



## Objectives

In this module, we will address the following questions:

- What is a 'know your customer' (KYC) policy?
- What are the principal elements and requirements of a KYC policy?
- What is ongoing customer due diligence (OCDD)?
- What are the risks of not implementing a KYC policy?

Your key learning objectives will be to respond effectively to each of the questions listed above.

### What is KYC?

We will begin by making sure we have a common understanding of the definition of 'know your customer' (KYC) policy and the objectives of implementing this type of policy.

It is critical for financial institutions, professionals working within the financial sector, bullion and gambling sectors as well as other regulated entities to know their customers very well.

Financial institutions and other reporting entities should have a proper understanding of their customers to satisfy their respective KYC obligations. It is equally important that employees of these organisations are properly trained regarding the importance of KYC and the specific KYC policies or procedures of their organisation.

KYC is important for a number of other reasons. For example, if a business knows its customers well, it may be able to prevent damage to its reputation and avoid fraud or excessive risk in financial transactions involving customers.

Under AML/CTF legislation, KYC policy refers to documentation which sets out a business's approach to ensuring that it can effectively identify, verify and monitor its customers and the financial transactions in which they engage, relative to the risks of money laundering and terrorism financing. Note that Financial Service legislation also uses the term KYC, but this is not to be confused with KYC in AML/CTF. KYC in Financial Services legislation relates to the understanding of a clients financial position, not their risk of practicing ML/TF.



For more information regarding KYC refer to:

- AML/CTF Programs module, and
- Chapters 1 and 4 of the [AML/CTF Rules](#)

### The principal objectives of a KYC policy include:

- ensuring that only legitimate and bona fide customers are accepted
- ensuring that customers are properly identified and that they understand the risks they may pose
- verifying the identity of customers using reliable and independent documentation
- monitoring customer accounts and transactions to prevent or detect illegal activities
- implementing processes to effectively manage the risks posed by customers trying to misuse facilities.

### What risks are mitigated by KYC?

Let's take a brief look at the risks that can be mitigated by an effective KYC policy.

There are five types of risks that an effective KYC policy can help to mitigate:

- reputational
- operational
- legal
- financial
- concentration.

**Reputational risk:** The reputation of a business is usually at the core of its success. The ability to attract good employees, customers, funding and business is dependant on reputation. Even if a business is otherwise doing all the right things, if customers are permitted to undertake illegal transactions through that business, its reputation could be irreparably damaged. A strong KYC policy helps to prevent a business from being used as a vehicle for illegal activities.

**Operational risk:** This is the risk of direct or indirect loss from faulty or failed internal processes, management and systems. In today's competitive environment, operational excellence is critical for competitive advantage. If a KYC policy is faulty or poorly implemented, then operational resources are wasted, there is an increased chance of being used by criminals for illegal purposes, time and money is then spent on legal and investigative actions and the business will be viewed as operationally unsound.

**Legal risk:** If a business is used as a vehicle for illegal activity by customers, it faces the risk of fines, penalties, injunctions and even forced discontinuance of operations.

Apart from regulatory risk, involvement in illegal activities could lead to third-party judgments and unenforceable contracts. In addition, professionals working within many financial and other professional sectors may also personally be subject to legal action or prosecution.

Due to the nature of business, these risks can never entirely be eliminated. However, if a business does not have an effective KYC policy, it will be inviting legal risk. By strictly implementing and following a KYC policy, a business can mitigate legal risk to itself and its staff.

**Financial risk:** If a business does not adequately identify and verify customers, it may run the risk of unwittingly allowing a customer to pose as someone they are not. The consequences of this may be far reaching. If a business does not know the true identity of its customers, it will also be difficult to retrieve any money that the customer owes.

**Concentration risk:** This type of risk occurs on the assets side of a business if there is too much exposure to one customer or a group of related customers. It also occurs on the liabilities side if the business holds large concentrations of funds from one customer or group (in which case it faces liquidity risk if these funds are suddenly withdrawn).

By implementing an effective KYC policy, a business can identify the entire scope of the asset and liability risk faced in relation to each customer and group of customers.



As you can now appreciate, success within the financial sector and success as a professional business is critically dependant on developing and implementing sound KYC policies and avoiding the risks that customers may pose.

## KYC policy elements

KYC policy has five major elements. We will take a brief look at each in turn.

**Customer acceptance:** The point at which a new customer is accepted or rejected is the easiest point at which the risk of dealing with illegal money can be avoided. By following good customer acceptance policies, dealing with entities and individuals who might engage in illegal transactions can be avoided.

**Customer identification:** Establishing the identity of customers is central to the KYC policy both for the customer acceptance or rejection decision and for the ongoing monitoring of customer accounts and transactions. By identifying customers effectively, the business is able to deal with them in the appropriate manner.

**Customer verification:** Verifying that customers are who they say they are is vital to any customer identification procedure. Merely collecting customer information is not enough for an effective KYC policy. Reliable and independent documentation should be used to support and confirm the identification details a customer provides. For example, citing an original primary photographic identification document such as a passport or drivers licence.

**Accounts and transactions monitoring:** In an effective KYC policy, customer accounts and transactions are properly classified in terms of risk and are regularly monitored. Through checks and thresholds, unusual activities, activities by high-risk customers, or suspicious behaviour can be detected and reviewed.

**Risk management:** To ensure that the risks posed by money laundering and other criminal activities are identified, mitigated and managed good risk management practices are essential. For further information on risk management refer to the Australian Standard on Risk Management: AS4360.

Another objective of the KYC policy is to look past the appearance of the customer and obtain visibility into the sources of the customer's money. The basic objective is to obtain an understanding of the risk the customer poses to business. Could the customer use the business to facilitate money laundering or terrorism financing?

## Ongoing customer due diligence

Reporting entities must monitor their customers to identify, mitigate and manage any ML/TF risk that may be posed by providing a designated service. OCDD obligations apply to all customers, including pre-commencement customers and also those who were identified by another reporting entity. There are three mandatory components of OCDD:

- KYC information
- a transaction monitoring program
- an enhanced customer due diligence program.

Reporting entities need to determine when and in what circumstances additional KYC information should be collected, updated or verified.

A transaction monitoring program that sets out how customer transactions will be monitored, how the reporting entity will identify transactions that are unusual or suspicious and how such transactions will be managed once they are identified as unusual or suspicious is a requirement of Part A of the AML/CTF program.

An enhanced customer due diligence (ECDD) program must be applied when the reporting entity determines there is high ML/TF risk or a suspicion has arisen under the provisions for reporting suspicious matters in section 41 of the AML/CTF Act. The ECDD program is another requirement of Part A of the AML/CTF program.

These obligations are effective from 12 December 2008. For further information about OCDD refer to chapter 8 of the *AUSTRAC Regulatory Guide*.

## Record keeping

Under the AML/CTF Act, a reporting entity must make and retain a record of its applicable customer identification procedures. The records must be retained for seven years after the end of the reporting entity's relationship with the relevant customers. Within a designated business group, a reporting entity may undertake this obligation for other members of the group.

## The Berlin-Edwards Case

The Berlin-Edwards story is a good case study of the problems that may arise if the KYC policy is not properly followed.

**Customer Referral:** Lucy Edwards, a Vice President at the Bank of New York (BONY), introduces her husband, Peter Berlin, as a customer to the bank. Despite her role, Lucy fails to inform the bank of her relationship with Peter Berlin and the bank never questions the relationship. The referral details in the application form are left incomplete.

**Comment:** If the KYC policy was being actively followed, one of the initial questions as part of the customer acceptance policy should have been 'What is your relationship with Lucy Edwards?' This is because Lucy introduced Peter as a customer. It also appears that the lack of complete details on the application form was not reviewed.

**Accounts:** Over a three-year period, Peter Berlin opens three accounts for three separate businesses. The three businesses do not engage in any business transactions. The only activity the accounts are used for is to receive funds transfers from Russian parties and to forward funds to offshore accounts or other individuals connected to the Russians.

**Comment:** KYC was not applied in this case; one of the first procedures is to verify the business activity and the legitimacy of the customers themselves. In cases like this, customer identification can include reviewing business-related documentation, such as rent and utility bills and payroll payments.

**Misuse:** These accounts were used by Berlin and his wife to help Russian banks and other Russian customers evade taxes and other government regulations. In one instance, one of these accounts received a total of \$166 million in one month, mostly through transfers from correspondent banks. The bank did not look into the origins of these unusually large money transfers.

**Comment:** The size of the money transfers, relative to the normal flows within the account, should have been an indication that due diligence needed to be applied and a suspicious activity report needed to be filed. Also, more stringent due diligence should have been applied since correspondent banks were involved in these transactions.

**Indictment:** Over the three-year period, the couple moved in excess of \$7 billion through accounts globally. They were eventually charged with conspiracy to commit a number of U.S. crimes, including money laundering and illegal money transmission.

**Comment:** Too late! The bank suffers substantial reputational risk and loss of business.

## The four principle areas of risk

### Type of person

In general, domestic customers may be at a lower risk due to the easy availability of information to verify their identities. Offshore customers, especially those who do not have a domestic business or residence, may be a higher risk due to the difficulty in easily obtaining and verifying information about such customers.

Offshore customers may also be classified in terms of their country of origin. This is because the level of anti-money laundering regulation and enforcement varies considerably from country to country.

### Origins

A customer may have several origins. In the case of an individual, it could mean country of citizenship, place of birth or principal place of residence or business. In the case of a corporation, it could mean jurisdiction of incorporation or regulation, principal place of business or location of principal assets.

### Type of service or product

Reporting entities need to be aware of the type of product or service that they offer to a customer and the vulnerability that product or service poses to being used to launder money or finance terrorism. For example an account with multiple signatories may pose a higher risk than an account with one signatory. This is because the more people transacting on an account, the greater the exposure to criminal behaviour.

### Blacklists

When a business provides a different product or service to a new or existing customer it should be aware of the 'blacklist'. Regulators and government departments in different countries, such as the Australian Department of Foreign Affairs and Trade and the US Department of the Treasury, publish 'blacklists' of various entities.

### Blacklisted entities

Blacklists may cover:

- countries and government institutions
- individuals
- companies
- charitable organisations and non-profit associations
- known terrorist groups and their affiliates

## Blacklist purposes

The purpose of blacklists varies, but includes prevention or curtailment of the following:

- money laundering
- terrorism
- weapons of mass destruction
- drug production or smuggling
- corruption

## Blacklist sanctions

Sanctions imposed on blacklisted entities can include:

- arrest and extradition
- freezing of assets
- prohibition on dealing with third parties

## Blacklist laws

The laws under which blacklists are issued prohibit businesses (particularly in the financial sector) and individuals from dealing with blacklisted entities. However, to avoid legal problems and reputation risk, many businesses comply with the major blacklists even if such businesses are not expressly subject to regulation.

## Example

Under the [\*Charter of the United Nations \(Terrorism and Dealings with Assets\) Regulations 2002\*](#), the Australian Department of Foreign Affairs and Trade maintains a [list of prescribed persons and entities](#).



It is an offence to use or deal with such assets or facilitate using or dealing with such assets. Reporting such use or deals may also be triggered by the suspect transaction reporting obligations under the FTR Act and suspicious matter reporting obligations under the AML/CTF Act.

## Summary

KYC policies ensure that businesses can effectively identify, verify and monitor customers and customer-related transactions.

An effective KYC policy can help prevent or detect money laundering activities. It can also reduce other types of risks to a business.

The objectives of KYC policy include:

- accepting only legitimate customers
- identifying customers to understand the potential risks they pose
- verifying that customers are who they say they are
- monitoring customer accounts and transactions for illegal activities
- conducting ongoing customer due diligence particularly where your relationship with the customer is considered high-risk and/or a suspicious matter report has been lodged
- implementing risk management processes to effectively manage customer-driven risk

Well-conceived and effectively implemented KYC policies can mitigate the following risks:

- reputational
- operational
- legal
- financial
- concentration



A good policy is only as good as its implementation. Do your part!

## Know your customer quiz

This quiz will test your understanding of the 'know your customer' objectives.

### Question 1

Which of the following should be treated as a 'customer' for prudent KYC analysis?

- a) Any person or company which can conduct a transaction in relation to an account offered by a bank.
- b) Any person who is a signatory to an account offered by a building society.
- c) Any person or company which holds an account issued by a credit union.
- d) All of the above.

### Question 2

Rowena Rocket is a politician raising funds for an upcoming election. She regularly banks at Watermelon Bank and opens an account in which to place campaign contributions. The contributions are expected to reach about \$1 million. Rowena Rocket's private bankers at Watermelon Bank are aware of her profession and the purposes of the account. Since she is an old customer and has a solid reputation, they waive many of the checks to verify the funds.

What money laundering risks, if any, does Watermelon Bank face in this situation?

Watermelon Bank faces:

- a) reputational, operational, legal and concentration risk.
- b) reputational and operational risk.
- c) reputational, operational and legal risk.

### **Question 3**

What should you consider when managing AML/CTF in your business?  
This is known as:

- a) Knowing your customer
- b) Destination of funds
- c) Methods of delivery, such as cash, telephone and internet banking
- d) All the above

### **Question 4**

Please read the KYC practice stated below. Identify the KYC element which best relates to the stated practice.

Well-developed and applied customer assessments enable initial identification and classification of potentially high-risk customers.

This is known as:

- a) customer acceptance
- b) customer identification
- c) accounts and transaction monitoring
- d) risk management

### **Question 5**

Please read the KYC practice given below. Identify the KYC element which best relates to the stated practice.

High-risk customer activity is regularly reviewed and substantial high-risk customers are personally known to management.

This is known as:

- a) customer acceptance
- b) customer identification
- c) accounts and transaction monitoring
- d) risk management

### Question 6

Please read the KYC practice given below. Identify the KYC element which best relates to the stated practice.

Effective information-gathering strategies enable building of a solid information base about each customer.

This is known as:

- a) customer acceptance
- b) customer identification
- c) accounts and transaction monitoring
- d) risk management

### Question 7

During customer acceptance and identification activities, on which of the following customers should enhanced due diligence be conducted?

Select the **incorrect** response from the alternatives below.

Enhanced due diligence should be conducted on:

- a) trustees, nominees, and fiduciaries.
- b) personal customers with small deposits.
- c) non-face-to-face customers.
- d) correspondent accounts.

### Question 8

A well-established and well-regarded customer of your bank refers a new customer to you. The new customer is a leasing company that does business in the Philippines. It is also listed on the Philippine Stock Exchange.

What level of due diligence would be required?

- a) This situation requires a normal degree of due diligence. It is a public company and has been introduced by a trusted customer.
- b) This situation requires a very limited degree of due diligence because the new customer is a public company and has been introduced by a trusted customer.
- c) This situation requires an enhanced degree of due diligence. The customer is a non-bank financial company based overseas.

### Question 9

A lawyer who banks with you is a sole practitioner. He wants to open a trust account for a client. He provides you with the trust documents and the name and address of the trust beneficiary but is unable to provide additional details due to a client confidentiality obligation. You notice that the address is from an overseas jurisdiction.

What level of due diligence would be required?

- a) This situation does not require enhanced due diligence. You know the lawyer well and you have been provided with the trust documents and identity of the beneficiary.
- b) This situation requires enhanced due diligence because an offshore jurisdiction is involved.
- c) This situation requires enhanced due diligence because the lawyer is clearly hiding something when he says he is under a client confidentiality obligation.

### Question 10

Customer verification is vital to any KYC procedure. What is acceptable in verifying an individual customer?

Select the **incorrect** response from the alternatives below.

In verifying an individual customer, you can rely on:

- a) a certified copy of a birth certificate in conjunction with the customer's drivers licence and Medicare card.
- b) sighting original identification such as birth certificate and drivers licence.
- c) a reference from a good friend.

## Answers - Know your customer quiz

1. d) Correct
2. c) Correct. To manage risk, it is important for financial institutions to implement control measures such as compliance teams that make sure that KYC and related policies are implemented effectively.
3. d) Correct
4. a) Correct. At this stage, it is essential which financial institutions develop and apply customer assessments that enable them to recognise customers that may be high risk.
5. c) Correct. When monitoring accounts and transactions, it is imperative that high-risk customers and their account activity be reviewed regularly to minimise risk.
6. b) Correct. As part of the customer identification procedure, financial institutions gather detailed information about a customer. This information can be as basic as the customer's name and address or as confidential as the customer's banking history.
7. b) Correct
8. c) Correct. Although the new customer is listed, it is a non-bank financial company. Therefore, enhanced due diligence is recommended.
9. b) Correct. As this situation involves an offshore jurisdiction, you may decide that enhanced due diligence is required.
10. c) Correct

AUSTRAC intends to maintain its Introduction to AML/CTF 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.

© 2007, 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 Introduction to AML/CTF e-learning 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 Introduction to AML/CTF e-learning course. The Introduction to AML/CTF e-learning 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 Introduction to AML/CTF e-learning course is current as at the version date.

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.](#)