



Financial services for customers that financial institutions assess to be higher risk [H1] – draft guidance

Page title	Financial services for customers that financial institutions assess to be higher risk
Purpose	To provide guidance to financial institutions and customers on AUSTRAC's expectations when financial institutions provide services to customers that they assess to be higher risk.
Audience	ADIs, remitters, DCEs and fintech companies, and other business operating in relevant sectors.


In recent years, some financial institutions have declined, withdrawn or limited banking services to customers in certain industry sectors due to factors such as commercial considerations, reputational risk and regulatory risk exposure.

'Debanking' (or 'derisking') can have a devastating impact on legitimate businesses. It also reduces the capacity of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) framework to prevent and detect money laundering (ML), terrorism financing (TF) and other serious crimes by discouraging transparency and potentially forcing customers into unregulated channels.

This guidance seeks to outline a common understanding of the risk-based approach to AML/CTF regulation and the roles of financial institutions when providing banking services to businesses that financial institutions assess as higher risk. It also outlines approaches that affected businesses can consider when seeking or using banking services. For brevity, this guidance refers to both prospective customers and existing customers as 'customers'.

For **financial institutions** this guidance will:

- reassure you that within the AML/CTF framework financial institutions may provide services to businesses when you assess that the sector the business operates in is higher risk,

- 
- clarify AUSTRAC's regulatory expectations of financial institutions when assessing and providing services to these businesses, and
 - support financial institutions to apply appropriate risk identification, mitigation and management systems and controls when providing services to these businesses.

For businesses that financial institutions assess to be higher risk, including remitters, DCEs and financial technology (fintech) businesses, seeking or using the services of financial institutions, this guidance will help you to:


- understand the types of information financial institutions may request when considering whether your business is within their risk appetite, and
- ensure that you are prepared with the appropriate information when engaging with financial institutions whose services you wish to use.

Background [H2]

Sectors affected by debanking include businesses providing services for the transfer or storage of value for underlying customers such as remitters, digital currency exchanges (DCEs) and some fintech businesses (for example, payment service providers). Financial institutions may also consider other businesses, such as some not-for-profit organisations, the lawful sex work industry, adult stores, gun shops and some cash-intensive businesses, to be higher risk for other reasons.

Without access to the formal financial system, customers may seek out unregulated channels. The risk of debanking may cause some customers to provide financial institutions with less information about the true nature of their business activities, which limits transparency and increases risk.

For the risk-based approach to work effectively, both financial institutions and their customers must communicate openly and in good faith to ensure that the financial institution can be confident it understands the risks presented by the customer. Businesses seeking banking services must be transparent with financial institutions



about the nature of their business. This can assist financial institutions to better understand the risks of dealing with the business, and more effectively mitigate the risks.

Ultimately, financial institutions' engagement with customers reinforces the risk-based approach to combating ML/TF across the Australian economy more effectively than disengagement from risk.

AUSTRAC is committed to financial inclusion and working with financial institutions to ensure that AML/CTF regulation appropriately and effectively mitigates ML and TF risks.

Read more in [AUSTRAC's statement on debanking](#).


The role of financial institutions [H2]

Use a risk-based approach [H3]

The AML/CTF Act requires financial institutions to develop tailored risk-based systems and controls that are proportionate to the level of ML, TF and serious crime risk they face in providing services to particular businesses. Using a risk-based approach does not require disengagement from risk or prevent financial institutions from establishing business relationships with higher-risk customers.

ML/TF risks associated with individual businesses in a given industry sector can vary significantly, even if the sector as a whole may present higher inherent risks. AUSTRAC expects financial institutions to assess and understand ML/TF risks presented by each customer. By using a risk-based approach with appropriate systems and controls in place, a financial institution can satisfy their AML/CTF obligations when providing designated services to customers across the range of ML/TF risk profiles.

A risk-based approach does not imply a 'zero failure' approach to combating financial crime. Even if a financial institution implements appropriate risk-based



systems and controls, AUSTRAC recognises that no reporting entity can reduce financial crime risk to zero.

AUSTRAC recognises that financial institutions are commercial enterprises and may decline to provide designated services to whole sectors for commercial or other reasons, for example, where the financial institution does not have the resources to understand how a specific customer type or industry sector operates. However, as this guidance makes clear, there is no requirement in the AML/CTF Act or Rules to decline to provide designated services to whole industry sectors, notwithstanding a financial institution's assessment of the business sector's relative risk.

AML/CTF obligations are also not the only considerations that may be relevant to decisions about whether to provide banking services to a customer. For example, as noted in the Replacement Explanatory Memorandum for the AML/CTF Act, the protection from liability under s235 of the AML/CTF Act—where a reporting entity complies with the AML/CTF Act in good faith—is not intended to override anti-discrimination legislation, such as the *Racial Discrimination Act 1975*.


Refer to existing AUSTRAC guidance – [Preventing financial crime using a risk-based approach](#)

Assess the risks posed by each customer [H3]

Financial institutions are expected to assess and understand the ML/TF risks presented by each customer based on a reasonable understanding of the customer. Financial institutions should consider:

- the nature of your business relationship with the customer,
- risks associated with the product or service being provided,
- the methods of delivering the designated service to the customer, and
- any relevant foreign jurisdiction or geographic risks.

Your assessment of a customer's ML/TF risk profile should be informed by:

- 
- your up-to-date enterprise-wide or group-level ML/TF risk assessment,
 - any risk assessments and other relevant AUSTRAC guidance,
 - ongoing monitoring of your customers' activities, and
 - where applicable, any direct feedback you have received from AUSTRAC.

Risk is dynamic: where new or increased ML/TF risks are identified after the implementation of risk-based systems and controls, this should trigger a review to update the risk assessment and related systems and controls in your AML/CTF program as appropriate.

Taking a customer-specific approach to risk does not require a unique process for each customer. Developing standard templates and processes for engaging with businesses in relevant sectors based on this guidance, to help gather the key information relevant to a customer's specific risks, may assist financial institutions with keeping the costs of engagement to a reasonable level.


Conduct customer due diligence [H3]

Generally, financial institutions must complete applicable customer identification procedures (ACIP) *before* providing designated services to customers (section 32 of the AML/CTF Act). The ACIP must be designed to ensure that the financial institution is reasonably satisfied that the customer is who they say they are and knows who the customer's [beneficial owners](#) are (Rule 4.2.2 of the AML/CTF Rules).

The level of due diligence financial institutions undertake should be appropriate to the assessed risk. Not all customers need to be subject to the same level of customer due diligence, even if they operate in a sector that may present higher ML/TF risks.

Your [AML/CTF Program](#) must enable you to:

- understand the nature and purpose of your business relationship with your customers (Rules 8.1.5(1) and 9.1.5(1) of the AML/CTF Rules), and

- 
- consider the ML/TF risks arising from providing the designated service to the customer to determine whether to collect and verify additional [know your customer](#) (KYC) information (e.g. Rules 4.2.5 and 4.2.8 of the AML/CTF Rules).

Conduct ongoing and enhanced customer due diligence [H3]

Financial institutions must identify, mitigate and manage ML/TF risks throughout the course of a business relationship. The customer's ML/TF risk profile may change over time, with changes in business models, management or the availability of new information.


Higher ML/TF risk does not automatically mean that a financial institution must discontinue a business relationship. Customer due diligence measures, including transaction monitoring, should be proportionate to the ML/TF risks and done in accordance with the financial institution's enhanced customer due diligence program and transaction monitoring program.

Financial institutions must undertake ongoing customer due diligence (OCDD) for all customers, including keeping KYC and beneficial owner information up to date, as well as transaction monitoring (section 36 of the Act and Chapters 4 and 15 of the Rules).

You must apply [enhanced customer due diligence](#) (ECDD), when you determine that providing a designated service involves high ML/TF risk. As part of ECDD, you:

- may be required to seek senior management approval to provide designated services to the customer, and
- should record the final decision of senior management and the rationale.

The AML/CTF Rules do not prescribe particular ECDD measures to be undertaken in all cases. Your AML/CTF Program should set out the risk-based systems and controls to determine the appropriate measures to apply in the circumstances.



You also need to apply enhanced customer due diligence when you suspect you hold information relevant to the investigation of an offence, or have another suspicion referred to in s 41 of the AML/CTF Act. You must also submit a suspicious matter report (SMR). However, when you submit an SMR, the AML/CTF Act and Rules do not automatically require you to stop providing services to a customer.


The AML/CTF Act also provides protections for reporting entities that comply with reporting obligations. When you have reported information to AUSTRAC in an SMR, (as well as a threshold transaction report, international funds transfer instruction report or in response to a section 49 notice,) you are taken not to be in possession of that information at any time for the purposes of ML, TF and certain other offences against the Criminal Code (section 51 of the AML/CTF Act).

Special considerations for customers regulated by AUSTRAC [H3]

AUSTRAC-regulated businesses, including remitters, DCEs and some fintech businesses, can have particular inherent ML/TF risks due to their underlying customers, the services they provide and the jurisdictions they facilitate money transfers to or from. However, as reporting entities themselves, they are required to implement systems and controls to mitigate their ML/TF risks. Therefore, looking at the inherent risk associated with these industry sectors alone is not a complete picture of an individual business's risk profile.

It is important that you consider the *residual* ML/TF risks presented by AUSTRAC-regulated businesses such as remitters, DCEs and some fintech businesses. Residual ML/TF risk is the ML/TF risks the business poses *after* you take into account the risk-based systems and controls that the business has put in place to mitigate its ML/TF risks.

AUSTRAC does not expect you to undertake a full compliance audit of your customer's AML/CTF program (which sets out the risk-based systems and controls). You are also not required to redo the customer's own ML/TF risk assessment. The level of due diligence you undertake should be appropriate to your understanding of



the residual risk, developed during the establishment of the business relationship with the customer and throughout the course of the business relationship. The key question in assessing residual risk is: do the business's measures to identify, mitigate and manage ML/TF risks appear to be reasonable?

You should consider each customer individually in accordance with your AML/CTF Program including the standard ML/TF risk factors set out in Rule 4.1.3:

- customer type,
- customers' sources of funds and wealth,
- the nature and purpose of the business relationship with your customers,
- the control structure,
- the types of designated services provided, and
- the methods by which you deliver the designated service and the foreign jurisdictions you are dealing with.


The specific factors set out in the following sections may also assist you to understand the residual ML/TF risks of remittance arrangements, digital currency exchanges, and AUSTRAC regulated fintech businesses.

Registration with AUSTRAC [H4]

Remitters and DCEs, including fintech businesses where they provide relevant designated services, are legally required to register with AUSTRAC, unless specifically exempted.

As part of the registration process, AUSTRAC considers whether registration would involve a significant risk of ML, TF or other serious crime. AUSTRAC's consideration is informed by a range of information including:

- national police checks for all key personnel,
- evidence of the knowledge, training and experience of key personnel to support compliance with AML/CTF obligations, and

- 
- any registration information (ABNs, ACNs) and any registration or licensing details related to overseas operations.

Your customer's AUSTRAC registration does not remove the requirement for you to undertake initial and ongoing customer due diligence. However, in the absence of any significant 'red flags' which would suggest otherwise, you should consider the customer's registration with AUSTRAC as a mitigating factor when assessing its ML/TF risks. 'Red flags' may include:

- adverse media or information about key personnel associated with the business,
- evidence of phoenixing, for example, a business appears to have the same key personnel as a recently shut down business in the same sector, or
- evidence that a business has changed ownership or key personnel shortly after AUSTRAC registration without a reasonable explanation.

Financial institutions may wish to ask a remitter or DCE for evidence of registration with AUSTRAC. In the case of remitters, you can verify that they appear on AUSTRAC's [Remittance Sector Register](#). If the business has recently changed owners or other key personnel, you could request evidence from the business that AUSTRAC has been notified of the change.

AUSTRAC regulated businesses, including some fintech businesses, that do not provide remittance or DCE services are not required to register with AUSTRAC. However, they must be enrolled on the Reporting Entities Roll. On a case by case basis, you can ask AUSTRAC for confirmation of enrolment in these cases, if necessary to inform your risk-based decision making. Foreign businesses without a permanent establishment in Australia are not required to register or enrol unless they operate a remittance network in Australia.



Up-to-date and tailored ML/TF risk assessment [H4]

All AUSTRAC regulated businesses must have an enterprise-wide ML/TF risk assessment. Having an up-to-date risk assessment, tailored to the specific circumstances of the business, is essential to mitigating and managing ML/TF risks. Risk assessments should identify and document the ML/TF risks associated with the services they provide, recognising that not all services will present the same risks.

Financial institutions may wish to request and review a copy of the customer's ML/TF risk assessment to consider if it:


- is up to date,
- on its face, reasonably reflects the business's current business model and practices, and
- is tailored to the particular services provided by the business.

If you have questions about a business's ML/TF risk assessment after reviewing the documentation provided by the business, you may wish to request to speak to the business's AML/CTF compliance officer or other senior management to gauge their understanding of the ML/TF risks in their risk assessment. However, you only need to consider this on a risk basis, and it is not required in all cases.

Appropriate AML/CTF systems and controls [H4]

All AUSTRAC regulated businesses must have an AML/CTF program. AML/CTF programs must include risk-based systems and controls to manage and mitigate the risks identified in the business's ML/TF risk assessment. The steps a business takes to mitigate and manage its inherent ML/TF risks are central to determining the residual risk for a business.

AUSTRAC does not expect relationship managers or front line staff in financial institutions to have the expertise to review and assess a customer's AML/CTF program. However, as part of customer due diligence, it is reasonable to ask whether



a regulated business has an AML/CTF program, how it was developed and to seek to understand the priority the business places on implementing it.

In some cases, you may wish to request a copy of the business's AML/CTF program to consider if their systems and controls appear to be what you might reasonably expect to see based on the customer's ML/TF risks.

Examples of good practice could include AML/CTF programs that outline:

- how a remitter's transaction monitoring program applies to transactions involving higher-risk jurisdictions,
- what due diligence remitters and DCEs undertake when establishing relationships with counterparty businesses in other jurisdictions, or
- how a DCE uses blockchain analysis tools where they permit digital currency deposits from, and withdrawals to, external wallets.


This list is illustrative only. It is not exhaustive and is not intended to imply that the listed activities are inherently of concern.

However, if you decide in accordance with your risk-based systems and controls to review a business's AML/CTF program, a generic AML/CTF program template or a copy and paste text from the AML/CTF Rules should not be considered reasonable measures to identify, mitigate and manage ML/TF risks.

Some remitters are affiliates in networks operated by remittance network providers that apply additional AML/CTF policies and oversight. This additional level of scrutiny may assist with reducing the ML/TF risks presented by an individual affiliate. You could seek further information to understand the nature of oversight by the remittance network provider.

The types of customers and services the business provides [H4]

Financial institutions are not required to know your customer's customers. However, where required by risk, customer due diligence requires that financial institutions




understand the nature of the business relationship with your customer. This includes taking a risk-based approach to understanding the *types* of services the business provides and the *types* of customers they have including:

- the usual and expected values of typical remittances, digital currency exchanges or other transactions,
- for remitters, the payment corridors the remitter serves and whether its AML/CTF systems and controls are proportionate to the risks presented by the foreign jurisdictions it deals with. For example, a remitter that primarily facilitates lower-value remittances between family members in lower-risk payment corridors will likely have a lower ML/TF risk profile. Other remittance corridors may require the remitter to have additional systems and controls to mitigate and manage increased ML/TF and/or sanctions risks,
- for affiliates of remittance network providers, the remittance network providers' monitoring of, and support for, the affiliate's implementation of AML/CTF systems and controls. You should also seek to understand whether an affiliate also provides independent remittance services,
- for DCEs, the types of digital currencies exchanged. Different digital currency exchange services may present different risks. For example, if a DCE deals in significant volumes of privacy coins which may be withdrawn from the DCE, this will present specific risks that could require additional risk mitigation by the DCE, and
- for fintech businesses providing other designated services, the nature of the services, the methods by which the fintech business delivers these services and the types of customers that typically use the services.

There is no prescribed way to collect information about these factors. You may use a combination of approaches that could include:

- incorporating relevant questions in your standard customer on-boarding forms,
- a dedicated form with standard questions for on-boarding customers who are remitters, DCEs or fintech businesses, or

- 
- direct engagement and discussion with the business, including its AML/CTF compliance officer.

You may consider supporting these measures with targeted training for relevant product owners as part of your AML/CTF risk awareness training program. Whatever approach is adopted, you must have a reasonable understanding of the residual ML/TF risks presented by the remitter, DCE or fintech business and document your assessment and the outcomes.


Enhanced customer due diligence

Where you determine that a customer that is an AUSTRAC regulated business presents high ML/TF risk, you should consider:

- undertaking a more detailed analysis of the expected level of transaction behaviour, including future transactions, and
- periodically reviewing whether:
 - the customer continues to comply with relevant regulatory requirements, including registration with AUSTRAC if the customer is a remitter or DCE,
 - the customer's ML/TF risk assessment remains up to date and the business continues to set out reasonably appropriate AML/CTF systems and controls in its AML/CTF Program, and
 - you have a current understanding of the types of services the business provides, the types of customers the business provides them to, and the foreign jurisdictions the business deals with.

Ending the business relationship [H3]

Whether you provide financial services to a customer will ultimately be a commercial decision. If you decide not to provide services, or if you decide to discontinue providing services, to a customer after engaging with that customer and considering



possible systems and controls to mitigate any ML/TF risks, AUSTRAC strongly recommends you to:


- in all cases, record the rationale in writing for declining to provide services to the customer if done to comply with your AML/CTF program—AUSTRAC may review such records as part of its supervision of your implementation of risk-based systems and controls,
- where possible, give existing customers sufficient notice of your intention to discontinue providing services to allow them to find an alternative financial institution—AUSTRAC recognises that there may, however, be exceptional situations where this is not possible, and
- where possible, provide meaningful reasons to customers for deciding not to provide financial services—while financial institutions must avoid tipping off customers when suspicious matter reporting obligations arise, informing a customer of concerns about their risk profile in general terms or concerns about their AML/CTF systems and controls are unlikely to amount to tipping off if not linked to specific transactions or patterns of behaviour that gave rise to a suspicion. On the other hand, citing vague 'AML/CTF obligations' or 'tipping off' when speaking to the customer as the reason for declining to provide reasons may, itself, increase the risk of tipping off if the customer could infer from this that an obligation to submit an SMR has arisen.

Scenarios [H3]

Scenario 1: Lawful sex worker customer [H4]

K is a sex worker in the Australian Capital Territory, where sex work is lawful and regulated. K applies for a bank account with Eastern States Credit Union, and discloses their occupation as part of the application process.

Eastern States Credit Union asks for further details, including:

- 
- whether K is employed in a commercial brothel or escort agency—K advises that they are a sole operator and they are not required to be registered or licensed,
 - what revenue K expects, and how K expects to be paid—K provides an estimate and confirms that a large proportion of clients use cash, and
 - what jurisdictions K provides services in—K confirms that they only provide services from premises in the ACT.

Eastern States Credit Union undertakes routine customer screening and determines that there is no adverse information about K.


As K is a new customer with a cash-intensive business model, Eastern States Credit Union decides to apply enhanced due diligence with transaction monitoring tools to detect large fluctuations in deposits, unusually large deposits and cash deposits made to branches outside the ACT. Eastern States Credit Union decides that it will review this risk rating after one year once K has established a transaction history.

Scenario 2: Accepting a DCE customer [H4]

Zecchino Exchange Pty Ltd, a digital currency exchange in the process of setting up business in Australia, applies online for a business transaction account at Serenissima Bank. Serenissima Bank offers general business banking services to Australian customers as an authorised deposit-taking institution.

As part of its application, Zecchino states that it:

- is a digital currency exchange in the process of registering with AUSTRAC—it does not yet provide digital currency exchange services,
- it has undertaken an ML/TF risk assessment and developed an AML/CTF program, and
- its business model is providing digital currency exchange services to Australian resident retail customers who it anticipates will purchase moderate



amounts of digital currency for investment purposes, focusing on 10 popular digital currencies.


Serenissima Bank seeks further information from Zecchino and receives clarification that Zecchino:

- will not offer digital currency exchange services for privacy coins,
- will only accept deposits / withdrawals of Australian dollars to customers' bank accounts held with Australian financial institutions, and
- will permit customers to withdraw and deposit digital currency to and from external wallets, as it anticipates many customers wish to do so to safeguard their digital currency investment. However Zecchino has analysed the risk and has engaged the services of a blockchain analytics company to detect dealings by customers with high risk and sanctioned wallets.

Serenissima Bank decides that as Zecchino is a new business that is still going through the process of AUSTRAC registration that it will request a copy of Zecchino's ML/TF risk assessment and AML/CTF Program. From an initial review of the documents, Serenissima Bank is satisfied that they appear to be professionally developed and align with Zecchino's stated business model. On this basis, no further analysis of the documents is undertaken. Serenissima Bank adds the information to Zecchino's customer file and records its rationale that the documents were reviewed and appeared to be reasonable.

Serenissima Bank's standard adverse media and adverse information screening reveals no concerns about Zecchino's key personnel.

Serenissima Bank agrees to accept Zecchino as a customer, contingent on Zecchino being successful in its application for AUSTRAC registration and providing evidence of this to Serenissima Bank. Until Zecchino confirms that it is registered, Serenissima Bank sets rules in its transaction monitoring system to assure itself that Zecchino has not commenced providing services to retail customers. Upon confirmation of



registration, Serenissima Bank adjusts its transaction monitoring rules for Zecchino to reflect that Zecchino has moved to normal operation as a DCE.

Scenario 3: Declining a bank account due to adverse information

The Bank of Edwardia receives an application by a recently formed company HoenixPay Business Solutions. The Bank of Edwardia offers general business banking services to Australian customers as an authorised deposit-taking institution.

As part of its application, HoenixPay describes its business in vague terms connected with import and export.

In reviewing the application, the Bank of Edwardia:

- seeks further information from HoenixPay about the nature of its business, and receives vague answers despite several requests for clarification,
- asks about the types of customers and geographic locations HoenixPay services and receives evasive answers citing 'commercial sensitivities',
- identifies from social media that one of the managers of HoenixPay, Alice, is the sister of Bob who appears to be connected with a remittance business, and
- undertakes standard adverse media and information screening and discovers that Bob was recently charged with fraud and the AUSTRAC website lists his remittance business's registration as recently cancelled.

The Bank of Edwardia escalates the application internally and determines that it will not take on HoenixPay as a customer. It records the rationale for this decision in writing. The Bank of Edwardia also submits an SMR to AUSTRAC due to suspicions that HoenixPay may be attempting to engage in unregistered remittance activity related to phoenixing.




The role of business customers [H2]

You can increase the chances that financial institutions will provide services to you by being open about the nature of your business and the purposes for which you are seeking to use the financial institution's services. This helps financial institutions to meet their AML/CTF obligations when providing services to you.

If you are unable or unwilling to provide relevant information, your financial institution may be unable to be satisfied that you are not engaging in illicit activity or that your business practices are robust enough to prevent criminals misusing your services

To access the financial services you require to run your business, ensure you provide your financial institution with the information they require to verify that they know who you are and they know and understand the ML and TF risks that may be associated with your business so they can meet their customer due diligence obligations. This includes being prepared to provide information and relevant documentary or electronic evidence to:

- help the financial institution understand the legal structure of your business, and the individuals who ultimately own or control your business,
- describe in sufficient detail the types of services you provide to your customers,
- show that you understand, and have met, all licensing and other regulatory requirements applicable to your business under Commonwealth, state, territory or local laws and any relevant overseas laws,
- share the results of any reviews of your own regulatory and risk management systems and follow-up actions (where permitted),
- share information about the types of customers you provide services to (you do not need to disclose identifying information about individual customers),
- provide details of the geographical locations in which your customers reside and/or the locations to which they transfer value using your services, and

- 
- indicate the expected volumes of transactions you are likely to engage in using the financial institution's services.

Protecting your business, Australia's financial system and the community from criminal abuse is a collective responsibility. You can play your part by providing the information necessary for your financial institution to properly assess, manage and mitigate the risks your business poses for ML/TF. Building a relationship of trust with your financial institution can ensure that your business can operate within the legitimate economy and enjoy the protections of the AML/CTF framework.


The role of remitters, digital currency exchange providers and fintechs, and other reporting entities [H3]

If you are an AUSTRAC-regulated business, e.g. because you operate a remitter, DCE or a fintech business providing a designated service, financial institutions will seek assurance that you are undertaking appropriate due diligence on your customers when providing banking services to you.

Financial institutions do not have a direct relationship with your customers and will therefore consider whether *your business* is taking the required steps to identify, mitigate and manage the ML/TF risks that arise when you provide services to your customers.

You can support financial institutions to be comfortable that you are taking appropriate steps to address the risks associated with your business by being prepared to provide evidence that you are complying with your AML/CTF obligations and are implementing the systems and controls in your AML/CTF program effectively.

If your business provides remittance or DCE services, you must register with AUSTRAC. Failure to register is a criminal offence. AUSTRAC has issued a range of guidance to assist you to determine whether you are required to register and what you need to do to meet your obligations as a registered remitter or DCE:

- 
- [Remittance service providers](#)
 - [Digital currency exchange providers](#)
 - [Preventing financial crime using a risk-based approach](#)

Assess and understand your business's specific ML/TF risks [H4]

Your ML/TF risk assessment should be tailored to your business, including the specific products and services you provide, the types of customers you have, the jurisdictions in which you operate and the different ways you deliver your services. For example, your services will likely involve higher inherent ML/TF risks if your services involve:

- transmitting value into or out of Australia on behalf of customers, or
- providing the means for your customers to transmit value anonymously or pseudo-anonymously, e.g. by allowing them to withdraw large amounts of cash or to withdraw digital currency to self-hosted wallets.


These risks can be mitigated by appropriate risk-based systems and controls and other factors (such as serving low risk remittance corridors), but it is important that your ML/TF risk assessment identifies that the risks exist. You should also refer to any [AUSTRAC risk assessments](#) and other guidance applicable to your sector when identifying the risks faced by your business.

Using an off-the-shelf risk assessment that is not tailored to your business, or assessing that all of the services you provide are low risk, will likely raise questions about whether you truly understand the ML/TF risks of the services you provide and whether you can effectively mitigate those risks.

AUSTRAC has prepared a range of resources to help you assess your ML/TF risks:

Risk assessments and financial crime guides [H5]

- [Independent remittance dealers in Australia risk assessment 2022](#)

- 
- [Remittance network providers and their affiliates in Australia risk assessment 2022](#)
 - [Remittance corridors: Australia to Pacific Island countries risk assessment 2017](#)
 - [Preventing the criminal abuse of digital currencies](#)

Implement an AML/CTF program that is tailored to your assessed ML/TF risks [H4]

Your AML/CTF program must include risk-based systems and controls to manage and mitigate the risks identified in the business's ML/TF risk assessment.


You can assist financial institutions to understand the residual ML/TF risks presented by your business if you are prepared to demonstrate, if asked, that:

- your AML/CTF program was designed specifically for your business and is not an off-the-shelf template or a simple cut and paste of the AML/CTF Rules,
- senior management oversee and support implementation of your AML/CTF program,
- relevant staff in your business, including all customer-facing staff, understand and implement your AML/CTF program and receive appropriate introductory and ongoing training, and
- you have an AML/CTF compliance officer with the seniority, competency and resources to oversee compliance with your AML/CTF program, and who is able to understand, and speak with confidence to a financial institution about, the systems and controls you implement.

AUSTRAC has prepared a range of resources to help you develop your AML/CTF program and ensure appropriate oversight:

AML/CTF programs guidance [H5]

- [AML/CTF programs overview](#)
- [Guide to developing an AML/CTF program for remittance service providers](#)
- [A guide to preparing and implementing an AML/CTF program for your digital currency exchange business](#)



If you use AML/CTF advisers or consultants, you should ensure that they are suitably qualified and experienced. AUSTRAC has prepared guidance to assist you when [engaging an AML/CTF adviser](#).

Ensure your customer due diligence is adequate [H4]

Financial institutions do not have a direct relationship with your customers. When they provide services to you, they are placing trust in your capacity to identify, mitigate and manage the ML/TF risks presented by your customers.


Financial institutions may therefore seek to understand the types of customers you provide services to, and the types of services you provide. This could include understanding the foreign jurisdictions you deal with. This information, together with information about your internal systems and controls, is used to understand the ML, TF and other financial crime risks presented by your business model.

AUSTRAC recognises that this information may be commercially sensitive. However, it can also be essential to help a financial institution determine whether your business is within its risk appetite. Anything you do to increase the transparency of your business, including the types of customers and services you have, will assist financial institutions to assure themselves that your business does not present unacceptable risks.

Be responsive when financial institutions request further information [H4]

Financial institutions may seek further information from you throughout the course of your business relationship with them. This information assists financial institutions to have an up-to-date understanding of your business, and the associated ML/TF risks. Being responsive to such requests will assist financial institutions to meet their obligations.

If you are considering significant changes in your business model, such as a change in ownership or management or providing new services with a different ML/TF risk profile, you could consider proactively discussing this with your financial institution.



These discussions could include outlining your assessment of the ML/TF risks associated with the change and the systems and controls you plan to implement to mitigate those risks.

Related pages

- [AUSTRAC's statement on debanking](#)
- [Financial Action Task Force Statement on the Risk-based Approach and De-risking](#)
- [Financial Action Task Force guidance: Anti-money laundering and terrorist financing measures and financial inclusion](#)
- [\[Links to relevant Commonwealth, State and Territory web sites that provide information about the regulation of sectors not regulated by AUSTRAC\]](#)

Related legislation

- Rule 4.1.3 of the AML/CTF Rules
- Section 36 of the AML/CTF Act
- Chapters 4 and 15 of the AML/CTF Rules
- Section 32 of the AML/CTF Act
- Rule 4.2.2 of the AML/CTF Rules
- Rules 8.1.5(1) and 9.1.5(1) of the AML/CTF Rules
- Rule 4.2.5 of the AML/CTF Rules
- Rule 4.2.8 of the AML/CTF Rules