



Australian Government  

---

Australian Transaction Reports  
and Analysis Centre

**AUSTRAC** e-learning 

**Module 4**

**Risk assessment for  
your AML/CTF  
program**

AML/CTF Programs

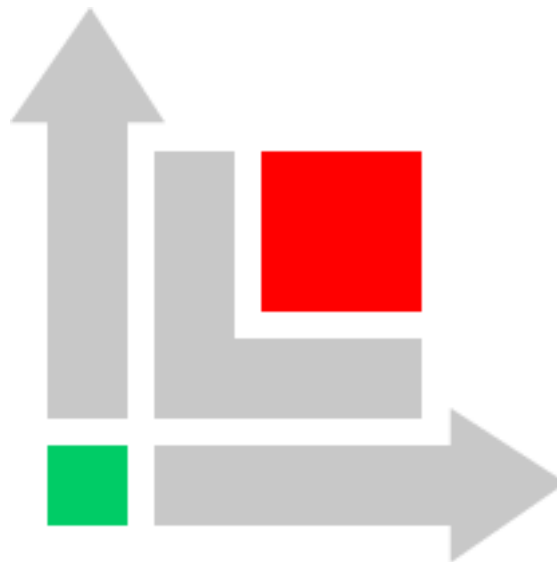


**Australian Government**

**Australian Transaction Reports  
and Analysis Centre**

## **Module 4**

# **Risk assessment for your AML/CTF program**



## Module 4

### Risk assessment for your AML/CTF program

#### Module overview

In this unit we will introduce a generic risk assessment process that can be used in the first step to plan and design an AML/CTF program. Note that this material for identifying and managing risks is offered as a starting point for developing an AML/CTF program; it may not cover every contingency or requirement for your specific business. However you can use this material, or any other any process that you choose, which is appropriate to your business (size, nature and complexity) and the ML/TF risks your business may reasonably face.

## Core Concepts

This module will address the following:

- Compliance and risk management
  - An approach to a compliance program
  - Compliance culture
  - Understanding the business's internal environment
- Risk management process
  - Which risks do you need to manage?
  - A risk management method
- Risk identification
- Risk assessment
  - Likelihood scale
  - Impact scale
  - Risk matrix and risk score
  - Applying risk appetite to risk assessment
  - Risk tolerance
  - Regulatory risk and risk tolerance
- Risk treatment
- Monitoring and Reviewing

## Compliance and risk management

Module 1 introduced the concepts of regulatory risk and business risk and explained the differences between them. Regulatory risk is associated with compliance, where a business's actions to comply may not meet the standards of regulatory practice. However it is important to note that compliance and regulatory risk management are not identical. Planning the AML/CTF program involves an understanding of both compliance and risk management; these two concepts are contrasted in the table below.

Compliance	Risk management
Compliance is about meeting obligations, which in this case are mandated by the AML/CTF Act.	Risk management involves: <ul style="list-style-type: none"> <li>• the identification of different types of risk</li> <li>• assessing the impact of these risks</li> <li>• determining the risk appetite of the organisation</li> <li>• putting in place risk management procedures and controls.</li> </ul>
Compliance is about meeting obligations that may have a mandatory component.	Risk management does not have a mandatory component as the organisation determines how to deal with the various risks it faces.  However, risk management may have to deal with both mandatory and non-mandatory elements.
All compliance risks must be dealt with.	Risk management is used to prioritise the compliance risks.
Compliance identifies all the obligations an organisation has.	Risk management techniques are used to prioritise the response to the obligations in terms of control procedures and processes, levels of monitoring and reporting requirements.

*Table 1: Compliance and risk management*

## An approach to a compliance program

Businesses operate in an increasingly regulated environment through which they are exposed to legal and financial risks that must be managed. Compliance programs are important for operating in a regulated environment to ensure that a business adheres to the requirements of laws, industry and organisational standards and codes, principles of good governance and accepted community and ethical standards.

While the AML/CTF program itself is designed to identify, mitigate and manage the business risk of money laundering and terrorism financing (ML/TF), the implementation of and continued adherence to the AML/CTF program within your business is the essence of a compliance program. A successful compliance program ensures that the business will continue to meet its AML/CTF obligations.

Some organisations may only require:

- a simple program because of the small size of the business and the minimal range of products and services offered to a limited range of countries.

More complex organisations may require:

- dedicated compliance staff
- detailed guidelines and procedures for different business units that face risks
- systems to keep track of the business's legal and regulatory requirements.



## Compliance culture

The 'culture' of a business comprises the experiences, attitudes, beliefs and values of the organisation. These control the way people interact with each other and with stakeholders outside the organisation such as customers, suppliers and regulators.

Organisations that are successful in embedding a compliance culture often follow a similar process. A useful first step to learn the extent of the compliance culture and indicate some of the things that may need doing is to complete a compliance culture checklist. A checklist can be downloaded from the 'Tools and resources' section of this topic.

### Australian Consumer and Competition Commission (ACCC) notes on compliance programs

According to the ACCC an effective compliance program is likely to have the following characteristics:

**Strategic vision**—compliance activities are linked to the business's strategic goals. The method the business uses to achieve those goals is communicated, as are benchmarks for implementation.

**Risk assessment**—the business actively identifies its compliance risks and reassesses those risks at regular intervals as part of entering into new business areas or activities. Specific compliance risks that may arise within each business unit or sphere of operations are considered.

**Control points**—each of the risks are managed at specified control points. Control points are reinforced by establishing behavioural and procedural controls. Procedural mechanisms address and mitigate high-risk areas in a business's operating environment, while the behavioural mechanisms emphasise the business's policies for those risks.

**Adequate documentation**—compliance endeavours are adequately documented to ensure they can be substantiated in the event of a breach.

**Identified positions that are accountable**—for managing each element of the compliance system.

**Continuous improvement**—the business self-evaluates its performance and its approach to ensure they are appropriate to its operations.

<http://www.accc.gov.au/content/index.phtml/itemId/54418/fromItemId/12226>

## Understanding the businesses' internal environment

An effective AML/CTF program manages the business risk of ML/TF. Before designing the AML/CTF program it is useful to assess your business's ability to implement and sustain a program. The following are some key elements that you should understand, as these may form the starting point of your design and implementation of your AML/CTF program.

### Risk management philosophy

An organisation's risk management philosophy is the shared values, attitudes and beliefs which characterise how its leaders consider risk. This a major contributor to the overall compliance culture.

Risk management philosophy affects strategy development, how risks are identified, the kinds of risks that are accepted, how risks are managed and the eventual implementation of the AML/CTF program.

No.	Questions to ask
1	What is management's risk management philosophy?
2	Has the risk management philosophy been spread throughout the organisation?
3	Has the risk management philosophy been taken on board by all staff?
4	If no to questions 2 and 3, is there a plan to develop the desired risk management culture within the business?

## Management commitment

This is one of the most important elements to a successful risk management program. The commitment of senior management affects the whole organisation and contributes to the success or otherwise of the risk management process.

No.	Questions to ask
1	Does senior management have values, attitudes and beliefs supporting a risk management and compliance culture?
2	Is senior management committed to implementing a risk management and compliance culture?
3	Does senior management drive the development of the desired values, attitudes and beliefs?
4	Does senior management provide leadership in defining and embedding the desired behaviours and culture?

## Risk appetite

This is the amount of risk that management is willing to accept. It reflects the risk management philosophy and influences the organisation's culture and operating style.

No.	Questions to ask
1	Has risk appetite been considered in the strategy?
2	Has risk appetite been considered in relation to key stakeholders such as customers and the regulatory agency?

## Integrity and values

The effectiveness of risk management in an organisation is strongly influenced by the integrity and values of the people involved.

No.	Questions to ask
1	Is there a code of ethics or other policies regarding acceptable business practice?
2	Do employees understand what behaviour is acceptable and unacceptable and know what to do when there is improper behaviour?
3	Are employees encouraged to 'do the right thing'?
4	Does management take appropriate action when someone does not abide by policies and procedures?

## Competence

Competence reflects the knowledge, skills and behaviour needed to perform tasks.

No.	Questions to ask
1	Have competency levels been established for particular jobs?
2	Have the skills, knowledge and behaviours for each level of competency been specified?
3	Is there a development process for staff to ensure they can meet the job expectations?

## Organisational structure

Structure allows the responsibilities for different functions and processes to be clearly allocated. An organisation's structure affects how it operates its functions, communicates and collaborates between its functions.

No.	Questions to ask
1	Is the risk management/compliance function structured in such a way that it can achieve its objectives?
2	Do the people responsible for the risk management/compliance function have access to senior management?

## Authority, responsibility and accountability

Authority, responsibility and accountability reflect the degree to which people are authorised and encouraged to use their initiative in day-to-day activities as well as assigning the limits to their authority.

No.	Questions to ask
1	Does the organisation have policies that describe its business practices, particularly those in relation to risk and compliance?
2	Do job descriptions specify roles, responsibilities and accountabilities?
3	Do staff understand their job function and how it contributes to the organisation's business objectives?
4	Do staff know what they are accountable for?

## Human resources

Human Resources (HR) practices include recruitment, training, evaluating, promoting, counselling, compensation and disciplinary action. The way an organisation performs these HR practices informs staff about the expected levels of performance, behaviour and integrity.

No.	Questions to ask
1	Generally speaking are the most qualified people recruited?
2	Does the organisation have a training and development policy?
3	Are staff given access to training so they are able to perform their job well in today's constantly evolving environment?

## Existing compliance programs

An organisation's management of the full range of regulatory and legal obligations is usually achieved through a number of specific compliance programs. These may include programs such as trade practices compliance, funds management compliance and occupational health and safety. There may be opportunities to leverage off these programs.

No.	Questions to ask
1	Does the organisation have any other compliance and/or risk management programs?
2	Does the organisation already have some knowledge and expertise in compliance and/or risk management?
3	Are there opportunities to integrate with existing programs and/or systems?

## Available resources and people

Existing resources and people available in the organisation which can facilitate the development and management of a risk management program are an obvious advantage.

No.	Questions to ask
1	Does the organisation have staff who can help the risk management process?
2	Does the organisation have systems and processes that can be used in the development of the risk management process?
3	Does the organisation already have some knowledge and expertise in compliance and/or risk management?

## Risk management process

### What is risk?

The International Organization for Standardization defines risk as the combination of the probability of an event and its consequences (ISO/IEC Guide 73). In simple terms risk can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result if it does occur.

### What is risk management?

Risk management is the process of recognising risk and developing methods to mitigate and manage it. This requires the development of methods to identify, prioritise, treat (deal with), control and monitor risk exposures. In risk management, a process is followed where the risks are assessed against the likelihood (chance) of them occurring and the severity or amount of loss or damage (impact) which may result if they do happen.

### Which risks do you need to manage?

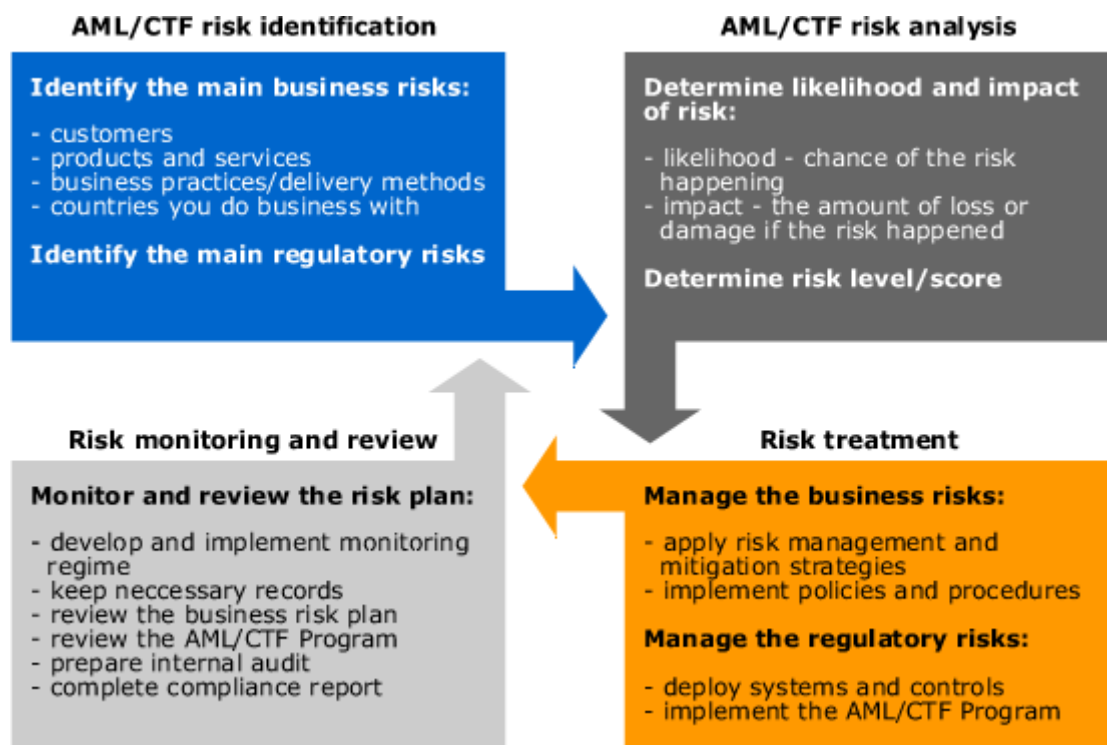
In Unit 1 *Fundamentals of AML/CTF programs*, the Risk Principles Framework identified two categories of risk that need to be managed in implementing an AML/CTF program.

- *Business risk* is the risk that your business may be used for money laundering or terrorism financing. Businesses must assess the following risks in particular: customer risks, products or services risks, business practices and/or delivery method risks and country or jurisdictional risks.
  
- *Regulatory risk* is associated with not meeting your obligations under the AML/CTF Act. Failing to meet regulatory obligations includes such things as *not* reporting suspicious matters, *not* conducting customer identification, *not* fulfilling customer identity verification requirements, or *not* having an AML/CTF Program.

Within these categories the first step to managing the risks is to identify both business and regulatory risks that your business may face for ML/TF and then work out the best ways to reduce and manage those risks. This is the process of following a risk management method.

## A risk management method

The following risk management method is based on the *AS/NZS 4360:2004: Standard for risk management (Australian Standard)*:



In following a risk management method what you do may be in proportion to the size of your business and the resources you have available. You also need to balance the costs to your business and customers against the risk of the business being used for ML/TF. The most relevant risks to counter will be those that your business may reasonably be expected to face while providing its services.

***HB 436:2004 Risk Management Guidelines; Companion to AS/NZS 4360:2004***

This handbook supports the respected standard for risk management released by Standards Australia in 2004. It provides generic guidance for establishing and implementing effective risk management processes. It contains detailed explanations for a range of approaches to following a risk management method.

The Risk Management Guidelines handbook is available from the Standards Australia website: [www.standards.org.au](http://www.standards.org.au)

## Risk identification

The first step is to identify what ML/TF risks exist for your business when providing designated services. When assessing this risk you may also like to consider legal and reputational considerations. There are two risk types: business risks and regulatory risks.

### Business risks

In terms of the AML/CTF Act four likely business risk categories have been identified (you may identify others depending on your business):

- customers, including politically exposed persons (PEPs)
- products and services
- business practices/delivery methods
- countries you do business in/with (jurisdictions).

### Regulatory risks

These risks are associated with not meeting the requirements of the AML/CTF Act. Examples of some of these risks include:

- customer verification performed incorrectly\
- failing to train staff adequately
- not having an AML/CTF program
- failing to report suspicious matters
- not doing an AML/CTF compliance report
- not appointing an AML/CTF Compliance Officer.

A risk management worksheet can be used to list specific sources of risk that your business expects to encounter in each risk category. The worksheet may also be used in the risk assessment and measurement step to list the likelihood, impact and risk scores against its source.

<b>Risk group:</b>	<b>Customers</b>			
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk score</b>	<b>Treatment/action</b>
New customer <i>(example only)</i>				
Customer who has a large cash-only business <i>(example only)</i>				
Customer who represents an unregistered charity <i>(example only)</i>				

## Risk assessment

Once you have identified the ML/TF risks you expect to encounter in your business, these risks need to be assessed or measured in terms of a combination of:

- **likelihood** that these will occur
- **impact** of the consequence of loss or severity of damage that may result if these do occur.

Using scales of likelihood and impact within a risk matrix will allow you to combine the two separate measures to generate a matrix of risk scores.



### Likelihood scale

A likelihood scale refers to the potential of a ML/TF risk occurring in your business for the particular risk being assessed. Three levels of risk likelihood are shown in the sample table below, but you can define as many levels of likelihood as you believe are necessary for your particular business.

Rating	Description/likelihood of a ML/TF risk
Very likely	Almost certain: will probably occur several times a year
Likely	Likely: high probability will happen once a year
Unlikely	Unlikely: but not impossible

## Impact scale

An impact scale refers to the consequence of loss or severity of damage that may result if the risk eventuates.

In assessing the possible impact or consequences, the assessment can be made from several viewpoints. Following is a list of ideas. It does not cover everything and it is not prescriptive.

Impact of a ML/TF risk could, depending on individual business circumstances, be rated or looked at from the point of view of the following:

- **The risk of actual losses to your business:** how it may affect your business if a failure of due diligence caused it to suffer a financial loss from the crime itself, or through prosecution by law enforcement or fines from a regulator.
- **The risk to reputation:** how it may affect your business if a failure of due diligence allowed it to have inadvertently aided an illegal act. Such a failure could result in adverse government sanctions and/or rejection by your customers. You may also consider how it may affect your wider business community (market, industry or professional communities). A whole industry may suffer from a bad reputation as well as your business.
- **The risk of furthering a criminal enterprise:** a particular transaction may result in a designated service your business provides being used to hide the proceeds of crime, or funds being returned to a criminal enterprise to facilitate further crimes. Money laundering has been associated with crimes such as corruption, bribery, smuggling of goods, people smuggling and slavery, illicit drug trading, illicit arms-trading, kidnapping, terrorism, theft, embezzlement and fraud.
- **The risk of causing harm:** that a particular transaction may result in people suffering through the conduct of crime, or result in the loss of life or property through a terrorist act.

Three levels of risk impact are shown in the sample below, but you can define as many levels of risk impact as you believe are necessary.

Rating	Description/impact of a ML/TF risk
Major	Huge consequences - major damage or effect Serious terrorist act or money laundering
Moderate	Moderate level of ML/TF impact
Minor	Minor or negligible consequences or effects

## Risk matrix and risk score

Use the risk matrix to combine LIKELIHOOD and IMPACT ratings and values to obtain a risk score. The risk score may be used to aid decision making and help in deciding what action to take in view of the overall risk. How the risk score is derived can be seen from the sample risk matrix and risk score table shown below. Four levels of risk level or score are shown in the matrix and table below but you can define as many risk scores as you believe are necessary.

Likelihood ↑	Very likely	Medium 2	High 3	Extreme 5
	Likely	Low 1	Medium 2	High 3
	Unlikely	Low 1	Low 1	Medium 2
	What is the chance it will happen?	Minor	Moderate	Major
		→ Impact		

Rating	Impact- of a money laundering or terrorism financing risk
5 Extreme	Risk almost sure to happen and/or to have very dire consequences Do not allow transaction to occur or reduce the risk to acceptable level
3 High	Risk likely to happen and/or to have serious consequences Do not allow transaction until risk reduced
2 Medium	Possible this could happen and/or have moderate consequences May go ahead but preferably reduce risk
1 Unlikely	Unlikely to happen and/or have minor or negligible consequences Okay to go ahead

Once threat levels and risk scores have been allocated they can be entered in the risk management worksheet against the risk that it represents.

<b>Risk group:</b>	<b>Customers</b>			
	<b>Likelihood</b>	<b>Impact</b>	<b>Risk score</b>	<b>Treatment/action</b>
New customer <i>(example only)</i>	Likely <i>(example only)</i>	Moderate <i>(example only)</i>	2 <i>(example only)</i>	
Customer who has a large cash-only business <i>(example only)</i>	Likely <i>(example only)</i>	Major <i>(example only)</i>	3 <i>(example only)</i>	
Customer who represents an unregistered charity <i>(example only)</i>	Very likely <i>(example only)</i>	Major <i>(example only)</i>	5 <i>(example only)</i>	

## Applying risk appetite to risk assessment

Risk appetite is the amount of risk an organisation is prepared to accept in pursuit of its business goals. Risk appetite is a guide to the risk management strategy and also informs how an organisation deals with risks. It is usually expressed as acceptable/unacceptable level of risk.

Some questions to ask are:

- What risks will the business accept?
- What risks will the business not accept?
- What risks will the business treat on a case-by-case basis?
- What risks will the business escalate?

The risk matrix can be used to show the risk appetite of your business.

In a risk-based approach to AML/CTF the assessment of risk appetite is a judgement that must be made by the reporting entity based on its business goals and strategies, as well as a due diligence assessment of the ML/TF risks it faces in providing the designated services to its chosen markets.

Likelihood ↑	Very likely	Acceptable risk Medium 2	Unacceptable risk High 3	Unacceptable risk Extreme 5
	Likely	Acceptable risk Low 1	Acceptable risk Medium 2	Unacceptable risk High 3
	Unlikely	Acceptable risk Low 1	Acceptable risk Low 1	Acceptable risk Medium 2
	What is the chance it will happen?	Minor	Moderate	Major
		Impact How serious is the risk? →		

## Risk tolerance

In addition to defining your business's risk appetite, you can also define a level of variation to how you manage that risk. This is called risk tolerance and it provides some operational flexibility while still adhering to the risk framework you have developed.

A remittance services business has decided that generally the risk is unacceptable to remit money to a particular country. However, the remitter does have some risk tolerance. In this case the business will remit to this region provided that it is a bank-to-bank transaction only, the customer provides three verifiable customer identification documents and the transaction is approved by a senior manager. As such, the business understands and accepts the consequences of a ML/TF risk being realised.

## Regulatory risk and risk tolerance

The business risk associated with ML/TF is that an entity can be used, whether inadvertently or otherwise, to facilitate money laundering or the financing of terrorism. Risk appetite/risk tolerance implies that the entity understands and accepts the limits of the ML/TF risk mitigation strategies that it has chosen to implement, and in balance with this understands and accepts the consequences of a ML/TF risk being realised.

However whilst it is appropriate for an entity to consider the factors as set out in the AML/CTF Rules in establishing any risk appetite/risk tolerance for the business risks that it can be used for ML/TF, the same cannot be done to define a risk tolerance for regulatory risk.

If an entity has mandatory obligations under the AML/CTF Act or the AML/CTF Rules it is expected and required under law that it will meet these obligations. For example, an entity's AML/CTF program will reflect the level of ML/TF risk it assesses itself to have, but it cannot use a risk appetite/risk tolerance approach to decide that it will not have or will not implement an AML/CTF program as this is an obligation under the AML/CTF Act.

## Risk treatment

This stage is about identifying and testing methods to manage the risks you have identified and assessed in the previous process. In doing this you will need to consider putting into place strategies, policies and procedures to help reduce (or treat) the risk.

Examples of risk reduction or treatment steps are:

- setting transaction limits for higher risk products
- having a management approval process for higher risk products
- having a process to place customers in different risk categories and apply different identification and verification methods
- not accepting customers who represent unregistered charities and wish to transact with a high-risk country.

<b>Risk group:</b>	<b>Customers</b>			
<b>Risk</b>	<b>Likelihood</b>	<b>Impact</b>	<b>Risk score</b>	<b>Treatment/action</b>
New customer <i>(example only)</i>	Likely <i>(example only)</i>	Moderate <i>(example only)</i>	2 <i>(example only)</i>	Standard ID check ID verification type X
Customer who has a large cash-only business <i>(example only)</i>	Likely <i>(example only)</i>	Major <i>(example only)</i>	3 <i>(example only)</i>	Non-standard ID check ID verification type X
Customer who represents an unregistered charity <i>(example only)</i>	Very likely <i>(example only)</i>	Major <i>(example only)</i>	5 <i>(example only)</i>	Do not accept as customer

Another way you can reduce the risk is to use a combination of risk groups to modify the overall risk of a transaction. You may choose to use a combination of your customer, product/service and country risk to modify an overall risk. For example, in the case of use of a bank-account-to-bank-account service (assessed as low risk by you), to a certain city/province (assessed as high risk area by you), in a certain country (assessed as low risk by you).

It is important to remember that identifying a customer, product or country as high risk does not necessarily mean that ML/TF is involved. The opposite is also true - just because a customer or transaction is seen as low-risk does not mean the customer or transaction is not involved in ML/TF. Experience and common sense should be applied to your risk management process.

## **Monitoring and review**

Keeping records and regular evaluation of the AML/CTF program is essential. The AML/CTF program cannot remain static as risks change over time - for example, changes to your customer base, your products and service, your business practices and changes to the law.

Once documented, your business should develop a method to regularly check whether your AML/CTF program is working correctly and well. If not, you need to work out what needs to be improved and put changes in place. This will both help keep your program effective and also meet the requirements of the AML/CTF Act.

AUSTRAC intends to maintain its AML/CTF Programs e-learning application as an evolving resource to reflect changing patterns of behaviour, legislative development and the broader Anti-Money Laundering environment. Should you require further information on the e-learning application, AUSTRAC's operations, the *Financial Transaction Reports Act 1988* (FTR Act) or the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), please contact:

**AUSTRAC Help Desk via:**

[help\\_desk@austrac.gov.au](mailto:help_desk@austrac.gov.au) or Telephone 1300 021 037.

© 2008, Commonwealth of Australia

Each cash dealer, reporting entity or other stakeholder may use this material internally as an educational tool. It may view and use this application solely in the usual operation of its web browser in visiting the AUSTRAC Site ("the Site"). Except for this purpose, the material may not otherwise be used, copied, reproduced, published, altered or transmitted in any form or by any means in whole or part (except where such use constitutes fair dealing under the *Copyright Act 1968* (Cth)) without the prior written approval of the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or posted at <http://www.ag.gov.au/cca>, with a copy to AUSTRAC.

The Commonwealth accepts no liability in regard to any loss or damage suffered by you resulting from a loss of service, malfunction, computer viruses, or any other cause connected with your use of the Site.

The information contained in this application is intended only to provide a summary and general overview on these matters. The AML/CTF Programs course is not intended to be comprehensive nor does it constitute legal advice. AUSTRAC may from time to time amend legislative instruments under the legislation it administers and this may impact on the form and content of the AML/CTF Programs course. The AML/CTF Programs course contains statements of policy that reflect AUSTRAC's administration of the legislation in performing its statutory functions. The Commonwealth accepts no liability for any loss suffered as a result of reliance on it. AUSTRAC recommends that cash dealers, reporting entities and other stakeholders should obtain their own legal and/or technical advice on matters arising from the AML/CTF Act, the FTR Act, regulations and/or the published Anti-Money Laundering/Counter-Terrorism Financing Rules (AML/CTF Rules) tailored to the cash dealer, reporting entity or other stakeholder's specific circumstances, prior to making any decisions. The information contained in the AML/CTF Programs course is current as at the version date which appears on the AML/CTF Programs course.

Your use of this application does not relieve you of any obligations you may have under any legislation, subordinate legislation, rules, requirements or standards, including but not limited to the AML/CTF Act and the FTR Act.

Cash dealers, reporting entities and other stakeholders using this application should be aware of any obligations they may have under the *Privacy Act 1988* (Cth). These obligations could include a duty of confidentiality to their customers and not using personal information for an improper purpose. Further information regarding privacy obligations can be obtained from the Privacy Commission via [www.privacy.gov.au](http://www.privacy.gov.au) or telephone **1300 363 992**. [Click here for AUSTRAC's privacy statement.](#)