Australian Government

AUSTRAC

FIGHTING FINANCIAL CRIME TOGETHER

PUBS AND CLUBS WITH GAMING MACHINES

REGULATORY GUIDE

Updated October 2025

CONTACT US

INITIAL CONTACT POINT

Enquiries about AUSTRAC, the legislation we administer or other information may be directed to the AUSTRAC Contact Centre, 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

ATTRIBUTION

WHAT THIS REGULATORY GUIDE IS ABOUT

This guide has been developed for pubs and clubs who have entitlements under licence to operate electronic gaming machines (EGMs), including multi-terminal gaming machines (MTGMs). This guide should be used in conjunction with existing guidance to gain a thorough understanding of your anti-money laundering and counter-terrorism financing (AML/CTF) obligations.

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

Throughout the guide the following terms are used to show the level of compliance required:

- **'must'** indicates a legal or regulatory requirement
- '**should**' is used to demonstrate best practice rather than a legal requirement.

ABOUT REGULATORY GUIDES

Regulatory guides provide detailed information about the compliance requirements for the provision of designated services regulated by AUSTRAC. They include case studies that can be used to inform your understanding of AML/CTF obligations.

CONTENTS

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

WHAT IS MONEY LAUNDERING AND TERRORISM FINANCING?

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 three 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. integration of those illicit funds into the financial system where they appear legitimate.

THE HARM OF MONEY LAUNDERING

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

Criminals rely on money laundering to be able to spend illicit funds, and to fund more illegal activities. The profits from their crimes can fund activities from tax evasion and fraud, to human trafficking and modern slavery. Money laundering can affect the price of goods, can deter foreign investors and impede economic growth. It also diminishes the tax revenue collected by governments and damages the credibility of our financial system and economy.

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 require 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 is estimated that the 2005 London bus bombings cost the equivalent of only a few hundred Australian dollars to carry out.

AUSTRALIA'S ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING LAWS

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) aims to combat money laundering and terrorism financing (ML/TF) in Australia.

The AML/CTF 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 go about meeting its obligations, based on the level of ML/TF risk faced. This is because it is the reporting entity that is best placed to know the ML/TF risks associated with their customers, their products, operating structures and business environment.

ABOUT AUSTRAC AND WHO WE REGULATE

AUSTRAC is Australia's AML/CTF regulator and financial intelligence unit.

AUSTRAC's purpose is to build resilience in the financial system and use financial intelligence and regulation to disrupt ML/TF 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 businesses to ensure they comply with their obligations under the AML/CTF Act
- collecting and analysing the financial data reported by regulated businesses
- 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.

Commonwealth, State and Territory law enforcement agencies investigate criminal activities including those related to possible money laundering.

You can watch videos to understand more about AUSTRAC at: **austrac.gov.au/about-us/austrac-overview**

WHO IS REGULATED BY AUSTRAC?

AUSTRAC regulates businesses in the financial services, bullion and gambling sectors that provide certain 'designated services' listed in the AML/CTF Act. These designated services have been identified as posing a risk for money laundering and terrorism financing.

This includes businesses that are licensed to operate electronic gaming machines (EGMs), including multi-terminal gaming machines (MTGMs). Many such businesses also offer a Totalisator Agency Board (TAB) service to their customers, however the TAB is responsible for meeting the AML/CTF Act obligations associated with this service. The TAB may rely on your business to undertake certain activities on their behalf to assist them in meeting 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) – 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.

LEARN MORE

For more information about reporting please see section two of this guide.

HOW CRIMINALS TRY TO EXPLOIT PUBS AND CLUBS

Proceeds of crime is often in the form of cash, so EGMs can provide an opportunity for criminals to launder 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 spend illicit funds.

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

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

Some examples of how gaming businesses are exploited by criminals 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 observation or monitoring by staff.
- 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.

OBLIGATIONS FOR PUBS AND CLUBS WITH ELECTRONIC GAMING MACHINES

The obligations for your business will depend on the number of EGM entitlements you have under licence to operate (regardless of how many are actually in operation at the time).

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

Did you know?

If your business has entitlements under licence to operate 15 or less EGMs you may be exempt from many obligations, including having an AML/CTF program, customer due diligence and submitting certain reports to AUSTRAC, although you must still enrol with AUSTRAC and report

suspicious matters. To determine if your business is exempt, you must meet the requirements in Chapter 52 of the AML/CTF Rules. If you are unsure, we recommend that you seek independent legal advice.

AML/CTF obligations according to the number of EGM entitlements your business has under licence to operate

Businesses exempt under Chapter 52 of the AML/CTF Rules - (entitlements under licence to operate 15 or less 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 an AML/CTF program • Carry out customer due diligence (Know Your Customer) procedures • Implement and maintain ongoing customer due diligence. • Undertake regular independent reviews of part A of the AML/CTF program • Submit suspicious matter reports • Submit threshold transaction reports • Submit annual compliance reports

EXAMPLE

You are a business with an entitlement under licence to operate 20 EGMs, however you only currently have 12 EGMs available to customers, as the other eight EGMs are in storage. As your entitlement under licence to operate EGMs is 16 or more, the obligations in the right hand column would apply.

WHAT HAPPENS IF YOU DON'T MEET YOUR OBLIGATIONS?

If you fail to meet your obligations, AUSTRAC has a range of enforcement actions available to it.

You are also potentially placing your business and community at greater risk of harm from ML/TF and other serious crimes.

ENFORCEMENT ACTIONS

Enforcement actions can include:

- A remedial direction to take specific actions to comply with certain parts of the AML/CTF Act. Remedial directions are generally made public.
- Infringement notices for contraventions of some obligations, for example:
    - customer identification procedures
    - reporting
    - enrolling with AUSTRAC
    - notifying AUSTRAC of changes to enrolment details
    - making and retaining 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, or
    - provide AUSTRAC with information about how you are complying with your obligations under the AML/CTF Act.
- An enforceable undertaking to AUSTRAC, detailing how you will comply with your AML/CTF obligations.
- Applying for a civil penalty order from the Federal Court of Australia.

LEARN MORE

For more information, go to **austrac.gov.au/consequences-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 from when you first allow a person to play on an EGM.

To enrol your business with AUSTRAC, go to **austrac.gov.au/enrol-register** and complete the AUSTRAC Business Profile Form (ABPF) online form.

On that website page you will find all the details you need to complete your enrolment. It also contains the ABPF explanatory guide which includes instructions on how to complete the form.

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 compliance officer
- contact information (phone number/email)
- address of the registered office
- certain other business information.

Changes to your details must only be updated using the ABPF online form in AUSTRAC Online.

Without up to date details, your business may miss out on receiving important information from AUSTRAC, including reminders and deadlines to provide Compliance Reports to AUSTRAC. Failure to keep your details up to date is a breach of your AML/CTF obligations.

DESIGNATED BUSINESS GROUPS

A designated business group (DBG) is a group of two or more businesses who join together to share the administration of some or all of their AML/CTF obligations (such as an AML/CTF program or record-keeping).

Any member of the group can fulfil some of the obligations for the other members. However each business is still ultimately responsible for meeting its own AML/CTF obligations.

A business can only be a member of one DBG at a time. Businesses must meet certain criteria to be eligible to form a DBG. For example, a DBG could be formed by businesses from related companies where each member is one or more of the following:

- a holding company of another member
- a subsidiary of another member
- a subsidiary of a holding company of another member.

Businesses who want to form a DBG must agree in writing to become members of the group.

LEARN MORE

For more information on Designated Business Groups, go to:
austrac.gov.au/chapter-3-designated-business-groups

CONDUCTING AN ML/TF RISK ASSESSMENT

You must complete a risk assessment to identify the money laundering and terrorism financing (ML/TF) risks your business faces. It's important to conduct a risk assessment so that you can develop systems and controls to mitigate and manage your ML/TF risks and protect your business.

You can watch a short video about risk assessments at: **austrac.gov.au/managing-risk**

WHAT IS RISK?

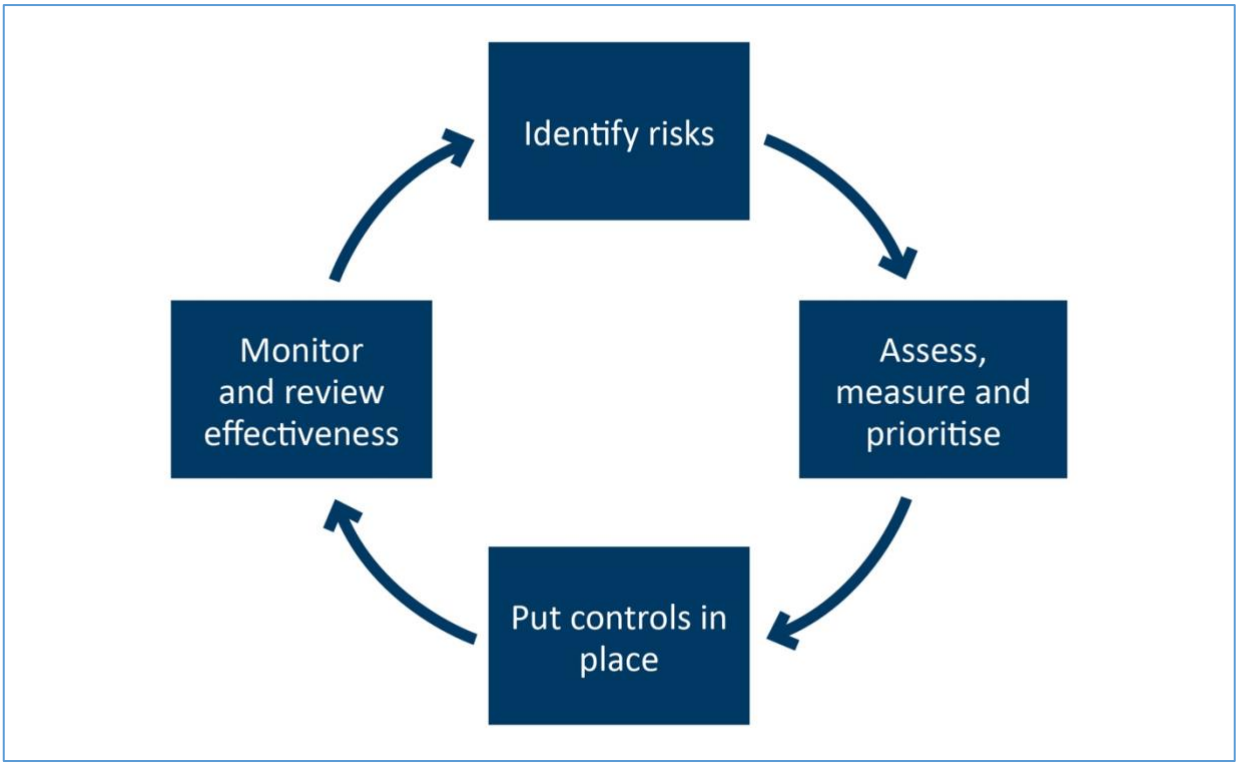
Risk is a combination of:

- the chance that something may happen (likelihood)
- the degree of damage or loss that may result if it does occur (impact).

MANAGING YOUR RISKS

The four basic steps of risk management include:

1. identifying the risks your business reasonably faces
2. assessing and measuring your identified risks
3. applying controls to mitigate and manage your risks
4. monitoring and reviewing the effectiveness of your controls.



1. IDENTIFY THE RISKS YOUR BUSINESS REASONABLY FACES

When identifying your ML/TF and other serious crime risks, consider these factors.

Your customers	• What kind of customers frequent your business and what is the source of their funds? For example are they business owners, salaried workers, tradespeople, students, frequent or infrequent patrons, members of the club, do they live locally or interstate or are they overseas visitors. • Do the majority of your customers play carded or uncarded? • How long are your customers present in the venue? Is the amount of time that they are present unusual given their declared occupation (where known)? • For clubs, are there different ML/TF risks posed by members or customers with an established pattern of play, compared to customers that are a visitor or guest of a member?
The designated services you provide	• How these designated services can be exploited by criminals • Do you provide any other designated services other than EGMs? • How many EGMs and MTGMs are you licensed to operate?
How you provide those services	• 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?
Where your business is located, hours of operation, gaming revenues	• Are there known common crime types in your locality? • Are there known issues with loan sharking in your locality? • Do you operate multiple venues, and do those venues pose different risks?

For larger venues or corporate groups, you should ensure any enterprise risk assessment appropriately assesses the ML/TF risks posed at each individual venue.

Make sure you document your risk assessment and update the document any time you review your risk assessment.

2. ASSESS AND MEASURE YOUR IDENTIFIED RISKS

Each risk needs to be considered, assessed and measured in terms of the likelihood it will occur and the impact (severity or damage) which may result if it does occur. The combination of likelihood and impact will provide you with the overall risk score.

Likelihood x Impact = Risk score

The following is an example of how you might assess and measure risks in your business.

Likelihood

Rate how likely each event is to occur in your business. Three levels are listed below but you can use as many levels as are suitable for your business.

- Very likely: almost certain, it will probably occur regularly.
- Likely: it may occur a few times a year.
- Unlikely: not likely to happen, but not impossible.

Likelihood assessments need to be based on evidence and data that you can provide to AUSTRAC. You should regularly review how often a particular event or risk has occurred in your business to inform this.

Impact

Consider the possible impacts if each event was to occur. Consider the impacts on your business, customers, industry and wider community. For example:

- facilitating crimes that impact your community and the country
- reputational damage if your business is used for criminal purposes
- financial loss from a crime
- the welfare and safety of your staff and customers
- enforcement action by government agencies and investigations by law enforcement.

These examples do not cover every scenario.

Below are three levels of impact or consequence you might use. You can include as many levels as you deem necessary for your business.

- major impact or consequence
- moderate impact or consequence
- minor impact or consequence.

Risk score

One way to determine what the risk score is for each of your identified risks is to use a risk matrix, such as the following example.

Risk matrix

OVERALL RISK SCORE			
	MINOR	**MODERATE**	**MAJOR**
VERY LIKELY	**2** Medium	**3** High	**4** Extreme
LIKELY	**1** Low	**2** Medium	**3** High
UNLIKELY	**1** Very low	**1** Low	**2** Medium

Risk score response

Once you have evaluated and scored each risk, develop responses to the risk scores. The higher the risk, the higher level of response. The appropriate response will differ for each business.

3. APPLY CONTROLS TO MITIGATE AND MANAGE YOUR RISKS

Once you have identified and scored the risks your business faces, your ML/TF risk assessment should then set out the systems and controls you will use to identify, mitigate and manage these risks. These systems and controls should not only refer to your AML/CTF obligations, they should reference the measures you will undertake in practice to identify, mitigate and manage the identified risk. For example, rather than simply stating your controls are "TMP", or "ECDD", you should state "TMP alert to identify minimal EGM play", "ECDD to determine customer's source of funds and source of wealth" etc.

Appropriate systems and controls **must** include:

- the circumstances in which you will seek to understand the source of funds and source of wealth of your customers
- how you will monitor EGM play for known money laundering typologies
- how you will identify high risk customers and then mitigate and manage the risk of those customers
- how you will identify, mitigate and manage the ML/TF risks posed by uncarded play, exposure to cash and CRTs
- how your Board and senior management will engage with your AML/CTF obligations and ML/TF risks
- obtaining compliant independent reviews that include testing the effectiveness of your AML/CTF Program and operational framework.

Example: How you could record your business' risks and controls

RISK EXAMPLE	RISK RATING			POSSIBLE CONTROLS
	Likelihood	Impact	Risk score	
Customer frequently brings cash into the business, inserts into EGMs and collects credits with minimal or no play	Likely	Major	**3**	• staff training on what activity to look out for • ensure staff regularly patrol gaming area • implement a requirement for customers to provide ID for payouts over a certain amount • staff to notify compliance officer and management of any suspicious behaviour • create transaction monitoring rules to identify when this occurs • cheque register reviews • source of funds enquiries • consider barring the customer.
Customer is unable to present identification when seeking to cash out	Likely	Moderate	**2**	• identification checks upon entry or upon large payouts • staff training on what to look out for and clear reporting lines for staff suspicions • refusal to provide designated services without identification.
Customer presents a counterfeit note	Likely	Minor	**1**	• counterfeit detection device • staff training on what to look out for and clear reporting lines for staff suspicions

4. MONITOR AND REVIEW THE EFFECTIVENESS OF YOUR CONTROLS

You must regularly review your risk assessment and the controls you have put in place to ensure they are working effectively to mitigate and manage the ML/TF risks to your business.

There may be certain events that trigger you to review your risk assessment, however you must also review it periodically. Below are some examples of things that might trigger a review:

- you offer additional EGMs or a new type of gaming product, such as multi-terminal EGMS
- adoption of new EGM technology, such as TITO or cashless cards
- introduction of CRTs or additional cashier locations
- there has been an influx of customers who use your EGMs
- changes to the demographic of the local area or your customers
- information received from AUSTRAC or law enforcement agencies, such as new ML/TF risks or typologies
- 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 document your risk assessment in addition to maintaining records of any changes you make.

Remember to:

- review your risk assessment at regular intervals
- document clear processes to mitigate and manage the risks you identify
- have clear accountability for who within senior management will take action following an updated risk assessment.

LEARN MORE: RISK MANAGEMENT RESOURCES

- Implement a risk management process: **austrac.gov.au/risk-management-process**
- Insights: Assessing ML/TF risk: **austrac.gov.au/managing-risk**
- You can search for risk assessment templates on the internet which may be suitable for your business.

AML/CTF ADVISERS

You may also choose to engage the services of an AML/CTF adviser to help conduct your risk assessment and develop your AML/CTF program.

Go to **austrac.gov.au/business/service-providers-reporting-entities/engaging-amlctf-advisers** for more information about AML/CTF advisers, including what to look for when engaging one.

APPOINT AN AML/CTF COMPLIANCE OFFICER

Your business' AML/CTF compliance officer is responsible for making sure you meet your AML/CTF obligations, including:

- driving the compliance culture and promoting the processes and procedures in place to address ML/TF risks
- escalating and remediating any issues of non-compliance and advising the board or senior management of how the business is meeting its obligations
- ensuring the AML/CTF program has been approved by senior management and the board, where applicable
- training staff so that ML/TF risks, and AML/CTF processes and procedures are understood and the business's compliance obligations are met
- submitting reports to AUSTRAC within specified timeframes
- keeping up to date with ML/TF risks in the industry
- regularly reviewing and updating the AML/CTF program and ML/TF risk assessment, and ensuring an independent review takes place at regular intervals
- being the primary contact for AUSTRAC
- updating your enrolment information with AUSTRAC within 14 days of any change.

The AML/CTF compliance officer must be someone who is at management level. They should also have the authority and resources to ensure they can carry out this role effectively. This requires access to all areas of your business, including the board and senior management, the capability to train and direct staff and the authority to deal with any issues relating to your business' ML/TF compliance, such as raising any issues with your board and/or senior management.

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.

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.

EXAMPLE: COMBINED ROLES IN A SMALL HOTEL WITH EGMS

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

Due to the small size of the hotel it is not practical to hire an additional staff member to be the AML/CTF compliance officer. The hotel decides to integrate the role of the AML/CTF compliance officer and venue manager into one position. This makes Jill the venue manager and AML/CTF compliance officer for the hotel.

To effectively manage both responsibilities, the hotel decides to implement a schedule of tasks and reminders of the responsibilities for Jill. This will allow her to manage the AML/CTF obligations and report on AML/CTF matters.

Jill is responsible for North East Hotel complying with its AML/CTF obligations and that its staff have a positive AML/CTF compliance culture.

LEARN MORE

For more information go to: **austrac.gov.au/compliance-officers**

Download the AML/CTF compliance officer's checklist at: **austrac.gov.au/amlctf-governance**

YOUR AML/CTF PROGRAM

Your AML/CTF program must be tailored to the ML/TF risks faced by your business. This is one of the reasons a thorough risk assessment is so important. It helps to protect your business and community from criminal activity. It is your responsibility to ensure that your AML/CTF program effectively mitigates and manages your ML/TF risks.

An AML/CTF program must be a written document that sets out your business's policies and procedures to comply with your AML/CTF obligations.

The systems and controls in your AML/CTF program must be appropriate for the level of risk your business may reasonably face so that you can effectively identify, mitigate and manage the risk of your business being used for money laundering, terrorism financing, or other serious crimes.

WHAT TO INCLUDE IN YOUR AML/CTF PROGRAM

There are two parts to an AML/CTF program.

- **Part A** must include the processes and procedures to help your business identify, mitigate and manage the ML/TF risks it may reasonably face.
- **Part B** sets out your procedures for identifying your customers and verifying their identity.

To comply with your AML/CTF obligations, your AML/CTF program must include:

- an ML/TF risk assessment
- senior management/board formal approval and adoption of the program
- a procedure to appoint an AML/CTF compliance officer
- an employee due diligence program
- a risk awareness training program for your staff
- procedures for ongoing customer due diligence
- reporting and enrolment update procedures
- a procedure for responding to AUSTRAC feedback
- a procedure for independent reviews of the AML/CTF program
- procedures for collecting and verifying KYC information
- a procedure for record keeping.

EXAMPLE: AML/CTF PROGRAM MUST FIT THE BUSINESS

You are best placed to identify and assess the risks your business faces, and tailor your AML/CTF program to meet the specific features, risks and characteristics of your business.

For example, a smaller venue that has 20 EGMs, may have an AML/CTF program that implements a manual review of customer transactions and the venue's cheque register as a control to address some of the 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 implement additional controls, such as automated transaction monitoring, and allocate additional resources to its AML/CTF compliance measures.

Remember to:

- regularly review your AML/CTF program and risk assessment to ensure it is up to date
- promote a culture of compliance
- obtain senior management and board approval of the program
- have a regular independent review of your AML/CTF program
- ensure staff receive initial and ongoing training tailored to their roles
- ensure you keep records of all your AML/CTF programs
- develop clear handover procedures for when there is a change in your AML/CTF compliance officer.

LEARN MORE: ADDITIONAL AML/CTF PROGRAM RESOURCES

- You can download the guide: Preparing and implementing an AML/CTF program: pubs and clubs sector at: **austrac.gov.au/pubs-clubs-amlctf-program**
- AML/CTF programs overview: **austrac.gov.au/amlctf-program-overview**
- You may also choose to engage the services of an AML/CTF adviser to help conduct your risk assessment and develop your AML/CTF program.
- Go to **austrac.gov.au/business/service-providers-reporting-entities/engaging-amlctf-advisers** for more information about AML/CTF advisers, including what to look for when engaging one.

SUSPICIOUS MATTER REPORTING

Submitting suspicious matter reports (SMRs) to AUSTRAC are an important way you can protect your business, your customers and the community from ML/TF and other serious crimes. SMRs are a vital piece of the puzzle for law enforcement investigations.

SMRs are one of the most important obligations for all pubs and clubs with gaming machines.

It's critical that your front line staff are trained to recognise indicators of criminal activity and know your business' procedures for escalating a suspicious matter to their manager or compliance officer for consideration and reporting of the SMR to AUSTRAC.

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

For detailed information about SMRs, including videos, go to: **austrac.gov.au/smr**

WHEN TO SUBMIT AN SMR

You must submit an SMR if you suspect that the customer is not who they claim to be, or the customer or your provision of designated services to the customer is related to:

- terrorism financing
- money laundering
- an offence against a Commonwealth, State or Territory law
- proceeds of crime
- tax evasion.

This also includes prospective customers, regardless of whether you provide them with any designated service.

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 after you have considered all the information and circumstances available, a reasonable person would conclude that an SMR should be submitted.

HOW LONG DO YOU HAVE TO SUBMIT YOUR SMR TO AUSTRAC?

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

WHAT TO INCLUDE IN AN SMR

An SMR should include as much detail as possible about your business, why the matter is suspicious, who the matter relates to, and any transactions or services involved.

Include the following information about the person, if known:

- their full name, address and telephone number
- other names used by the person
- postal address if different from full address
- date of birth
- country of citizenship
- occupation
- email address
- a description of any documents you have used to verify their identity.

If you don't have the person's identity information, include:

- a description of the person
- whether you have any video footage or photographs of the person
- any additional information which could assist to identify them.

LEARN MORE

You can download an SMR checklist and reference guide at: **austrac.gov.au/new-smr-guidance-resources**

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 game-play • 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 is inconsistent with their profile (e.g. customer receives welfare benefits but gambles with or carries substantial amounts of cash) • Sudden large increase in gambling activity inconsistent with customer's profile	• Customer arrives at business with substantial amounts of cash (no ATM use observed) • Customer becomes irate when questioned • Customer appears to be nervous when cashing out or requesting a cheque • Multiple same-day gambling activity • Cash being used has a distinct or unusual odour or is in particularly poor condition • Customer asks for cheques to be written in someone else's name • Customer approaches other patrons to purchase their winning tickets • Customer brings in a large quantity of cash to be exchanged at the cashier for higher denominations

Further indicators of suspicious activity for the pubs and clubs sector can be found at **austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/indicators-suspicious-activity-pubs-and-clubs-sector**

You can download a poster to display at your business to help your gaming staff identify and report suspicious customer behaviour at: **austrac.gov.au/pubs-clubs-staff-awareness**

HOW TO SUBMIT AN SMR

1. Log into your AUSTRAC Online account at **online.austrac.gov.au/ao/login.seam**
2. Click the **+ (plus)** symbol on the left side of Transaction Reporting
3. Click on the **+ (plus)** symbol on the left side of Reports
4. Click **Create/amend reports**
5. Look for the SMR report type and click **Create**.

You can also access SMR guides through AUSTRAC online.

1. Click **Transaction Reporting**
2. Click **AML/CTF Act reporting forms, file specifications and explanatory guides**
3. On the right hand side of the blue table under a heading named Data entry form guides there are two guides which may help you with your SMR submission.

TIPPING OFF

It is 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 *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 not 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) does not 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 ECDD and deciding to end the business relationship, that do not breach the tipping off prohibition: **austrac.gov.au/about-us/amlctf-reform/current-reporting-entities/tipping-off**

Advising law enforcement and regulatory agencies

The tipping off offence does not prevent you from sharing information with State and Territory police and other Australian law enforcement agencies on a voluntary or cooperative basis.

You are permitted to disclose that you have submitted, or are required to submit, an SMR to AUSTRAC, including the information set out in that SMR to State and Territory police and other Australian law enforcement agencies.

If in doubt about whether or not you are lawfully permitted to disclose SMRs or SMR related information in compliance with a law of the Commonwealth, State or Territory or to a government law enforcement agency, seek advice from AUSTRAC. Contact details are included at the end of this guide.

EXAMPLE: RESPONDING TO SUSPICIOUS ACTVITY WITHOUT TIPPING OFF

Mary is the compliance officer for the South Side Club, which has a license to operate 30 EGMs. Mary has noticed that a regular customer, Wayne has been approaching other customers and attempting to purchase their winning gaming tickets. Mary has also seen Wayne carrying a bag and on at least two occasions provided cash from that bag to other customers. Mary believes

Wayne's behaviour is suspicious, so she is required to submit an SMR to AUSTRAC and conduct enhanced customer due diligence.

Mary asked Wayne why he was approaching other customers and giving them cash. The tipping off requirement doesn't prevent Mary from asking customers questions.

Wayne refused to engage with Mary and answer her questions. Mary decided to conduct more detailed analysis of Wayne's previous payouts and noticed that here had been a gradual increase in their value and frequency over the previous week.

Mary called the local police to report her suspicion. The tipping off requirement doesn't prevent her from sharing information with law enforcement agencies. She sent a suspicious matter report to AUSTRAC and, as required, included details in the SMR regarding the fact that she had informed the local police.

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

You do not have to stop providing services to a customer because you have formed a suspicion about them. You must follow your business's policies and procedures, taking into account the risks of continuing to allow your customer to use your business's facilities and how you manage and mitigate those risks. If you choose to stop serving 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 have reported an SMR to AUSTRAC.

Once you submit an SMR you *must* apply enhanced customer due diligence. 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 customers 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?

By law, SMRs you provide are kept confidential by AUSTRAC and our partner agencies. SMRs cannot be used as evidence in court or tribunal proceedings.

EXAMPLE: SUSPICIOUS ACTIVITY IN A CLUB

David is the compliance officer for the Far North Club. The business offers food and beverage services in addition to having a license to operate 50 EGMs. David ensures all applicable staff at the Far North Club have completed ML/TF risk awareness training and that procedures are in place to identify and submit suspicious matters to AUSTRAC.

A staff member, Sally, has noticed a customer who has been visiting the Far North Club's gaming room twice a day during the week. The customer spends a large portion of time in the gaming

room and has been seen 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 is reluctant to provide identification, he appears to be nervous, avoids eye contact and doesn't appear to want to engage with any of the staff. Sally recalls her ML/TF risk awareness training and recognises this customer's behaviour as potentially suspicious.

Sally follows the Far North Club's SMR reporting procedures and tells David. David then speaks with other members of the gaming staff to gather additional information, and then submits an SMR to AUSTRAC.

As part of the process of submitting an SMR, David is required to undertake ECDD. Following the Far North Club's ECDD program, David reviews the cheque register and notices that the customer has engaged in this activity several times over the last few months. David then undertakes an open source search on the customer and discovers the customer has recently been charged with drug offences. David raises this with his venue's senior management to determine whether they should continue to allow the customer to gamble at the venue.

THRESHOLD TRANSACTION REPORTS

A threshold transaction is when there is a transfer of $10,000 or more of physical currency (i.e. cash) (or the foreign currency equivalent) as part of providing a designated service. A transfer can involve either receiving or paying out $10,000 or more in physical cash.

Electronic funds transfers and cheques of amounts of $10,000 or more must not be reported as threshold transaction reports (TTR) 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.

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 does not need to submit a TTR. This is because the transaction does not involve $10,000 or more in physical cash.

WHEN MUST YOU SUBMIT A TTR?

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

WHAT MUST YOU INCLUDE IN A TTR?

When submitting a TTR to AUSTRAC you must include details about:

- the customer's full name, DOB and full address
- the transaction, including the amount of cash transferred (paid out)
- your business
- the date of the threshold transaction
- the type of designated service your business provides (eg. EGMs).

HOW DO YOU SUBMIT A TTR?

1. Log into your AUSTRAC Online account at **online.austrac.gov.au/ao/login.seam**
2. Click on the **+ (plus)** symbol on the left side of Transaction Reporting
3. Click on the **+ (plus)** on the left side of Reports
4. Click **Create/amend reports**
5. Look for the TTR-GS report type and click **Create**

You can also access TTR guides through AUSTRAC online.

1. Click **Transaction Reporting**
2. Click **AML/CTF Act reporting forms, file specifications and explanatory guides**
3. Look for the guides under **Data entry form guides**.

DO I NEED TO SUBMIT A TTR?

If your business has entitlements under licence to operate 16 or more EGMs then you must submit TTRs to AUSTRAC.

ANNUAL COMPLIANCE REPORT

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

- assess how you are 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 January and 31 March of each year. AUSTRAC will email you to notify you about the compliance report due dates so it is important that your contact details are up to date.

DO I NEED TO SUBMIT A 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.

HOW DO YOU SUBMIT A COMPLIANCE REPORT?

1. Log in to AUSTRAC Online at **online.austrac.gov.au/ao/login.seam**
2. On the left side of 'My Business,' click the **+ (plus)** symbol
3. Click **Compliance Reports**
4. Click **Open Compliance Report**
5. Complete the questions
6. Review and submit.

You do not have to complete the report in one session. You can save the form as you go and come back to it later.

COLLECT AND VERIFY INFORMATION - KNOW YOUR CUSTOMER

You need to document the customer identification procedures you use to collect and verify your customers, also known as Know Your Customer (KYC) information.

You must conduct customer identification procedures when:

- paying out winnings of $10,000 or more, regardless of how it is paid, or
- applying enhanced customer due diligence (ECDD) that requires you to obtain and verify this information (such as where a customer is high-risk or you have formed a suspicion).

KYC involves collecting details from the customer, and then verifying those details against reliable and independent sources such as a driver's licence, a passport or through e-verification.

COLLECTING DETAILS FROM A CUSTOMER

The minimum information that must be collected for a customer is the:

- full name
- date of birth
- residential address (not a post office box).

VERIFYING DETAILS FROM A CUSTOMER

Verification involves confirming the customer's identification details against identification documents, such as a driver's licence or passport or through e-verification.

The minimum identification information that must be verified for a customer is:

- the customer's name, and
- either their date of birth or residential address.

LEARN MORE

For information about reliable and independent document-based and electronic-based verification, go to: **austrac.gov.au/verify**

IS YOUR CUSTOMER A POLITICALLY EXPOSED PERSON?

You must have risk based procedures to determine whether a customer is a politically exposed person (PEP). A PEP is a person who holds a prominent public position or function in a government body or an international organisation, either in Australia or overseas. This includes, but is not limited to:

- a head of state or head of a country or government
- government ministers or equivalent politicians
- a senior government official
- a judge of the High Court of Australia, the Federal Court of Australia or a Supreme Court or a judge of an equivalent overseas court
- a senior foreign representative, ambassador or high commissioner
- a high-ranking military officers
- board members or executives of a state enterprise or international organisation.

Their immediate family members and/or close associates are also considered PEPs.

Being a PEP doesn't automatically mean that the individual's activities are suspicious, just that there is a potential for the person to be targeted for corruption or bribery, making the person potentially higher risk.

Your enhanced customer due diligence program must be applied for customers who are foreign PEPs. For more information please read the Enhanced customer due diligence section.

LEARN MORE

For information about PEPs and examples of how to identify them, go to:
austrac.gov.au/politically-exposed-persons

ADDITIONAL KYC INFORMATION

In certain circumstances, you will need to collect additional identification details about a customer, for example, where you have identified the customer to be a PEP or your regular transaction monitoring has identified a potentially suspicious pattern of behaviour.

In some circumstances, evidence of a customer's occupation or their source of funds can provide further context for their activity and may help to clarify the ML/TF risk of that customer, for example:

- where a customer advises they are a student or are unemployed; and/or
- where a customer brings substantial amounts of cash into the business.

In situations where you have collected additional information about a customer, you may need to verify the additional identification details you collected.

ONGOING CUSTOMER DUE DILIGENCE

You must develop, implement and document procedures for ongoing customer due diligence (OCDD).

OCDD includes a transaction monitoring program (TMP) and enhanced customer due diligence (ECDD) program.

It's important that you proactively monitor your customers throughout your entire relationship with them.

Monitoring isn't just limited to identifying, mitigating or managing the risks posed by an individual customer; it should also assist you in identifying patterns of ML/TF risk across your customer base, and help you mitigate and manage those risks at a business level.

TRANSACTION MONITORING PROGRAM

You will need to implement a TMP to monitor all customers. It must be based on the ML/TF risk faced by your business and trigger alerts for transactions that may be suspicious, such as:

- size, frequency, or patterns of transactions that may indicate unusual or suspicious activity
- activities that may be inconsistent with a customer's risk profile or history
- other unexpected activity from a customer which may indicate ML/TF
- a transaction that appears suspicious.

ENHANCED CUSTOMER DUE DILIGENCE PROGRAM

ECDD involves carrying out extra checks that are appropriate when specific ML/TF risks are identified.

Your business' ECDD program must be applied when certain things occur, including:

- when you determine through your risk-based systems and controls that the ML/TF risk is high
- your customer is a foreign PEP or has a beneficial owner who is a foreign PEP
- a customer's suspicious activity or behaviour may lead to you making an SMR

When ECDD is triggered, you must undertake measures **appropriate to the situation**, which may include:

- identifying a customer's source of funds and wealth
- asking for further information or documentation to identify a customer
- verifying or re-verifying the KYC information originally provided by the customer
- undertaking more detailed analysis and monitoring of the customer's transactions
- seek senior management approval as to whether or not to allow a customer to operate an EGM.

Carrying out ECDD allows you to decide whether a suspicious matter should be reported. It's important to note that SMR reporting is not a risk mitigation strategy, so even if you submit an SMR, you still have an obligation to mitigate and manage the risk you have identified. ECDD plays an important role in detecting, disrupting and preventing ML/TF.

You should also make records when you undertake ECDD, including which measures were undertaken, by whom and any findings made. These records help AUSTRAC determine how well your business is able to mitigate and manage its ML/TF risk.

DID YOU KNOW: ABILITY TO OBTAIN INFORMATION

You can request information from a customer that is likely to assist you to comply with your Part A Program.

Consider what you need to obtain from a customer in conducting KYC and ECDD and how best to obtain that information to inform your decision making about that customer and the risk that they present.

EXAMPLE: TMP AND ECDD IN PRACTICE

Hotel South's transaction monitoring includes the review of cheques and electronic fund transfers made to customers. A review of the previous week's payments to customers revealed a larger than normal volume of payments to one particular customer.

Hotel South's compliance officer, Jennifer decided to review recent CCTV footage and identified that the customer attended the venue on several occasions with a bag that appeared to contain large amounts of cash. At no time was he observed using Hotel South's ATM. Jennifer became suspicious and spoke with staff to find out whether they had observed anything. Cashier staff advised that the customer had requested to have winnings split into two separate cheques, as well as requesting the transfer of funds to an account held in a friend's name. Jennifer made a record of this information (as per the Hotel's ECDD program), including why she believed it was suspicious, advised senior management and submitted an SMR to AUSTRAC.

EMPLOYEE DUE DILIGENCE PROGRAM

You must have risk based procedures to screen:

- prospective employees before they are employed in a position that may facilitate ML/TF.
- existing employees before they are transferred or promoted to a position that may facilitate ML/TF.

Some examples of screening that you should consider include:

- verifying their identity
- confirming their employment history (for example through references or referee reports)
- considering their suitability for the position and whether they may pose a risk to the business.

Some roles in your business might be higher risk than others, for example, roles with duties that might make the employee a target for collusion with, or coercion by, criminal groups. If this is the case you may also consider checking whether the person:

- has a criminal record or links to known criminals
- is or has been subject to any regulatory, court or legal action
- has used bankruptcy laws to their advantage

Your employee due diligence program must also set out the steps that will be taken if an employee fails to comply with your AML/CTF program.

This might include:

- mandatory training to refresh their knowledge of the AML/CTF program
- disciplinary actions, ranging from formal warnings to instant dismissal, or reconsideration of role suitability, depending on the seriousness of the breach.

EMPLOYEE ML/TF RISK AWARENESS TRAINING

You must provide ML/TF risk awareness training to your employees, and document your employee training program in Part A of your AML/CTF program.

Your risk awareness training program must ensure staff are aware of:

- your business's obligations under the AML/CTF Act
- the consequences of not complying with the AML/CTF Act
- the type of ML/TF risk your business might face, and the consequences of those risks
- how your business's obligations are met, including what your specific processes and procedures are as they relate to AML/CTF obligations.

You should also consider providing ML/TF risk awareness training to board members, senior managers, directors, and consultants who are involved in providing designated services to customers.

The type and frequency of training will depend on the ML/TF risks specific to your business. Some examples you should consider include:

- online training courses
- in-house or external training with an instructor
- on-the-job training, particularly where the risks are specific to a certain role
- induction training for new employees, or existing employees who take on new roles or positions

If you engage the services of an external entity or AML/CTF advisor to provide training to your staff, it's important that you ensure the training is specific to your business and the designated services you provide, and appropriately addresses the ML/TF risks present in your industry.

You will need to regularly review your AML/CTF awareness training program to make sure it covers the level of ML/TF risk your business faces, and addresses any recent changes to your business or the way you provide designated services.

RECORD KEEPING

Record-keeping involves the creation, storage, and management of full and accurate records, which are necessary to comply with your AML/CTF obligations.

Generally you will have to keep records of or about:

- transactions
- customer identification procedures
- your AML/CTF program.

You must store these records securely, in a format that allows them to be retrieved and audited. They can be:

- hard copy or electronic
- stored at your premises or offsite.

How long you need to retain records for depends on the type of record. You will need to keep transaction records for seven years after the date you created or collected them, customer identification records for the life of your relationship with the customer plus a further seven years after you last provided them with a designated service, and AML/CTF program records for seven years after the program has ceased.

Keeping records will help you manage the risks of your business or organisation being exploited for ML/TF. If your business or organisation is misused for criminal purposes, your records may help AUSTRAC and other authorities investigate this.

NB. These record keeping requirements may involve the retention of the same documentation as required under State or Territory legislation, however the time periods for retention may vary.

You also need to comply with the Privacy Act. For more information, contact the Office of the Australian Information Commissioner for help in understanding your obligations. Learn more: **oaic.gov.au**

BUSINESSES EXEMPT UNDER CHAPTER 52 OF THE AML/CTF RULES (ENTITLEMENTS UNDER LICENCE TO OPERATE 15 OR LESS EGMs)

If your business has entitlements under license to operate 15 or fewer EGMs you may be exempt from many of the record-keeping requirements outlined in the AML/CTF 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 are 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 seven years after the date they are created or provided to you.

NB. These record keeping requirements may involve the retention of the same documentation as required under State or Territory legislation, however the time periods for retention may vary.

AML/CTF ADVISERS

To assist your business to understand and meet your AML/CTF obligations, you may choose to engage the services of an AML/CTF consultant or adviser.

It is 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.

When selecting an AML/CTF adviser, you should consider whether the AML/CTF adviser:

- has the AML/CTF experience, training and qualifications necessary to review a business of your nature, size and complexity
- has experience in providing AML/CTF advice to the pubs and clubs sector
- simply provides template, off-the-shelf AML/CTF programs and ML/TF risk assessments, or whether they will attend your venue, ask questions about your systems and controls and provide you with tailored advice
- when engaged to undertake an independent review, is able to provide an appropriately independent review of your business i.e. are they independent from any AML/CTF adviser you chose to assist you meet your other AML/CTF obligations such as drafting your AML/CTF program or ML/TF risk assessment.

If your AML/CTF adviser is not sufficiently qualified, they may provide you with a product that does not meet your needs. This can have serious consequences.

Where you have engaged an AML/CTF adviser, senior management, the AML/CTF Compliance Officer and the Board should have proactive oversight of that engagement to ensure that the product being provided meets the requirements of the AML/CTF Act and Rules.

The AUSTRAC website has a range of resources to help you ensure you can engage an AML/CTF adviser effectively:

- **Engaging an AML/CTF adviser**
- **Factsheet on engaging an AML/CTF adviser**
- **Checklist for engaging an AML/CTF adviser**

Expectations for AML/CTF advisers

It is critical that the AML/CTF adviser you select can provide you with high quality advice and professional services, including assistance with your ML/TF risk assessment and AML/CTF program.

Your AML/CTF program and ML/TF risk assessment must be tailored to the nature, size, and complexity of your individual venue. In developing appropriate systems and controls, an AML/CTF adviser is expected to consider the factors outlined in Section 2, *Conducting an ML/TF risk assessment*.

The same considerations apply to anyone you engage to conduct your independent review.

The AUSTRAC website has a factsheet which provides further information on the **expectations of AML/CTF advisers**.

AUSTRAC does not endorse or approve AML/CTF advisers or their programs. If a third-party provider makes claims that they or their programs are endorsed by AUSTRAC, this is not the case.

INDEPENDENT REVIEW

An independent review is an impartial assessment of Part A of your AML/CTF program. It checks that your business is complying with its program, and that the program:

- properly addresses your ML/TF risks
- complies with your legal obligations, and
- is working as it should.

The independent reviewer should be someone who:

- understands your business; and
- understands ML/TF risks.

The independent reviewer must not have been involved in any part of developing, implementing, or maintaining your risk assessment, related internal controls or AML/CTF program.

The reviewer can be someone in your business or organisation, or someone external to it. An example of an internal reviewer might be an auditor in your business who does not have a compliance role, or an example of an external reviewer could be a lawyer, an accountant, or an AML/CTF adviser or consultant.

You must put measures in place to demonstrate the reviewer's independence. This should include documenting that the reviewer was not involved in the design of the risk assessment, related internal controls or AML/CTF Program. It may also include an assessment and management of any conflicts of interest which may tend to call into question the independence of the reviewer.

In assessing how suitable someone is to be an independent reviewer, you may want to consider:

- whether they belong to a professional body that requires its members to meet relevant professional standards
- whether they are influenced by the people who were involved in your risk assessment, related internal controls or the development of your AML/CTF program, and
- how well the person understands AML/CTF legislation, particularly as it relates to your industry.

In addition to a review of Part A of your AML/CTF Program against your ML/TF risks and compliance with AML/CTF Rules, the independent reviewer must assess whether your Part A Program has been effectively implemented and complied with.

As a part of the review process your independent reviewer should test your systems and controls, and ask your staff questions about policies and procedures. Your independent reviewer should also engage with your board or senior management, to understand your governance processes and their effectiveness.

An independent reviewer's process of reviewing your AML/CTF program should not be tick-a-box. Instead, at a minimum AUSTRAC recommends it should involve the independent reviewer:

- visiting your venue/s;
- reviewing the systems and controls you have in place to meet your AML/CTF obligations;
- determining whether those systems and controls are appropriate to the nature, size and complexity of that venue and the rationale that supports those findings;
- testing the effectiveness of your systems and controls, and
- where these systems and controls are not appropriate to the venue, providing recommendations to make those systems and controls appropriate, and the rationale that supports those recommendations. This may include working with you to develop appropriate systems and controls.

How often you need to conduct an independent review will depend on the size and complexity of your business, and its ML/TF risks.

If your business is high-risk you should conduct an independent review at least every two to three years.

In addition to your regularly scheduled reviews, an independent review should also occur where there are material changes to your ML/TF risks, feedback is received from AUSTRAC about your business, or to the industry as a whole.

MORE INFORMATION

To keep up to date with updates from AUSTRAC, subscribe to the AUSTRAC InBrief newsletter: **austrac.gov.au/inbrief**

You may also submit a query online: **austrac.gov.au/contact-us/form** or call our Contact Centre:

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

Overseas enquiries: +61 299500055 (international charges may apply)

Section 3: Glossary

AML/CTF Act

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

AML/CTF Rules

The Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No.1)

AML/CTF Compliance officer

A staff member at management level who is appointed to oversee the business' compliance with the AML/CTF Act and AML/CTF Rules.

AML/CTF program

A document that sets out how a reporting entity meets their AML/CTF compliance obligations.

Compliance report

An annual report that includes questions about how you have met your AML/CTF obligations during the previous calendar year.

Customer due diligence (CDD)

The process where pertinent information of a customer's profile is collected and evaluated for potential ML/TF risks.

Designated business group (DBG)

A group of two or more reporting entities who join together to share the administration of some or all of their anti-money laundering and counter-terrorism financing obligations.

DBGs can only be formed by:

- related companies
- joint ventures
- accounting practices that are reporting entities
- legal practices that are reporting entities
- registered remittance service providers.

An entity can only be a member of one designated business group at a time. The group agreement must be in writing.

Designated service

A service that is listed in section 6 of the AML/CTF Act (because it has been identified as posing a risk for money laundering and terrorism financing) and which meets the geographical link. Designated services include a range of business activities in the financial services, bullion, gambling and digital currency exchange sectors. Entities that provide any of these services are reporting entities. Reporting entities have obligations under the AML/CTF Act.

Employee ML/TF risk awareness training program

A written training plan to help your employees understand:

- your obligations under Australia's AML/CTF law
- the consequences of not complying with AML/CTF legislation
- the type of money laundering (ML) or terrorism financing (TF) risk your business might face and the consequences of the risk
- how you meet your obligations, including your processes and procedures to identify, mitigate and manage the risk.

Enhanced customer due diligence (ECDD)

The process of undertaking additional measures, such as customer identification and verification and analysis of transactions, in circumstances deemed to be high risk.

Impact

The degree of damage or loss that may result if something occurs.

Independent review

An impartial assessment of Part A of your AML/CTF program, which checks that your business is complying with its program, and that the program:

- properly addresses your ML/TF risks
- complies with your legal obligations, and
- is working as it should.

Indicators of suspicious activity

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

Inherent risk

The amount of risk that exists in the absence of AML/CTF controls implemented by the reporting entity.

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

An initial and ongoing process whereby a business determines and verifies the real identify of a customer and their transaction activities. Confirming this information allows businesses to identify irregularities to a customer's normal behaviour which may form a suspicion for criminal activity.

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 chance that something may happen.

Money laundering

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

ML/TF

Money laundering and terrorism financing.

ML/TF risk

The risk a business may face in the provision of services that involves or facilitates money laundering or terrorism financing.

Physical currency

Australian or foreign money (coin and notes) that is designated legal tender.

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 AML/CTF Act identifies three 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).

Reporting entity

An entity that provides any designated services listed under section 6 of the AML/CTF Act. These entities generally provide financial, gambling, bullion or digital currency exchange services. All reporting entities must meet obligations under the AML/CTF Act.

Residual risk

Residual risk is the amount of risk that remains after a reporting entity's AML/CTF controls are implemented.

Source of funds

The particular funds or other assets involved in one or more transactions between you and the customer.

Source of wealth

The origin of entire wealth including the volume of wealth the customer would be expected to have accumulated and how the customer acquired that wealth.

Structuring

Structuring is where a person deliberately splits cash transactions to avoid a single large transaction being reported in threshold transaction reports

Structuring can be a money laundering technique and is an offence under the AML/CTF Act.

Suspicious matter report (SMR)

A report a reporting entity must submit under the AML/CTF Act if they have reasonable grounds to suspect that a transaction may be related to money laundering, terrorism financing, tax evasion, proceeds of crime or any other serious crimes under Australian law. An SMR must also be submitted if the reporting entity has reasonable grounds to suspect the customer is not who they say they are.

Terrorism financing

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

Tipping off

Telling a person (other than an AUSTRAC entrusted person) information about an SMR, that would or could reasonably be expected to prejudice a current or future investigation. Tipping off is a criminal offence.

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 AUD 10,000 or more (or the foreign currency equivalent).

Transaction monitoring program

A program that comprises appropriate systems and controls to monitor the transactions of customers and identify suspicious transactions.

AUSTRAC.GOV.AU