes businesses that are licensed to operate EGMs or MTGMs. In this guide, 'EGM entitlements/licenses' refers to the legal authority, issued under relevant state or territory law, that permits a venue to operate gaming machines. This includes:

- clubs that hold 'entitlements'
- hotels that hold 'operating authorities' or 'entitlements'.

It's important to understand that the terminology used in this guide applies to pubs and clubs across Australia. The terms used by your state or territory licensing authority or regulator may differ. For example, the authority to operate EGMs may be described using different terms depending on the jurisdiction, including licences, entitlements and other regulatory authorisations.

If you're unsure how many EGM entitlements/licenses you're permitted to operate, we encourage you to check with your relevant regulator.

Many businesses that are licensed to operate EGMs also offer a Totalisator Agency Board (TAB) service to their customers. However, the TAB is responsible for meeting the Act obligations associated with this service. The TAB may rely on your business to undertake certain activities on their behalf to help them meet these obligations.

Businesses that have entitlements under licence to operate EGMs must submit certain reports to AUSTRAC. The reports you may be required to submit are:

- suspicious matter reports (SMRs) – all businesses
- threshold transaction reports (TTRs)¹ – businesses that have entitlements under licence to operate 16 or more gaming machines
- compliance reports – businesses that have entitlements under licence to operate 16 or more gaming machines.

The reports you provide to AUSTRAC help combat ML/TF and other serious criminal activity.



For more information about reporting see Section 2: how to comply with your obligations in this guide.

How criminals try to exploit pubs and clubs

Proceeds of crime are often in the form of cash, so EGMs can provide an opportunity for criminals to launder and use their funds. Criminals take advantage of the anonymity, ease of access and the cash intensive nature of the pubs and clubs industry to launder and use illicit funds.

All your gaming staff, including management and owners, must be aware of your ML/TF risks and take steps to mitigate and manage them.

Criminals seek out and attempt to take advantage of businesses that don't have the proper resources or processes in place to identify, assess, manage and mitigate their ML/TF risks.

Some examples of the ways criminals exploit gaming businesses include:

- Offering to pay cash to a legitimate player who has accumulated credits or has winning tickets. The criminal then claims the legitimate credits or winnings as their own.
- Inserting large amounts of cash or credits into EGMs or MTGMs and engaging in minimal or no game play to appear like a real player, before cashing out.
- Deliberately using multiple cashiers or only using cash redemption terminals (CRTs) to avoid staff observing or monitoring them.
- Exchanging lower denomination notes into higher denominations (cash refinement).
- Individuals or groups working to gain the trust of gaming staff or colluding with staff to avoid detection or providing identification when collecting winnings.

¹ A TTR applies only when a **single** cash transaction of \$10,000 or more is conducted. State and territory restrictions on cash payouts for gaming machine winnings mean most venues won't conduct a transaction of this size; **therefore, it won't trigger a TTR**. It's important to note that a TTR isn't triggered by aggregating multiple smaller payouts made throughout the day.

Obligations for pubs and clubs with electronic gaming machines

The AML/CTF obligations your business has depends on its number of EGM entitlements under licence to operate. This is regardless of how many EGMs are physically being operated at the time.

In this guide, the term 'EGM entitlements' is used to describe any legal authority issued under state or territory law that permits a venue to operate a gaming machine.²

Example: Under the *Gaming Machine Act 1991*, Queensland has a 2-layered approval model for gaming machines. Under this model, 'EGM entitlements' includes:

- entitlements (for clubs)
- operating authorities (for hotels).

Queensland clubs and hotels may have a gaming machine licence that permits a greater number of machines. However, the threshold for AUSTRAC is determined by the **number of operating authorities**.

If your business has entitlements under licence to operate 15 or fewer EGMs you may be exempt from many obligations. **But you must still enrol with AUSTRAC and submit suspicious matter reports.** Below is a table listing the AML/CTF obligations a pub or club will have, based on the number of EGM entitlements it's licensed to operate, as noted in its enrolment with AUSTRAC.

Businesses with entitlements under licence to operate 15 or fewer EGMs	Businesses with entitlements under licence to operate 16 or more EGMs
• Enrol with AUSTRAC • Keep enrolment details up to date • Keep certain records • Submit suspicious matter reports	• Enrol with AUSTRAC • Keep enrolment details up to date • Keep certain records • Appoint a compliance officer • Conduct and maintain an ML/TF risk assessment • Adopt and maintain AML/CTF policies • Carry out customer due diligence (CDD) • Coordinate regular independent evaluations of the AML/CTF program • Submit suspicious matter reports • Submit threshold transaction reports • Submit annual compliance reports

² This guide should be considered in the context of your respective state and territory laws.

Below are some examples of when each column of the above table might apply to a reporting entity.

Example 1: you're a business with an entitlement under licence to operate 20 EGMs, however you currently only operate 12 EGMs, as the other 8 EGMs are in storage. As your entitlement under licence to operate EGMs is 16 or more, the obligations in the right-hand column apply.

Example 2: you're a business with an entitlement under licence to operate 20 EGMs. You currently operate 20 EGMs, 12 are under your licence and 8 are leased under the licence of another unrelated business. As you're entitled to operate the 20 EGMs under licence, the obligations in the right-hand column apply.

Example 3: you're a business with a gaming machine licence that allows up to 20 EGMs. However, your venue holds only 10 operating authorities, which are the actual legal permissions required to operate EGMs. This means your venue can legally operate 10 machines. Because the entitlements under licence to operate EGMs is 15 or fewer, the obligations in the left-hand column apply.

What happens if you don't meet your obligations?

If you fail to meet your obligations, you're potentially placing your business and community at greater risk of harm from ML/TF and other serious crimes. AUSTRAC can take steps to enforce your compliance and/or seek a penalty if you don't meet your AML/CTF obligations.

It's important to remember that a business of any size could be exploited by criminals and potentially used to commit crimes.

Enforcement actions

Enforcement actions we can take include:

- A remedial direction to take specific actions to comply with certain parts of the Act. Remedial directions are generally made public.
- Infringement notices for contraventions of some obligations, for example:
 - collecting know your customer (KYC) information
 - reporting
 - enrolling with AUSTRAC
 - notifying AUSTRAC of changes to enrolment details
 - making and keeping certain records.
- Written notices requiring you to do any of the following:
 - appoint an external auditor to review your ML/TF risk management or AML/CTF compliance
 - undertake an ML/TF risk assessment
 - provide AUSTRAC with information about how you're complying with your obligations under the Act.
- An enforceable undertaking to AUSTRAC, detailing how you'll comply with your AML/CTF obligations.
- Applying for a civil penalty order from the Federal Court of Australia.



Visit the AUSTRAC website to learn more about [the consequences of not complying](#).

Section 2: How to comply with your obligations

Enrolment and keeping your details up to date

You must enrol with AUSTRAC within 28 days after the day you first provide a gambling service. For example, from when you first:

- allow a person to play an EGM
- pay out winnings for EGM play.

Read more about how to [enrol with AUSTRAC](#), including instructions and the information you must provide.

Enrolment with AUSTRAC is separate from any other requirements in your state or territory.

Keeping your enrolment details up to date

You must notify AUSTRAC within 14 days of any changes to your enrolment details, including:

- a new contact person
- a new AML/CTF compliance officer
- changes to key personnel or ownership
- contact information (phone number/email)
- a change in the number of EGM entitlements under licence to operate
- certain other business information that affects your AUSTRAC enrolment.

Changes to your details can only be updated using [AUSTRAC Online](#).

Without up-to-date details, your business may miss out on receiving important information from AUSTRAC, including:

- updates to sector-specific guidance about ML/TF risks
- reminders and deadlines to provide annual compliance reports to AUSTRAC.

Failure to keep your details up to date is also a breach of your AML/CTF obligations.

Reporting groups

Reporting groups allow reporting entities to share and centralise AML/CTF functions by sharing resources, reducing costs and ultimately managing and mitigating ML/TF risks more effectively.

A reporting group is made up of a group of persons, including at least one reporting entity. It consists of a 'lead entity' and 'ordinary members' who have group-wide AML/CTF policies. This allows them to share ML/TF risk-related information and AML/CTF compliance-related information.

While all reporting entities in the group have AML/CTF obligations, the lead entity is also legally accountable for:

- developing a group-wide ML/TF risk assessment and AML/CTF policies
- implementing group-wide AML/CTF policies
- ML/TF risk management
- AML/CTF compliance management.



The governing body still owns accountability over their AML/CTF policies, training and oversight mechanisms, even if these responsibilities have been outsourced through a reporting group.



Visit the AUSTRAC website to learn more about [reporting groups](#).

Your AML/CTF program

You must develop, maintain and comply with an AML/CTF program, which includes both your:

- Money laundering and terrorism financing risk assessment. This identifies and assesses your business's money laundering, terrorism financing and proliferation financing risks (we refer to these as ML/TF risks). It's the first step in developing your program and shapes the AML/CTF policies that protect your business.
- AML/CTF policies. These detail the policies, procedures, systems and controls you'll use to manage and mitigate your ML/TF risks. They make sure you comply with your AML/CTF obligations.

Different reporting entities face different ML/TF risks. This is why an effective program must be 'risk based' and designed to address the specific risks of your business along with its needs and characteristics.

Your AML/CTF program must also be:

- in place before you start providing a designated service
- clearly documented in writing
- approved by a senior manager
- complied with.

AML/CTF program obligations

There are several steps involved in developing your AML/CTF program. These include:

- establishing your governance framework
- conducting an ML/TF risk assessment
- developing AML/CTF policies
- documenting and approving your AML/CTF program
- complying with your program
- reviewing and updating your program
- independent evaluation.

Step 1: establish your governance framework

There are 3 roles in the AML/CTF governance structure, the:

- governing body
- senior manager
- AML/CTF compliance officer.

These roles are typically held by different people, but in a small business one person can hold multiple roles.

Governing body

The governing body is the person or group primarily responsible for the governance and executive decisions of the business. For larger pubs and clubs this may be the board. In pubs it may be the business owner.

Responsibilities of the governing body

As part of its responsibility for oversight of the risks at your venue, the governing body must exercise appropriate ongoing oversight of how you identify and assess ML/TF risks in your risk assessment, and take reasonable steps to make sure your business is:

- appropriately identifying, assessing, managing and mitigating ML/TF risks
- complying with your AML/CTF policies
- complying with its AML/CTF obligations.

The governing body must also receive reports from the AML/CTF compliance officer at least every 12 months about your:

- compliance with your AML/CTF policies and obligations
- ML/TF risk mitigation and management.

We expect your governing body to question and review matters in these reports, where appropriate, and take reasonable steps to address non-compliance and any failure to identify and assess risks.

Senior manager

The senior manager is an individual who makes decisions affecting all or a substantial part of your business or is involved in those decisions. For a small pub, this might be a director or business owner. For larger pubs and clubs, this could be a general manager.

Responsibilities of the senior manager

Senior managers must fulfil their AML/CTF obligations personally and cannot delegate them to other staff.

Senior managers must approve:

- your risk assessment, AML/CTF policies and updates to both
- certain business relationships before they are entered into
- entering into any written agreement with a third party that will collect and verify customer due diligence (CDD) information for you
- providing a designated service to any customer who you've established on reasonable grounds is a:
 - foreign politically exposed person (PEP)
 - high-risk customer that's also a domestic PEP
 - high-risk customer that's also an international organisation PEP.



Visit the AUSTRAC website to learn more about [politically exposed persons](#).



It's important that your AML/CTF policies make sure senior manager approvals are appropriately recorded.

AML/CTF compliance officer

The AML/CTF compliance officer is responsible for communicating with AUSTRAC for your business. They must also oversee and coordinate your day-to-day AML/CTF compliance and give reports to the governing body at least once every 12 months on AML/CTF compliance.

In practice, this might mean your AML/CTF compliance officer is responsible for:

- overseeing and coordinating the effective operation of and compliance with your business's AML/CTF policies
- training staff so that ML/TF risks, and AML/CTF processes and procedures are understood
- checking that staff training is up to date, and testing that it's effective
- reporting issues or making recommendations to the governing body
- submitting reports to AUSTRAC within specified timeframes
- keeping up to date with information on ML/TF risks in the industry
- being the primary contact for AUSTRAC
- updating your enrolment information in AUSTRAC Online within 14 days of any change.

Your AML/CTF compliance officer must have the authority, independence and resources to do their job effectively. This may include access to all areas of your business and the capability to train and direct staff.

The AML/CTF compliance officer may delegate certain duties to other employees but should retain responsibility for implementing and assessing the ongoing operation of the business's AML/CTF program.

Who can be an AML/CTF compliance officer

Your AML/CTF compliance officer must meet eligibility requirements. This includes being:

- employed or engaged at management level
- a resident of Australia
- a fit and proper person.

Management level depends on the size and structure of the business.

- In larger pubs and clubs, this may be a general manager, operations manager or compliance manager.
- In smaller venues, this may be the business owner, a director or another person with sufficient authority to manage AML/CTF compliance. A person may be at management level without having direct reports.

For smaller businesses, the AML/CTF compliance officer role may be incorporated into the duties of another role. Larger businesses with larger volumes of business and EGMs may require additional resources for AML/CTF compliance activities.

Your AML/CTF compliance officer doesn't need to be an employee. If you engage an external compliance officer, they must have sufficient authority, resources and expertise to perform the role.

You must also assess whether the person meets **fit and proper person** requirements, regarding their competence, integrity and any conflicts of interest. The AML/CTF compliance officer doesn't need to be an AML/CTF expert at the time of appointment but must be capable of understanding the ML/TF risks that your business may reasonably face, sector-specific ML/TF risks, and applying appropriate AML/CTF policies.

Visit the AUSTRAC website to learn more about [AML/CTF compliance officer eligibility and fit and proper person requirements](#).

We expect you to periodically reassess your AML/CTF compliance officer. If your compliance officer becomes ineligible or leaves the business, you must appoint a replacement within 28 days and notify AUSTRAC of the new compliance officer within 14 days of them being appointed.



When your AML/CTF compliance officer is absent

You must always have someone fulfilling the functions of an AML/CTF compliance officer and inform AUSTRAC of who you designate to this role. If your compliance officer is absent from the business, the responsibilities and functions of their role must be covered by appointing a new compliance officer.

Short term absences may not require you to designate a new compliance officer, as their role is overseeing and coordinating compliance – they don't need to fulfil obligations personally like the senior manager.

It's a good idea to identify which other employees could be your compliance officer, so you can quickly designate a replacement if the compliance officer becomes ineligible or is absent for a long period.

Example: combined roles in a small hotel with EGMs

A small country hotel has a gaming room with 20 EGMs. The hotel is a family run business that has a venue manager, Jill, and a food and beverage manager, James.

Due to the small size and low complexity of the hotel, it isn't practical to appoint separate individuals to each AML/CTF governance role. The hotel decides that Jill will perform the roles of senior manager and AML/CTF compliance officer. The business owner retains responsibility as the governing body.

To effectively manage both responsibilities, and ensure effective oversight, the hotel:

- documents Jill's responsibilities
- establishes clear reporting arrangements
- schedules regular reviews of AML/CTF compliance matters by the governing body.



Visit the AUSTRAC website to learn more about the [governance framework](#) and to download our governance quick guides.

Step 2: identify and assess your risks

You must conduct a risk assessment to identify and assess the ML/TF risks your business may reasonably face. This will inform the AML/CTF policies you must put in place to manage and mitigate the ML/TF risks you've identified.

What is ML/TF risk?

ML/TF risk refers to the potential that a person could exploit your business's vulnerabilities to enable money laundering, terrorism financing or proliferation financing.

You don't have to directly witness a person targeting your business to be at risk of this happening.

Your risk assessment obligations

Your risk assessment must be documented, and it must identify and assess the ML/TF risks your business may reasonably face in providing its designated services. The assessment must cover both when you provide a designated service and when you plan to provide designated services.

Follow these 3 steps to conduct your risk assessment:

1. Identify your inherent risks – understand the types of risks you may reasonably face.
2. Assess your inherent risks – understand the scale of each risk and the likelihood and impact of the risk occurring.
3. Evaluate and prioritise your risks – provide your business with a framework of how to prioritise and address risk.

Identify your inherent risks

Your risk assessment must consider ML/TF risks arising from:

- your kinds of customers
- your kinds of designated services
- your delivery channels
- the countries you deal with.

You must also assess any planned designated services, customers, delivery channels or countries that could increase ML/TF risk. In addition, you must consider any new or emerging technologies which could expose your business to sudden risks.

When identifying your inherent ML/TF risks, consider the following:

Your kinds of customers	• What kind of customers frequent your business and what's the source of their funds? For example, are they business owners, salaried workers, tradespeople, retirees, students, frequent or infrequent patrons, members of the club, do they live locally or interstate or are they overseas visitors? • Do most of your customers play with membership or pre-commitment cards, or is most of the play uncarded? • How long are your customers present in the venue? Is the amount of time that they're present unusual given their declared occupation (where known)? • For clubs, are there different ML/TF risks posed by members, compared to customers that are a visitor or guest of a member?
Your kinds of designated services	• How can these designated services be exploited by criminals? • Do you provide any other designated services other than EGMs? • How many EGMs and MTGMs are you licensed to operate?
Your kinds of delivery channels	• Is a particular service provided face-to-face (such as issuing a cheque) or non-face-to-face (such as paying out winnings via a CRT)? • Do you use Ticket In Ticket Out technology (TITO) or cashless cards, and how might these be exploited by criminals? • What is the maximum cash a customer can insert into an EGM/MTGM or CRT at a single time? • Do you have a high proportion of high value EGMs at a particular venue?
The countries you deal with	• What countries are your customers residents of? While pubs and clubs don't tend to deal in or with other countries when providing designated services, your ML/TF risk exposure can still be influenced by where your business operates within Australia. For example, you may wish to consider factors such as: • whether there are known common crime types in your locality • whether there are known issues with loan sharking in your locality • whether you operate multiple venues, and whether those venues pose different risks due to their location or operating environment.

AUSTRAC information on ML/TF risks

You must consider information that we communicate that identifies or assesses ML/TF risks relevant to you. This includes:

- national risk assessments
- indicators of suspicious activity
- direct or indirect communications from us.

Keep in mind, the national risk assessment's sector risk rating reflects AUSTRAC's assessment of the average ML/TF risk across pubs and clubs, relative to the broader regulated population. This doesn't mean that your business's ML/TF risk necessarily aligns with this sector-wide rating.

We may also provide feedback directly to you or your sector on relevant ML/TF risks.

We expect that you maintain a register to show that you've considered the information we've communicated. Below is an example of a register you could use to document consideration of our communications:

Relevant information from AUSTRAC	Date communicated	Why is the information relevant?	What changes were implemented and how?	Date information was considered or implemented	Name and role of individual completing review
New indicators of suspicious activity for pubs and clubs added to AUSTRAC website	DD/MM/YYYY	Contains information about new risks within our industry	Risk assessment and ongoing CDD procedures updated to capture new risks	DD/MM/YYYY	John Doe – AML/CTF compliance officer

Other information to consider in identifying your risks

We expect you to consider other information and data that could help identify and assess your ML/TF risks. This may include information from internal and external sources.

For pubs and clubs, this may include qualitative and quantitative information such as:

- data on trends in the use of your products, services or channels
- customer information relevant to ML/TF risk
- internal feedback, workshops or insights from staff and stakeholders, including those who interact with customers, work in compliance roles or conduct audits
- reports or guidance from industry bodies
- reports from relevant state and territory gaming regulators and the Australian Sanctions Office
- trends identified through suspicious matter and transaction reporting data
- local crime data
- findings from AML/CTF reviews and independent evaluations.

Proliferation financing risk

Your risk assessment must assess the risk of proliferation financing. However, you don't need to develop separate policies to address proliferation financing risk if you've assessed that your:

- proliferation financing risk is low
- AML/CTF policies appropriately manage your inherent risk of proliferation financing.

However, you must still document your proliferation financing risk assessment within your AML/CTF program.



Visit the AUSTRAC website for a comprehensive [definition of proliferation financing](#).

Assess your identified risks

Once you've identified your inherent ML/TF risks, you must then assess these risks. We expect you to consider how easily criminals could exploit the risk categories you've identified to facilitate ML/TF, including how each risk category:

- could be exploited to conceal a person's identity or source of wealth or source of funds
- is easy to access and use
- allows value to be raised, moved or stored
- is known to be exploited by criminals or is a common channel for ML/TF.

A good starting point for you to look at is our risk products to help you determine how to assess your risks. For example:

- [the national risk assessment on money laundering](#)
- [the national risk assessment on terrorism financing](#)
- [the national risk assessment on proliferation financing](#)
- [indicators of suspicious activity](#).

We expect that your assessment of each risk be informed and it must be clearly documented.

Method

Your risk assessment could use the following approach to assess the inherent risk for each risk factor.

Start by assessing the risks you may reasonably face without any controls or mitigation measures in place. You could consider using:

- for medium complexity businesses – the likelihood and impact
- for smaller, low complexity businesses – just the impact.

These approaches may not be appropriate for large, high-complexity businesses that have more dynamic risk profiles. These businesses may want to consider more extensive methods to make sure that their risk assessment both:

- appropriately reflects the nature of their ML/TF risks
- can be kept up to date as risks change.

Impact

Impact is the consequence or damage if criminals exploit your ML/TF risks.

When deciding the impact of an ML/TF risk factor, you could break this down into the following:

Impact ratings	Impact of an ML/TF risk occurrence
High	Significant impact – major damage or effect. Serious terrorism or extensive money laundering.
Medium	Moderate level of money laundering or terrorism financing impact.
Low	Minor or negligible consequences or effects.

Likelihood

Likelihood assesses the possibility of a risk occurring within a given timeframe. Example of likelihood ratings:

Likelihood ratings	Likelihood of an ML/TF risk occurring
Very likely	Almost certain to occur or will occur at a high frequency or probability. This might mean it's a known or recurring issue.
Likely	High probability it will occur, but not certain.
Not likely	Unlikely to occur, but not impossible.

Using a risk matrix

If you're a medium complexity business assessing the likelihood of each ML/TF risk, a risk matrix can help you generate a risk rating. You do this by multiplying the likelihood by impact of each risk.

$$\text{Likelihood} \times \text{impact} = \text{inherent risk}$$

Depending on the complexity of your business, you could include more risk levels. However, it should be clear where the cut-off points for low and high risk are. This is central to understanding the nature and impact of the ML/TF risks you identify.

Example of a risk matrix to establish inherent risk:

	Low	Medium	High
Very likely	Medium	High	High
Likely	Low	Medium	High
Not likely	Low	Low	Medium

Using the above matrix, a likelihood of 'very likely' and an impact of 'low' = risk rating of 'medium'.

This is one way you can simplify, visualise and prioritise your ML/TF risks. You can use any other approach more suitable to your business's requirements.

We expect you to include an explanation of the likelihood and/or impact a risk may have.

Evaluate and prioritise your risks

After you assess your inherent risks, you may evaluate and prioritise which require the most attention by deciding how you'll respond based on your risk ratings (low, medium or high).

For pubs and clubs, low risks may be managed through your standard processes, while high risks may require additional controls. These may include:

- increasing monitoring of gaming activity and payments
- regularly reviewing records of cheques paid out
- applying closer scrutiny to unusual or inconsistent gaming patterns
- reconsidering whether to continue providing a designated service to a customer.

This process will help you to allocate your resources effectively and will help make sure your mitigation measures are appropriate and proportionate to the nature, size and complexity of your business and targeted to your risks.



Visit the AUSTRAC website to learn more about [how to identify and assess your risks](#), including a risk assessment table and additional methods of assessment.

Step 3: mitigate and manage your risks – AML/CTF policies

Once you've identified and assessed the risk that your services could be exploited for ML/TF, you must then set out your AML/CTF policies in your AML/CTF program. Your AML/CTF policies include policies, procedures, systems and controls to appropriately manage and mitigate the risks you've identified.

To meet this obligation, you must do all of the following:

- tailor and adopt policies, procedures, systems or controls that are required under the Act and Rules to address your ML/TF risks
- develop and maintain policies and any further procedures, systems and controls that are necessary to manage and mitigate the ML/TF risks you identified in your ML/TF risk assessment.

This will help make sure your business is protected against the specific threats that it's likely to face and can demonstrate compliance with its legal obligations.

To appropriately manage and mitigate your ML/TF risks, we expect your AML/CTF policies to be:

- **Targeted** to the specific ML/TF risks identified in your risk assessment. For pubs and clubs, this means linking your policies and controls to vulnerabilities associated with gaming machine play, cash-intensive environments and payout activity, and describing the actual measures you use to manage these risks.
- **Proportionate** to the level of risk. Higher-risk activities or behaviours should be managed with stronger or additional controls, while lower risks may be managed through simpler measures. This helps make sure your resources are focused where they're most needed.
- **Ongoing**, as ML/TF risks can change over time. AML/CTF policies should support regular monitoring and reassessment and include clear steps for reviewing and updating controls when there are changes to your business, operations or risk profile.
- **Effective in practice**. This means they must operate as intended and be reviewed and updated where they aren't working as expected.

For example, some appropriate policies for pubs and clubs may include:

- how you monitor EGM play for known money laundering typologies
- how you monitor and manage the risks associated with CRTs (if you have them at your venue)
- the circumstances in which you'll seek to understand the customer's source of funds and source of wealth
- how you identify higher-risk customers and manage and mitigate the risk they pose
- how your board and senior management take accountability for AML/CTF obligations and oversee ML/TF risks
- how you obtain compliant, independent reviews that test the effectiveness of your AML/CTF program, policies and operational framework.



You may face civil penalties if you don't adopt and maintain AML/CTF policies that appropriately manage and mitigate your ML/TF risks.

Meeting your AML/CTF obligations

For businesses with entitlements under licence to operate 16 or more EGMs, your AML/CTF policies must set out how you will comply with all your AML/CTF obligations.

Your key obligations are summarised in the list below:

- You must enrol with us and keep your details up to date.
- You must have and comply with an AML/CTF program, which includes:
 - conducting a ML/TF risk assessment
 - developing and maintaining AML/CTF policies
 - documenting and obtaining senior management approval of your AML/CTF program
 - reviewing and updating your AML/CTF program
 - making and keeping records
 - conducting independent evaluations of your AML/CTF program.
- You must appoint an AML/CTF compliance officer, identify your governing body and senior managers and make sure they can fulfil their responsibilities.
- You must train and conduct due diligence on your personnel to make sure they can meet your AML/CTF obligations.
- You must report to us, in the form of:
 - suspicious matter reports (without tipping off)
 - threshold transaction reports³
 - annual compliance reports.



Visit the AUSTRAC website to learn more about [AML/CTF policies](#).

³ A TTR applies only when a **single** cash transaction of \$10,000 or more is conducted. State and territory restrictions on cash payouts for gaming machine winnings mean most venues won't conduct a transaction of this size; **therefore, it won't trigger a TTR**. It's important to note that a TTR isn't triggered by aggregating multiple smaller payouts made throughout the day.

Step 4: review and update your AML/CTF program

Reviewing and updating your AML/CTF program helps you identify and assess your ML/TF risks as they change over time. It also helps you adopt and maintain AML/CTF policies that appropriately manage and mitigate those risks.

You must regularly review your risk assessment to make sure it's current, as well as the AML/CTF policies you have put in place to make sure they're working effectively to manage and mitigate your ML/TF risks.

Review and update your ML/TF risk assessment

You must review your risk assessment at least once every 3 years, and whenever there's a significant change to any of the following:

- your kinds of designated services
- how you deliver your designated services
- your kinds of customers
- the countries you deal with
- any new or emerging technologies related to your designated services or how you deliver them.

Different review and update requirements apply for your risk assessment if there's a significant change. For example, if a significant change is within your control, you must review and update if required before the significant change occurs.

Below are examples of significant changes that might trigger a review:

- the number of EGMs you offer changes, or a new type of gaming product, such as multi-terminal EGMs is introduced
- you adopt new EGM technology, such as TITO or cashless cards
- you introduce CRTs or the number of cashier locations changes
- there has been an influx of customers who use your EGMs
- the purchase of a new hotel by an existing hotelier or group
- the amalgamation or merger of 2 or more existing clubs
- changes to the demographic of the local area or your clients
- changes to relevant state or territory gaming legislation, such as prize payment limits
- game play monitoring identifies unusual ongoing patterns of activity across your customers.

You must also conduct a review if either:

- we communicate information to you or the gaming sector that identifies or assesses risks associated with the provision of gaming services you provide
- an independent evaluation report has adverse findings about your risk assessment.



You may face civil penalties if you don't review and update your risk assessment as required.

You must make and keep records that are reasonably necessary to show you're compliant with your obligations.



Remember to:

- review and update your AML/CTF program in response to AUSTRAC communications and mandatory triggers
- review your risk assessment at regular intervals, at least every 3 years, to make sure it's current
- review your risk assessment and controls when you have a significant change to your business
- have clear accountability for who will take action following an updated risk assessment.

Review and update your AML/CTF policies

You must review and, if required, update your AML/CTF policies in any of the following circumstances:

- at a minimum, at least once every 3 years
- following a review of your risk assessment
- following an independent evaluation report that contains adverse findings in relation to your AML/CTF policies.

Your AML/CTF policies must set out how you'll review and update your policies when required. These policies must be appropriate to the nature, size and complexity of your business, and appropriately manage and mitigate the ML/TF risks your business may reasonably face.

You must document the updates to your AML/CTF policies in your AML/CTF program within 14 days after making the update. This means you must record these updates in writing, along with the dates that these changes were made.

Once you complete your review and update, we expect that you communicate and implement any updates to your AML/CTF policies across your business.

Example: AML/CTF program must fit the business

You're best placed to identify and assess the risks your business faces, and to tailor your AML/CTF program to meet the nature, size and complexity of your business.

For example, a smaller venue that has 20 EGMs may have AML/CTF policies that rely on manual review of customer transactions and the venue's cheque register to manage some of the ML/TF risks that it faces. A larger venue may have a different risk profile given its size and potentially the complexity of its EGM service provision. As such, the larger venue may adopt additional AML/CTF policies and controls, such as automated transaction monitoring, and allocate additional resources to managing and mitigating its ML/TF risks.



Key considerations:

- Regularly review and update your AML/CTF program, including both your AML/CTF policies and risk assessment at least once every 3 years, to make sure they remain up to date and effective.
- Promote a culture of compliance.
- Obtain senior management approval of your AML/CTF program, with the governing body providing oversight.
- Have a regular independent review of your AML/CTF program. At a minimum, at least once every 3 years.
- Make sure your AML/CTF policies cover initial and ongoing training for staff who perform AML/CTF functions.
- Make sure you make and keep records that are reasonably necessary to demonstrate compliance, including AML/CTF program records, CDD records and transaction records relating to designated services.
- Develop clear handover procedures for when there's a change in your AML/CTF compliance officer.

Customer due diligence

Customer due diligence (CDD) involves understanding who your customers are before you start providing them with designated services, and throughout the course of a business relationship.

There are 4 kinds of CDD:

- initial
- ongoing
- simplified
- enhanced.

Summarised information on CDD is provided in this guide, with detailed explanations available on the AUSTRAC website.

- You must complete **initial CDD** before you start providing a designated service to your customer. Initial CDD is about identifying your customers and other specified persons and identifying your customers' ML/TF risk.
- After you conduct initial CDD, you must monitor your customers so that you can identify, assess, manage and mitigate their ML/TF risks over time. This is called **ongoing CDD**.
- **Enhanced CDD** means taking additional steps to identify your customer and other specified persons, and to identify, manage and mitigate their ML/TF risks. You must conduct enhanced CDD either when the customer's ML/TF risk is high, or in other specified circumstances.
- **Simplified CDD** allows you to streamline customer identification and verification for certain low-risk customers.

You must conduct customer identification procedures when:

- paying out winnings of \$5,000 or more, regardless of how it's paid
- applying ongoing CDD that requires you to identify, assess, manage and mitigate ML/TF risks over time
- applying enhanced CDD that requires you to obtain and verify this information (such as where a customer is high-risk or you have formed a suspicion).

Initial customer due diligence

Once you pay out a customer \$5,000 or more, then your initial CDD obligations apply.

You must complete initial CDD before providing a designated service to a customer. This is to identify the customer and their ML/TF risk before providing a designated service.

Initial CDD helps you to decide what you need to do to manage and mitigate the ML/TF risks involved in providing that customer with a designated service.

The pubs and clubs sector is only exempt from this obligation when **all the below apply**:

- the designated service is provided through an EGM
- the designated service isn't provided at a casino
- enhanced CDD doesn't apply to the customer
- the designated service involves less than \$5,000.

In practice, this means you **must complete initial CDD** when paying out more than \$5,000 to a customer for EGM play, or when enhanced CDD is triggered.

To fulfil your initial CDD requirements, you must establish on reasonable grounds:

- the identity of the customer
- the identity of any person on whose behalf the customer is receiving a designated service
- the identity of any person acting on behalf of the customer, and their authority to act
- whether the customer, any person on whose behalf the customer is receiving the designated service or any person acting on behalf of the customer, is a PEP or designated for targeted financial sanctions
- the nature and purpose of the business relationship or occasional transaction
- the source of funds and source of wealth of foreign PEPs, and high-risk domestic or international organisation PEPs
 - where enhanced CDD is required, the customer's source of funds and source of wealth, if relevant to the nature of the customer's ML/TF risk.

Identifying your customer

You must establish the identity of your customer.

To establish their identity, you could collect information on your customer's:

- full name
- other name(s) (if any) that they're commonly known by. For example, a former name or an anglicised name if the customer has adopted one
- date of birth
- residential address
- unique identifier (if the customer has one). For example, a passport or driver's licence number or a foreign national identity number.

Verifying customer information

We expect you to verify information to establish that the individual customer exists.

To verify your customer's information, you could verify their full name and date of birth. You could verify this information using a:

- current driver's licence
- passport
- proof of age card
- foreign national identity card.

Otherwise, you could verify this information with a primary non-photographic identification document (for example, a birth certificate, citizenship certificate or concession card), and a secondary identification document showing the individual's name and address (such as a utility bill or notice issued by a Commonwealth, state, territory or local government body).

Politically exposed persons (PEPs) and sanctions

As part of your initial CDD obligations, you must establish whether your customer, or any person acting on their behalf or receiving a service on their behalf, is a:

- PEP
- person designated for targeted financial sanctions (TFS).

Collecting PEP information

There are different ways you can establish if a person is a PEP, depending on the size, nature and complexity of your business. For example, you could:

- ask a person if they, a family member or a close associate is a PEP during onboarding and throughout your relationship with the customer
- check the person's background on the internet, including [sanctions lists](#) and other government lists, and on social media
- use databases and reports from third-party providers that specialise in analysing corruption risks.



Visit the AUSTRAC website to learn more about [politically exposed persons](#).

Targeted financial sanctions (TFS)

For TFS checks, you can use the identity information you collected about the customer during initial CDD to conduct a TFS screening.

Visit the AUSTRAC website to learn how to [conduct a TFS screening](#).

If you have information that a person is subject to TFS you **must not**:

- deal with their assets
- provide a designated service without a permit from the Australian Sanctions Office.



Dealing with a sanctioned person's assets may lead to criminal penalties.
Learn more on the [Australian Sanctions Office website](#).

Customer risk rating

Part of your initial and ongoing CDD obligations is understanding the ML/TF risks of your customers. This is different to the process of an ML/TF risk assessment, which identifies broad risks across the business.

Assigning risk ratings in CDD involves determining customer risk on a case-by-case basis based on information available through initial CDD, and risk factors present for that customer identified through ongoing CDD. Information and factors you should consider include:

- the kind of customer
- what kind of designated services you're providing to the customer
- the delivery channels you'll use to provide designated services to the customer
- what countries you'll provide your designated services in or through.

In developing your risk rating system, we expect you to identify risk factors in each of these categories that could impact the customer risk and assign each factor with a rating. These ratings could be as simple as low-, medium- and high-risk customers.

A good method when rating customer risk is using the 'impact' rating in the ML/TF risk assessment as a starting point. We expect you to include your chosen method in your AML/CTF policies, so your staff can assign a risk rating to each customer by:

- checking which risk factors are present for the customer
- balancing the scale of each risk factor present to reach an overall risk rating for the customer
- considering any indicators of unusual or criminal activity that may be present.

Below are some common examples of customer risk ratings.

Low-risk customer:	the customer is an Australian resident seeking a low-risk service through a low-risk channel. No red flags or enhanced CDD triggers are present.
Medium-risk customer:	there are no red flags or enhanced CDD triggers present, but there are some ML/TF risk factors that may have a moderate impact. For example, the customer: • wants a service you've assessed as medium risk • is a low-profile domestic PEP.
High-risk customer:	the customer has high-risk indicators. For example, the customer: • is a foreign PEP • has been involved in criminal activity • has wealth that they can't explain, which is grossly disproportionate in value to their known sources of lawfully obtained wealth • is seeking designated services from you that don't have a clear economic or lawful purpose or reason.

The presence of particular risk factors, and the customer's overall risk rating, will then determine the:

- further KYC information you collect and/or verify (for initial CDD)
- monitoring process (for ongoing CDD)
- need for enhanced CDD measures.

You must establish the risk rating for your customer during initial CDD and continue to monitor them for anything that might trigger a change to their risk rating throughout ongoing CDD.



Visit the AUSTRAC website to learn more about [assigning customer risk ratings for initial and ongoing CDD](#).

Ongoing customer due diligence

You **must** monitor your customers to appropriately identify, assess, manage and mitigate your customer's ML/TF risks over time.

There are 2 key purposes for monitoring your customers on an ongoing basis.

The first is to monitor your customers for unusual transactions and behaviours, and behaviour that may require you to submit a suspicious matter report (SMR) to us.

The second applies to customers you have an ongoing business relationship with. For these customers, you must review and if appropriate update how you identify and assess the customer's ML/TF risk and reverify KYC information relating to the customer.

Your AML/CTF policies must include when and how you'll conduct ongoing CDD. This must be appropriate to manage and mitigate the ML/TF risks you reasonably face in providing your designated services, based on:

- your ML/TF risk assessment
- your customer's ML/TF risks that you identify during initial CDD
- any changes to the customer's ML/TF risk that you identify as they use your services.

Your AML/CTF policies must set out how you'll do all of the following:

- monitor for unusual transactions and behaviours and criminal activity
- review and, where appropriate, update and reverify your customer's KYC information
- review and, where appropriate, update your assessment of the customer's ML/TF risk
- respond to unusual transactions and behaviours and additional ML/TF risks you identify during ongoing CDD
- make sure your ongoing monitoring is working effectively
- keep records that demonstrate how you complied with your ongoing CDD obligations.

Monitoring your customers

Your customer monitoring measures can be manual, automated or both. What's appropriate will depend on the nature, size and complexity of your business, and will be informed by both:

- your identification of their ML/TF risk in initial CDD
- any changes to their ML/TF risk during your business relationship.

We expect your AML/CTF policies for customer monitoring to include processes to:

- effectively monitor and analyse your customers' transactions and behaviour
- capture all relevant sources of customer and transaction data or information
- identify unusual transactions and behaviour
- review and manage the internal escalation and investigation of unusual transactions and behaviour
- manage the consistent reporting of suspicious matters to us
- include sufficient assurance processes to review how your business manages identified issues
- reassess a customer's ML/TF risk and determine if they remain within your risk appetite
- document and audit your monitoring processes.

Reviewing and updating customer's ML/TF risk and KYC information

Your customer's ML/TF risk profile and KYC information may change over time. You must review, and where appropriate, update and reverify, your customer's KYC information at a frequency appropriate to their ML/TF risk.

You must also review, and if appropriate, update and reverify KYC information in certain circumstances, including if any of the following occur:

- you have doubts about whether the information previously collected is adequate or true
- the customer or associated person becomes a foreign PEP
- the customer or associated person becomes a domestic or international organisation PEP, and their ML/TF risk is high.

Your AML/CTF policies must also set out additional circumstances where you'll collect, or collect and verify, additional KYC information in relation to a customer, including details about their source of funds and source of wealth. Triggers could include if:

- your customer seeks a new designated service or product that has a higher ML/TF risk
- there's a sudden and unexplained increase in transaction volumes
- you become aware of potential changes to their KYC information. For example, during interactions with your customer
- there's a change to the way you deliver services to the customer.

You must review and, where appropriate, update your assessment of the customer's ML/TF risk if there's a change to any of the following:

- your business's ML/TF risk assessment which could impact how you identify and assess customer's ML/TF risk
- the type of customer, such as becoming a PEP
- the kinds of designated services you're providing or are asked to provide
- the channels you use to deliver designated services to the customer.

Your AML/CTF policies must set out how:

- often you'll review and update different kinds of customers' KYC information, including the behaviour and triggers that prompt further checks
- you'll make sure you're applying appropriate measures if there's a change to their ML/TF risk.

We expect your AML/CTF policies to describe how you'll identify changes in a customer's circumstances and KYC information that may impact their ML/TF risk.

Enhanced customer due diligence

Enhanced CDD involves taking additional steps to identify your customer, and to identify, manage and mitigate their ML/TF risks.

You must apply enhanced CDD when:

- the customer's ML/TF risk is high
- you're required to submit a suspicious matter report (SMR) in relation to the customer and intend to continue providing a designated service to the customer
- your customer is a foreign PEP or any person they're acting on behalf of is a foreign PEP (for example, if they seek to redeem an EGM payout on someone else's behalf, or if they're part of a syndicate).

You must also apply enhanced CDD when a customer requests a designated service that involves any of the following:

- transactions that are unusually complex or large
- transactions that have no apparent economic or legal purpose
- an unusual pattern of transactions.



While the transaction threshold for conducting initial CDD on a customer is \$5,000, there's no transaction threshold for enhanced CDD. Enhanced CDD must be conducted in the above circumstances, regardless of the value of a transaction, and even when no transaction took place at all.

Example: suspicious incident with no transaction

A customer at a pub separately approaches 3 other patrons playing EGMs, over the course of an hour. The customer offers to purchase their TITO tickets for \$1,000 cash.

An employee at the pub, Alex, notices this and asks the customer if they need any assistance. The customer appears irritable and gives a vague response before walking over to an EGM.

Because the behaviour appears unusual, Alex informs the pub's AML/CTF compliance officer. The compliance officer identifies that the customer's behaviour presents a high ML/TF risk, triggering the need to conduct enhanced CDD.

The compliance officer collects identifying information using CCTV footage and available patron records. The compliance officer then approaches the customer and asks them to leave, in line with the pub's policies around approaching other patrons. This customer's photo is also provided to staff, to prevent them from attending the pub in the future.

Based on the lack of information justifying the customer's behaviour, the compliance officer submits an SMR to AUSTRAC outlining the suspicious approach to patrons, the enhanced CDD undertaken, and the reason for the suspicion. CCTV footage is attached to the SMR.

We expect that your AML/CTF policies will include a range of enhanced CDD measures appropriate to managing and mitigating your customer's ML/TF risks.

It's important that the enhanced CDD measures you apply in each case are informed by the reason why the customer was identified as high ML/TF risk, and designed to manage and mitigate the ML/TF risk.

For example, it may be appropriate to apply one or more of the following enhanced CDD measures:

- collecting and/or verifying more KYC information about the customer
- collecting and/or verifying information about the customer's source of funds or source of wealth
- conducting more in-depth customer monitoring and analysis of transactions and behaviours
- increasing the frequency of reviews of the business relationship, to assess whether the customer's risk has changed and whether the risk remains manageable
- updating the customer's KYC information more frequently than you would for other customers.



You must establish the customer's source of funds and source of wealth on reasonable grounds as part of initial CDD, when it's relevant to the nature of their high ML/TF risk.

When you're carrying out enhanced CDD, we expect you to take active steps to manage and mitigate any ML/TF risks, rather than just undertaking additional monitoring.

For example:

- deciding not to provide a designated service where this falls outside your business's risk appetite
- where you're exposed to high-value cash transactions – implementing a transaction limit for physical currency or requesting customers complete transactions through bank transfer or EFTPOS only.

You may also need to escalate issues for further decision by your senior management in accordance with your AML/CTF policies.

Example: enhanced CDD in practice

A club's ongoing customer monitoring includes the review of patrons' EGM play on a weekly basis. A review of the previous week's carded gameplay reveals one of the club's regular patrons has a substantial increase in the amount they're gambling.

The club's AML/CTF program outlines that sudden increases of this nature are considered high risk, therefore triggering enhanced CDD.

As the customer's source of funds and source of wealth is relevant to the nature of their high ML/TF risk, the club must establish the customer's source of funds and source of wealth on reasonable grounds.

In line with the club's enhanced CDD policies, the AML/CTF compliance officer, Jennifer, reviews information the club holds about the customer's source of funds and source of wealth. Jennifer checks the information the customer provided in their membership application, which states they work in a medium-wage job, which doesn't line up with the amount of increased gaming activity. Jennifer confirms the occupation listed aligns with what gaming floor staff know about the customer, and that no one has further information on other sources of funds or sources of wealth.

Jennifer conducts open-source searches to see if there's any public information about the customer's employment profile, or whether the customer comes up in any adverse media. After finding no further information, Jennifer flag's the customer's account. She notifies the gaming floor managers that they must speak to the customer on their next visit to collect and verify information about the customer's source of funds and source of wealth.

On the customer's next visit, the gaming floor manager, Alvin, speaks to the customer and asks them for more information. The customer says they've recently sold shares from an investment and emails across a statement to verify this. Alvin documents the conversation, along with the supporting statement, and reports this to Jennifer.

Considering the information available, Jennifer is satisfied that the customer's increased gameplay is explained but decides to do more in-depth customer monitoring and transaction analysis for the next month.

Jennifer completes the club's records of the high-risk circumstances, enhanced CDD measures undertaken, information collected and verified, and the decision to increase the club's monitoring and transaction analysis for this customer.

Simplified customer due diligence

Simplified CDD allows you to streamline customer identification and verification for certain low-risk customers.

It isn't an exemption from your initial or ongoing CDD obligations, however. You must still collect all the required KYC information and collect/verify enough KYC information to identify the customer's ML/TF risk and establish matters on reasonable grounds.



Visit the AUSTRAC website to learn more about [customer due diligence](#).

Personnel due diligence and AML/CTF training

Personnel due diligence

You must conduct personnel due diligence to assess the people you employ or engage to perform AML/CTF roles. This also includes people you otherwise engage, for example contractors or consultants, volunteers and people employed by service providers you use.

As part of this, you must assess the person's skills, knowledge and expertise relevant to their AML/CTF responsibilities, as well as their integrity. This must be done before you employ or engage the person, and on an ongoing basis during their employment or engagement.

Assessing a person's skills, knowledge and expertise means checking that they can carry out the AML/CTF responsibilities of their role. This includes determining whether they can understand your business's ML/TF risks and AML/CTF obligations, and apply your AML/CTF policies effectively. To do this, you might:

- conduct interviews for the role
- consider prior qualifications or experience
- seek evidence of their previous performance.

Integrity assessments make sure that individuals uphold ethical standards and don't pose an undue risk to your AML/CTF compliance. To assess their integrity, you might:

- verify their identity
- request police or bankruptcy checks
- screen them for adverse media
- seek reference checks from previous employers.

Some roles in your business have a higher ML/TF risk than others. For example, a staff member working on the gaming floor may not require as much personnel due diligence as your AML/CTF compliance officer responsible for overseeing the effectiveness of the entire AML/CTF program. We expect that the level of due diligence will be tailored to the person's role and the ML/TF risks associated with it.

Ongoing personnel due diligence

As well as doing due diligence when a person is first hired, you must also carry out ongoing personnel due diligence to make sure people continue to have the skills, knowledge, expertise and integrity needed to meet your AML/CTF obligations.

We expect you to make sure the frequency and scope of reassessment is in line with the person's role, including associated ML/TF risks and their skill, knowledge and expertise requirements.

Trigger-based reassessment

We also expect you to make sure your AML/CTF policies outline when you'll conduct personnel due diligence in response to certain triggers. For example, if:

- the person's responsibilities or role change
- their existing role becomes exposed to more ML/TF risk
- there is a change in the person's circumstances relevant to their integrity or suitability.

Your AML/CTF policies must ensure you conduct initial and ongoing personnel due diligence.

We expect your AML/CTF policies to outline how you'll:

- assess roles that need personnel due diligence
- make sure personnel due diligence is appropriate to the risk associated with the role
- make sure personnel due diligence is appropriate to the seniority of the role
- develop procedures to assess and make sure an individual has the skills, knowledge and expertise to perform their AML/CTF functions
- conduct checks to assess the integrity of personnel, including background checks where appropriate
- schedule frequency and triggers for periodic reassessment to make sure ongoing suitability
- respond to adverse assessments
- document all assessments and decisions reasonably necessary to demonstrate compliance.

If a person doesn't meet your integrity, knowledge, expertise and skills requirement, we expect you to take appropriate action, which may include:

- Low-level integrity concern: you may monitor them more frequently or move them to a lower-risk role.
- Significant risk or integrity concern: you may consider removing them from their AML/CTF duties.
- Employee fails to comply with your AML/CTF policies: depending on the severity, you could make them conduct mandatory training to address the concerns, issue a formal warning, take disciplinary action or remove them from their AML/CTF duties.
- Insufficient skills to perform their role: you may need to replace them with someone who has the required skills if they can't be sufficiently trained.

AML/CTF training

You **must** provide AML/CTF training to your personnel, including your governance personnel and contractors who are involved in performing AML/CTF functions on your behalf.

This is to make sure they understand:

- your business's AML/CTF obligations
- your ML/TF risks
- procedures and policies they must follow to manage and mitigate your ML/TF risks.

You **must** provide training when a person is employed or engaged, and that's ongoing throughout their employment with you.

The AML/CTF training you provide must be tailored to the person, their role and the responsibilities and ML/TF risks relevant to their role. For example:

- All personnel in customer-facing roles need an awareness of indicators of suspicious activity and your reporting procedures.
- Personnel responsible for undertaking enhanced CDD and investigating suspicious matters need a deeper understanding of the ML/TF risks your business faces and procedures they must follow.

You have flexibility to choose the type of training you provide based on your ML/TF risk, resources and the roles and responsibilities of your personnel. Common delivery methods can include:

- online training courses or certifications
- in-person training courses
- on-the-job training, especially if there's a ML/TF risk specific to certain roles
- review of publications on current/relevant AML/CTF issues
- participation in industry events or seminars
- regular communication with employees by email, intranet updates or newsletters. For example, about updates to your ML/TF risks or AML/CTF policies
- informal education, such as day-to-day supervision, mentoring and peer review.

If you engage the services of a third party to provide AML/CTF training to your staff, it's important that you make sure the training is specific to your business and its ML/TF risks. Avoid relying on generic training not specific to your industry without first assessing if it's appropriate for your business and adapt it as needed. You remain responsible for making sure training is tailored, appropriate and understandable to your personnel. You may also need to supplement it with role-specific training and content specific to your business and industry.

We expect you to periodically assess and continuously monitor the effectiveness of your training, updating it where necessary.

Your policies must ensure the training you provide is tailored and appropriate to the person, based on the functions they perform and the ML/TF risks relevant to their functions, as well as their specific responsibilities under your AML/CTF policies. We expect your AML/CTF policies to outline how you do the following:

- develop a training plan and schedule tailored training to different roles and their relevant ML/TF risks
- include updates on AML/CTF regulatory changes and emerging risks in training materials
- include steps taken to make sure your personnel are getting training
- use a register to record completion dates and track when further training is due
- monitor the effectiveness of your training
- evaluate if personnel are retaining knowledge from your training and applying it appropriately.



Visit the AUSTRAC website to learn more about [personnel due diligence and training](#).

Suspicious matter reporting

Submitting suspicious matter reports (SMRs) to AUSTRAC alerts authorities to potential money laundering, terrorism financing, proliferation financing and other serious crime. They play an important role in protecting your business, your customers and the community, and are a vital piece of the puzzle for law enforcement investigations.

It's critical that your staff are trained to recognise indicators of criminal activity and know your business's procedures for escalating potential suspicious matters.

Reporting SMRs to AUSTRAC doesn't indicate that your business is involved in ML/TF. In fact, reporting SMRs shows that you're vigilant and have procedures in place to protect your business, patrons and community from criminal activity.

When you must submit an SMR

You must submit an SMR if you suspect, on reasonable grounds, that:

- information you have may be relevant to a crime
- a customer, future customer or a person acting on their behalf isn't who they claim to be
- a person is planning an ML/TF offence using a designated service.

This includes where you suspect on reasonable grounds you have information that concerns:

- money laundering
- terrorism financing
- Commonwealth, state or territory offences
- spending proceeds of crime
- offences such as tax evasion.

SMR obligations apply when you start or propose to provide a designated service, for example if someone asks for a designated service. The obligation applies even if you don't end up providing the designated service to your customer.

You must also submit an SMR even if you can't identify the suspected offender or victim.

You don't have to be sure that a crime is being or has been committed, however your suspicion must be based on reasonable grounds. 'Reasonable grounds' means that a reasonable person in your position would form a suspicion based on the facts, circumstances and information available. This includes all the information and circumstances that you know or could reasonably be expected to have known at the time.

Multiple suspicions about a customer

You must submit an SMR to us each time you form a new suspicion on reasonable grounds. This applies even if you've already reported someone.

You should include reference numbers for any previous SMRs on the same customer. This helps us identify patterns of behaviour and activity.

For example, you might submit a report because you suspect on reasonable grounds that a customer is money laundering or evading being reported to AUSTRAC by repeatedly collecting winnings just below the \$5,000 initial CDD threshold. If the customer returns to request further transactions that raise reasonable grounds for suspicion, submit a separate SMR and include the reference number for any previous related SMRs.



While you don't have to end your relationship with a customer if you submit an SMR, you must appropriately mitigate or manage any ML/TF risks. Submitting SMRs to AUSTRAC doesn't mitigate or manage ML/TF risks.

How long do you have to submit your SMR?

- SMRs about **terrorism financing must be submitted within 24 hours** of forming the suspicion.
- SMRs about **any other matter must be submitted within 3 business days** after the day of forming the suspicion.

Steps to follow when identifying a suspicious matter

Your AML/CTF policies must set out the steps your venue will take when you identify a suspicious matter. These steps help ensure your business recognises, reviews and reports suspicious activity within the required timeframes.

1. **Identify suspicious activity:** train your personnel to recognise suspicious activity and monitor for unusual transactions and customer behaviour that may require you to submit an SMR.
2. **Review material:** conduct timely reviews of material relevant to a suspicious matter, such as indicators of suspicious activity and alerts generated by your transaction monitoring program.
3. **Decide if there are reasonable grounds for the suspicion:** you must do this as soon as practical.
4. **Submit:** SMRs within the required timeframe, as discussed in the previous section.

To make sure your submissions are timely, we expect your AML/CTF policies to:

- outline how you'll train personnel to recognise suspicious activity and follow reporting processes
- include processes to prioritise reviewing and responding to alerts from your monitoring program according to the level of risk
- include processes for personnel to escalate suspicious activity for internal review
- specify personnel or teams responsible for assessing suspicious activity and submitting SMRs.

Possible indicators of suspicious activity for pubs and clubs

There are many things that could lead you to form a suspicion about a person or their activities. Some examples include:

- cashing out credits with minimal or no gameplay
- redeeming credits using different cashiers or CRTs each time
- only redeeming credits through CRTs to avoid cashiers
- refusing or being reluctant to produce identification upon request
- use of false identification
- gaming in a way that's inconsistent with their profile (for example, customer receives welfare benefits but gambles with or carries substantial amounts of cash)
- sudden large increase in gambling activity inconsistent with customer's profile
- customers exchanging cash or gaming tickets with other customers in circumstances that lack an apparent legitimate purpose, particularly where the individuals don't appear to be associated
- customers loitering in gaming machine areas primarily observing other patrons while undertaking minimal or no gambling activity
- customers arriving at your business with substantial amounts of cash (no ATM use observed)
- customers becoming irate when questioned, or refuses to answer questions
- customers appearing to be nervous when cashing out or requesting a cheque
- multiple sessions of same-day gambling activity
- cash being used has a distinct or unusual odour or is in poor condition
- customers asking for cheques to be written in someone else's name
- customers approaching other patrons to purchase their winning tickets, particularly where a patron has won a jackpot or gaming feature
- customers bringing in a large quantity of cash to be exchanged at the cashier for higher denominations.



While gambling behaviours related to superstitious play are common in some communities, they can also align with indicators of money laundering.



Visit the AUSTRAC website for further [indicators of suspicious activity](#) for the pubs and clubs sector.

Writing your grounds for suspicion

Your SMR must include a description of the grounds for your suspicion. An effective grounds for suspicion clearly explains:

- a summary of your suspicion
- what suspicious activity you believe is or has occurred
- what led you to form the suspicion.



Tips for writing a good grounds for suspicion:

- provide a high-level summary of the suspicious activity or indicators in the first sentence
 - provide a chronological sequence of events
 - provide other background to the suspicious activity, including the ‘who, what, where, when, why and how’:
 - who – the persons involved, both individuals and non-individuals and their involvement
 - what – the types and purpose of designated service involved and suspicious activity
 - where – where the activity took place
 - when – times and dates of the activity
 - why – your reason for suspicion and crime type you believe may be involved
 - how – you believe the activity is conducted
 - include as much detail as possible and avoid any terms someone outside your business or sector may not understand.
-

Tipping off

It’s a criminal offence to disclose certain types of information to another person, where it would or could reasonably be expected to prejudice an investigation. This is called tipping off.

Prejudicing an investigation means doing something that would or *could* negatively affect an investigation, such as telling a customer that you have formed a suspicion about their activity or that you have submitted an SMR to AUSTRAC.

Asking the customer for more information, including about their identity or what their source of funds is, is unlikely to be considered tipping off. However, you should take care when seeking further details to avoid tipping off.

Deciding to exclude a customer or suspend or withdraw their membership (or refuse to renew their membership) is unlikely to amount to tipping off unless you tell the customer this is because you have formed a suspicion or submitted an SMR.

AUSTRAC’s [tipping off guidance](#) includes examples of suitable reasons for undertaking enhanced CDD and deciding to end the business relationship, that are unlikely to breach the tipping off prohibition.

Use our [quick guide](#) to help staff in pubs and clubs reduce the risk of tipping off during enhanced CDD.

Advising law enforcement and regulatory agencies

If a law of the Commonwealth, a state or a territory requires you to disclose that you have submitted, or are required to submit, an SMR to AUSTRAC, then it's unlikely you'll breach the tipping off prohibition by complying with the requirement of that law.

The tipping off offence also doesn't prevent you from sharing information with Australian law enforcement agencies on a voluntary or cooperative basis. You're permitted to disclose that you've submitted, or are required to submit, an SMR to AUSTRAC, including the information set out in that SMR, to an Australian Government body that has responsibility for law enforcement, such as the Australian Federal Police (AFP), Australian Criminal Intelligence Commission (ACIC), a state or territory police force, the Australian Securities and Investments Commission (ASIC) or the Australian Prudential Regulation Authority (APRA).

If in doubt about whether you're lawfully permitted to disclose SMRs or SMR-related information in compliance with a law of the Commonwealth, state or territory or to a government agency with law enforcement responsibility in the specific circumstances of your case, seek advice from AUSTRAC.

Do you have to stop providing services to a customer if you submit an SMR?

You don't have to stop providing services to a customer because you've formed a suspicion about them. You must follow your business's policies and procedures, considering the risks of continuing to allow your customer to use your business's facilities. If you choose to stop providing services to them, for example by banning them from the business or the gaming area, you must not tell the customer you have formed a suspicion or that you've reported an SMR to AUSTRAC. If banning a customer, you may need to consider other obligations and the rights of the customer.

Once you submit an SMR you must apply enhanced CDD if you continue providing designated services to them. This includes undertaking appropriate measures such as seeking information from the customer to clarify and update KYC information or taking reasonable measures to identify the customer's source of funds or source of wealth. You may also seek senior management approval to continue the business relationship with the customer or continue to provide designated services to the customer.

Did you know? SMRs you provide are kept confidential. This is to protect you and your staff.

Example: suspicious activity in a club

David is the duty manager and compliance officer for a club that has a license to operate 50 EGMs. David makes sure all applicable staff at the club have completed their AML/CTF training and that procedures are in place to identify suspicious matters and submit SMRs to AUSTRAC.

A staff member, Sally, has noticed a customer has been inserting large sums of cash into EGMs and subsequently cashing out and requesting a cheque after only a few plays. When the customer requests to cash out, he reluctantly provides identification, appears nervous, avoids eye contact and doesn't appear to want to engage with any of the staff. Sally recalls her AML/CTF training and recognises this customer's behaviour as potentially suspicious.

Following the club's AML/CTF policies, Sally escalates this to David, the duty manager.

As the customer's activity is identified as a high ML/TF risk in the club's ML/TF risk assessment, David is required to undertake enhanced CDD. In line with the club's enhanced CDD policies, David reviews the cheque register and EGM data and identifies that the customer has engaged in this pattern of activity several times over the last few months. To collect further information relevant to the customer's ML/TF risk, David conducts an open-source search on the customer and discovers the customer has recently been charged with drug offences. This prompts David to form a suspicion on reasonable grounds, so he submits an SMR to AUSTRAC with information on the customer's activity and the enhanced CDD undertaken. David then escalates this to the venue's senior manager so they can reassess the customer's ML/TF risk rating and decide whether to continue providing designated services to the customer.



Visit the AUSTRAC website to learn more about [suspicious matter reports](#).

Threshold transaction reports

If your business has entitlements under licence to operate 16 or more EGMs then you have the obligation to submit threshold transaction reports (TTRs) to AUSTRAC, when triggered.

A threshold transaction is when there is a transfer of \$10,000 or more of **physical currency (cash)** (or the foreign currency equivalent) as part of providing a designated service. That means either receiving or paying out \$10,000 or more in bank notes or coins.

Electronic funds transfers and cheques of amounts of \$10,000 **must not** be reported as TTRs, as there is no physical currency component. However, depending on the circumstances such payments may be considered suspicious and reportable as an SMR.

Your state or territory may have laws that limit the amount of physical currency a customer can receive, before a cheque or bank transfer is required.⁴

⁴ This guide should be considered in the context of your respective state and territory laws.

Example: TTR not required

In Victoria, a maximum of \$2,000 can be paid in cash to a customer. If a customer wins \$10,000 or more, under state legislation that entire amount must be paid out as a cheque or electronic funds transfer. Therefore, the business doesn't need to submit a TTR. This is because the transaction doesn't involve \$10,000 or more in physical currency.

A TTR **must** be submitted within 10 business days after the day the transaction takes place.



Visit the AUSTRAC website to learn more about [threshold transaction reports](#).

Annual compliance report

If your business has entitlements under licence to operate 16 or more EGMs then you have an obligation to submit a compliance report to AUSTRAC.

The compliance report is an annual report that includes questions about how you've met your AML/CTF obligations during the previous year. AUSTRAC uses the information you provide in your compliance report to:

- assess how you're meeting your AML/CTF obligations
- ascertain if you need any additional help in meeting your obligations
- improve the education and guidance for your business and industry.

You must submit your compliance report between 1 July and 30 September of each year. Your report will cover your business activities for the previous financial year of 1 July to 30 June.

AUSTRAC will notify you about the compliance report due dates, so it's important that your contact details in AUSTRAC Online are up to date. This includes email addresses for your compliance officer and primary contacts.

There can be penalties for failing to submit your compliance report.



Visit the AUSTRAC website to learn more about [annual compliance reports](#).

Step 5: conduct an independent evaluation

An independent review is an impartial assessment of your AML/CTF program that:

- evaluates how you undertook or reviewed your ML/TF risk assessment against the requirements in the Act, the regulations and the Rules
- evaluates the design of your AML/CTF policies against the requirements of the Act, regulations and Rules
- tests and evaluates whether you appropriately identified, assessed, mitigated and managed your ML/TF risks and complied with your AML/CTF policies.

Your AML/CTF policies must set out the frequency of your independent evaluations, which must occur at least once every 3 years and be appropriate to the nature, size and complexity of your business. We expect you to document the rationale for the frequency of your independent evaluation. This includes the factors related to your business's nature, size and complexity that contributed to the decision.

You must conduct an independent evaluation in addition to your own reviews of your AML/CTF program. In addition to your regularly scheduled reviews, an independent review should also occur where there are material changes to your ML/TF risks, or when feedback is received from AUSTRAC about your business or your industry.

Who can do an independent evaluation

The independent evaluator must be free from relationships and circumstances that could compromise their objectivity and professional judgment.

We expect that your AML/CTF policies set out how you'll determine if an evaluator is both:

- independent
- suitable given your business's nature, size and complexity.

If they're sufficiently independent, an evaluator can be someone who is either:

- internal (for example, a member of an internal audit team)
- external to your organisation.

For an evaluation to be **independent**, we expect that your evaluator:

- has the authority to exercise independent judgment
- be empowered to conduct the evaluation as they see fit
- not be involved in developing, implementing or maintaining your AML/CTF program, systems and controls
- not be involved in assessing your ML/TF risks
- be independent of the work areas they're evaluating. For example, isn't your AML/CTF compliance officer or a member of the compliance team.

There are no mandatory qualifications for the person carrying out the independent evaluation. However, we expect your evaluator to have knowledge of the AML/CTF obligations that apply to your business. We also expect that your evaluator has sufficient experience and knowledge of the pubs and clubs sector, and the ML/TF risks that pubs and clubs reasonably face.

How to conduct an independent evaluation

Your AML/CTF policies must set out how independent evaluations will be conducted, appropriate to the nature, size and complexity of your business.

Your AML/CTF policies must require your independent evaluator to do all the following:

- evaluate how you undertook or reviewed your ML/TF risk assessment against the requirements in the Act, regulations and Rules
- evaluate the design of your policies against the requirements of the Act, regulations and Rules
- test and evaluate whether you appropriately identified, assessed, mitigated and managed your ML/TF risk and complied with your policies.

In practice, this might mean:

- visiting your venue/s
- asking your staff questions about your AML/CTF policies
- engaging with your governing body or senior managers, to understand your governance processes and their effectiveness
- where your AML/CTF policies don't effectively manage and mitigate your ML/TF risks, providing recommendations to make them appropriate, and the rationale that supports those recommendations
- working with you to develop appropriate AML/CTF policies to manage and mitigate your ML/TF risks.

We expect you to make sure your evaluator has access to documents, key personnel and systems to conduct the evaluation, such as:

- your ML/TF risk assessment and AML/CTF policies, and documents about the development of these
- access to relevant staff members and senior managers
- access to records, such as customer identification and transactions
- the results of your own monitoring and reviews of your ML/TF risk assessment and AML/CTF policies
- previous independent evaluation reports.

Responding to an independent evaluation

Your AML/CTF policies must set out how your business will respond to an independent evaluation. This includes how you'll review and, if required, update your ML/TF risk assessment and AML/CTF policies in response to adverse findings.

If your independent evaluation report contains adverse findings about your ML/TF risk assessment, you must review and, if required, update your risk assessment to address any issues. You need to update your AML/CTF policies to reflect the changes in your risk assessment.

If your independent evaluation report contains adverse findings about your AML/CTF policies, you must also review and, if required, update your AML/CTF policies.

Record keeping

Keeping records helps you comply with the law and shows us you're fulfilling your AML/CTF obligations.

Additionally, if your business is misused for ML/TF, your records may help us and other authorities investigate.

Proper record keeping involves creating accurate and complete records, and keeping them for a specific period, usually 7 years.

The AML/CTF records you must keep are:

- AML/CTF program records
- CDD records
- transaction records related to a designated service.

Records may be stored in hard copies or electronically, at your premises or offsite. We expect you to keep records in their original format or the format you usually use.

How long you need to keep records for depends on the type of record:

- AML/CTF program records must be kept from the time the record is made to 7 years *after* the record is no longer relevant.
- CDD records must be kept for 7 years from when either the provision of an occasional transaction is complete, or the business relationship ends.
- Transaction records related to a designated service must be kept for 7 years from the day the record is created.

These record keeping requirements may involve keeping the same documentation as required under state or territory legislation, however the time periods for retention may vary.

All reporting entities must comply with the *Privacy Act 1988*. For more information, contact the [Office of the Australian Information Commissioner](#).



Visit the AUSTRAC website to learn more about [record keeping](#).

Record keeping for pubs and clubs with 15 or fewer EGM entitlements

If your business has entitlements under licence to operate 15 or fewer EGMs, you're exempt from many of the record keeping requirements outlined in the Act. You will however need to keep records of transactions if they relate to a customer playing an EGM.

If a customer gives you any documents relating to designated services you're providing or intend to provide, you must also keep those documents as a record.

You must keep all transaction records and customer-provided documents relating to a designated service for 7 years after the date they're created or provided to you.

These record keeping requirements may involve keeping the same documentation as required under state or territory legislation, however the time periods for retention may vary.

Outsourcing

To help your business understand and meet your AML/CTF obligations, you may choose to outsource some AML/CTF functions to access specialist AML/CTF knowledge and expertise or to manage the cost of compliance.

For example, you may choose to engage an AML/CTF consultant or adviser, or a regulatory technology solution.



If you outsource AML/CTF functions, you remain responsible for complying with your obligations under the Act and Rules.

Generally, your business will remain legally liable for any breach of its AML/CTF obligations, even under outsourcing arrangements. You'll incur any penalty that arises from a breach.

It's ultimately your responsibility to ensure that any third parties your business engages are suitably qualified and experienced to provide products and services that comply with your AML/CTF obligations.

It's critical that any third party you engage can provide you with high quality advice and professional services, including help with your ML/TF risk assessment and AML/CTF program. We expect that you take steps to manage any risks of outsourcing and have appropriate oversight of your providers.



AUSTRAC doesn't endorse or approve AML/CTF advisers or their programs, or regulatory technology solutions. If a third-party provider makes claims that they or their programs are endorsed by AUSTRAC, this isn't the case.

When selecting a third party, you should consider whether they:

- have the AML/CTF experience, training and qualifications necessary to support a business of your nature, size and complexity
- have experience in providing AML/CTF support to the pubs and clubs sector
- simply provide template, off-the-shelf ML/TF risk assessments, AML/CTF policies or solutions; or whether they will attend your venue, ask questions about your systems and controls and provide you with tailored advice.

If a third party isn't sufficiently qualified, they may provide you with services or a product that don't meet your needs. This can have serious consequences.

Where you have engaged a third party, your senior managers, AML/CTF compliance officer and the governing board should have proactive oversight of that engagement to make sure that the product or services being provided meet the requirements of the Act and Rules.

The AUSTRAC website has guidance and a sample checklist to help you can engage outsourced providers effectively:

- [Using outsourcing to help meet your AML/CTF obligations](#)
- [Sample checklist for engaging an outsourced service provider](#)

Section 3: Glossary

The Act

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

AML/CTF Rules

The *Anti-Money Laundering and Counter-Terrorism Financing Rules 2025*.

AML/CTF compliance officer

A designated individual within a reporting entity who oversees and coordinates the entity's day-to-day compliance with the Act, the Rules and associated regulations. The AML/CTF compliance officer acts as the primary point of contact with AUSTRAC on AML/CTF matters and oversees and coordinates the operation and compliance with AML/CTF policies.

AML/CTF program

An AML/CTF program includes:

- A money laundering and terrorism financing risk assessment. This identifies and assesses your money laundering, terrorism financing and proliferation financing risks. We refer to these as ML/TF risks. It's the first step to develop your program and shapes the AML/CTF policies that protect your business.
- AML/CTF policies. These detail the policies, procedures, systems and controls you'll use to manage and mitigate your ML/TF risks. They make sure you comply with your AML/CTF obligations.

Reporting entities must have and comply with an AML/CTF program.

Annual compliance report

A report you submit to AUSTRAC each year that includes questions about how you have met your AML/CTF obligations under the Act, regulations and the Rules.

Designated service

A designated service is a service listed in section 6 of the Act.

Designated services are regulated under the Act because they've been identified as posing a risk for money laundering, terrorism financing and proliferation financing.

You must comply with AML/CTF obligations in relation to your provision of designated services that have a [geographical link](#) to Australia.

Designated services include a range of business activities in:

- financial services
- bullion
- gambling
- remittance
- virtual assets
- real estate
- professional services
- precious metals, stones and products.

A person that provides designated services is a [reporting entity](#).

EGM entitlements

In this guide, we refer to EGM entitlements as any legal authority issued under state or territory law that permits a venue to operate a gaming machine. This includes entitlements for clubs, and operating authorities or entitlements for hotels.

Enhanced customer due diligence

The process of undertaking additional customer due diligence measures in circumstances where:

- there's high ML/TF risk
- a suspicious matter reporting obligation associated with a customer continued to be provided a designated service
- a customer or associated person is a foreign politically exposed person
- a customer or associated person is in a high-risk jurisdiction
- designated services are provided in a nested service relationship.

Enhanced CDD measures may include enhanced customer identification and verification and analysis of transactions.

Impact

The degree of damage or loss that may result if an identified risk occurs.

Independent evaluation

An impartial assessment of your AML/CTF program, which:

- evaluates how you undertook or reviewed your ML/TF risk assessment against the requirements in the Act and Rules
 - evaluates the design of your AML/CTF policies against the requirements of the Act, regulations and Rules
 - tests and evaluates whether you appropriately identified, assessed, mitigated and managed your ML/TF risks and complied with your AML/CTF policies.
-

Indicators of suspicious activity

Behaviours that could lead you to form a suspicion about a person or their activities.

Initial customer due diligence

A process of identifying a customer and assessing their ML/TF risk before providing a designated service, to determine what measures are needed to manage and mitigate those risks.

Inherent risk

The amount of risk that exists in the absence of AML/CTF policies implemented by the reporting entity to manage or mitigate the risk.

Integration

The final stage of the money laundering cycle, in which illicit funds or assets are invested in further criminal activity, 'legitimate' business or used to purchase assets or goods. At this stage, the funds are in the mainstream financial system and appear to be legitimate.

Know your customer information (KYC information)

Any information about a customer that either:

- provides reasonable grounds to establish certain matters required for [initial customer due diligence](#)
- enables you to identify or assess the ML/TF risk of the customer.

KYC information includes both information sourced from the customer and from other independent sources.

For example, the customer may provide KYC information about their identity while you may source other KYC information from searches online or third-party sources.

Layering

The second stage of the money laundering cycle, which involves moving, dispersing or disguising illegal funds or assets to conceal their true origin.

Likelihood

The possibility of a risk occurring within a given timeframe.

Money laundering

Turning the proceeds of crime into funds or assets that seem legitimate.

ML/TF

Money laundering, terrorism financing and proliferation financing.

ML/TF risk

The risks of money laundering, terrorism financing and proliferation financing that a reporting entity may reasonably face in providing its designated services.

Ongoing customer due diligence

The process of monitoring customers and their behaviour over the course of the business relationship, to appropriately identify, assess, manage and mitigate ML/TF risks that the reporting entity may reasonably face in providing designated services.

Ongoing CDD may include by reviewing and updating the customer's risk assessment and KYC information where appropriate.

Personnel due diligence

A framework for assessing a person's skills, knowledge, integrity, and expertise relevant to their AML/CTF responsibilities. This assessment is conducted before employment or engagement and on an ongoing basis throughout their employment or engagement.

Physical currency

Coins and printed money (of Australia or a foreign country) that's designated as legal tender and circulates and is used and accepted as a medium of exchange in the country of issue.

Placement

The first stage of the money laundering cycle, in which illicit funds first enter the formal financial system.

Politically exposed person (PEP)

An individual who holds a prominent public position or role in a government body or international organisation, either in Australia or overseas. Immediate family members and/or close associates of these individuals are also considered PEPs. PEPs often have power over government spending and budgets, procurement processes, development approvals and grants.

The Act identifies 3 types of PEPs.

- Domestic PEP – someone who holds a prominent public position or role in an Australian government body.
 - Foreign PEP – someone who holds a prominent public position or role with a government body in a country other than Australia.
 - International organisation PEP – someone who holds a prominent public position or role in an international organisation, such as the United Nations (UN), the World Trade Organisation (WTO) or the North Atlantic Treaty Organisation (NATO).
-

Proliferation financing

Proliferation financing enables the spread of weapons of mass destruction. It's when a person makes available an asset, provides a financial service or conducts a financial transaction that's intended to facilitate the proliferation of weapons of mass destruction.

Reporting entity

An entity that provides any [designated services](#) listed under section 6 of the Act, or the lead entity of a reporting group. This includes services related to:

- financial services
- bullion
- gambling
- remittance
- virtual assets
- real estate
- professional services
- precious metals, stones and products.

Reporting group

A business group or group of persons that includes one or more reporting entities.

Residual risk

ML/TF risk that remains after a reporting entity has implemented their AML/CTF policies.

Serious offence

Any offence, committed in Australia or overseas, where the punishment under Australian law would be 2 or more years in prison.

Source of funds

Source of funds refers to how and where the funds were obtained from for a specific transaction.

Source of wealth

Source of wealth refers to where the customer's entire wealth and assets come from. This can be from economic, business or commercial activities, along with other circumstance that generated, or significantly contributed to, the customer's overall net worth.

Structuring

Structuring is where a person:

- splits a single transaction into 2 or more transactions with the sole or dominant purpose of avoiding a transaction being reported in threshold transaction reports
- travels with cash or monetary instruments in a way that has the sole or dominant purpose of avoiding cross-border movement reporting. For example, a family asking a child to carry cash so that each individual is under the threshold.

Structuring is an offence under the Act.

Suspicious matter report (SMR)

A report a reporting entity must submit to AUSTRAC when it forms a suspicion on reasonable grounds that:

- information it holds may be relevant to money laundering, terrorism financing or other serious crime
 - a customer or a person acting on their behalf isn't who they claim to be
 - a designated service may be used to facilitate criminal activity.
-

Terrorism financing

The financial support, in any form, of terrorism or of those who encourage, plan or engage in terrorism.

Tipping off

Tipping off is a criminal offence. It occurs when a person discloses certain types of information to another person where the disclosure would or could reasonably be expected to prejudice an investigation. This includes investigations of offences against Commonwealth, state or territory law, and investigations under proceeds of crime legislation.

Threshold transaction report (TTR)

A report submitted to AUSTRAC about a designated service provided to a customer by a reporting entity that involves a transfer of physical currency of \$10,000 or more (or the foreign currency equivalent).



Need something else?

To get updates from AUSTRAC subscribe to [AUSTRAC's newsletter, InBrief](#).

You may also [submit a query online, or contact us](#).

