Australian Government
AUSTRAC

Proposed updated guidance on Enhanced customer due diligence (ECDD) program

Page title	Enhanced Customer Due Diligence
Format	Web content
Audience	All reporting entities

Enhanced customer due diligence (ECDD) program

About this guidance

As part of your initial customer due diligence processes and ongoing monitoring of your customers and their transactions, you must be able to identify whether the money laundering or terrorism financing (**ML/TF**) risk posed by a customer, the business relationship with the customer or transaction(s) is **high**.

Where the ML/TF risk is identified and assessed as high in line with your internally-approved risk appetite, you must apply enhanced customer due diligence (**ECDD**) procedures to understand, mitigate and manage the risks.

This guidance includes best practices to help you mitigate and manage risks you may face when providing designated services to help you to meet your ECDD program obligations.

The guidance relates to situations which pose the highest ML/TF risk and may, in places, exceed the minimum requirements as set out in the AML/CTF Act and Rules. Therefore, this guidance makes reference to where best practice may apply.

This guidance is intended to be general, and not specific to any particular industry sector. You should tailor your ECDD program to meet the specific circumstances you may face when dealing with higher ML/TF risk situations, in line with your approved ML/TF risk appetite, or where you have specific legal obligations imposed under other legislation, for example, that may prevent you from withdrawing services provided to the customer.

Recognising the AML/CTF regime is risk-based, the examples included in this guidance are not exhaustive and are illustrative of how you *may* comply with these obligations.

Commented [A1]: Please see below two overarching bullet points on the document.
- Where there is an expectation for a reporting entity to complete an activity, it would be very useful if AUSTRAC provided the reference to the regulatory requirement.
- Best practice should be separated from regulatory requirements, there are several examples in the draft where best practice is referred to as an expectation without a clear regulatory driver.

Commented [A2]: This will hyperlink to a new proposed glossary term. To review the new glossary term please see **page 19** of this draft.

Commented [A3R2]: This comment is provided by AUSTRAC.

Commented [A4]: If it's best practice, is AUSTRAC suggesting it is a requirement under the ECDD program?

Suggest that this sentence be removed as the main points are captured in the next sentence.

Commented [A5]: The guidance refers to highest / higher and high. Suggest consistency and in keeping with the Act and Rules.

Commented [A6]: We ask AUSTRAC to consider rewording to ***'your risk-based approach'.***

On this page

Commented [A7]: These will hyperlink to the sections below

Commented [A8R7]: This comment is provided by AUSTRAC.

Disclaimer

AUSTRAC provides this guidance for educational purposes only and it does not constitute legal advice. The information in this guidance should be read together with, and not as a substitute for, the AML/CTF Act and Rules.

AUSTRAC does not guarantee, nor accepts any legal liability whatsoever arising from, or connected to, the use or reliance of any material contained in this guidance.

For further information please refer to the Disclaimer on the AUSTRAC website.

Your AML/ CTF program and ECDD

Part A of your anti-money laundering and counter-terrorism financing (**AML/CTF**) program must include an ECDD program that documents high ML/TF risk situations that would trigger ECDD (in accordance with paragraph 15.8 of the AML/CTF Rules).

Commented [A9]: Can AUSTRAC please review and confirm if this should reference ***paragraph 15.9 of the Rules?***

Your AML/CTF program must also document the range of actions you will take, and the additional information you will collect or verify, to carry out the ongoing customer due diligence (OCDD) of the customer.

Commented [A10]: Please confirm if this inclusion is correct? As ECDD is a subordinate to OCDD.

It is best practice for your ECDD program to take into consideration your approved and current ML/TF risk assessment, which identifies the ML/TF risks posed by:

- your customer types (including where appropriate their beneficial owners, politically exposed persons (**PEPs**), and in particular, foreign PEPs and their family members and close associates)
- your products and services
- your business practices and delivery methods/channels, and

Commented [A11]: The wording in this point should be more closely aligned to Part 15.9.2 of the Rules.

- the countries you do business in or with.

Call out box

Governance and oversight

The board and/or senior management of the reporting entity are responsible for determining the approved ML/TF risk appetite of the business. This involves adopting, maintaining and documenting in Part A of the AML/CTF program the appropriate systems and controls to mitigate and manage the full range of ML/TF risks across all designated services.

The board and/or senior management need to understand how the reporting entity operates to comprehensively review the business' risk appetite and be certain that the systems and controls implemented are appropriate and proportionate to deliver the designated service within the business' current risk appetite. This includes having a strong understanding of the size/structure of the business and, engaging in a questioning and challenging mindset of the ML/TF risks the business faces.

For your business to better understand the term senior management, Chapter 1 of the AML/CTF Rules defines senior management by describing a *senior managing official* as an individual who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of a customer of a reporting entity or who has the capacity to affect significantly the financial standing of a customer of a reporting entity.

AUSTRAC acknowledges some reporting entities may formally delegate senior management responsibilities to specified personnel.

For more information, read our insights paper on oversight and governance.

When to apply ECDD

In accordance with paragraph 15.9 of the AML/CTF Rules, you must conduct ECDD when:

- you have determined, having regard to your risk-based systems and controls, that the ML/TF risk is high
- you are providing a designated service to a customer who is (or has a beneficial owner who is) a foreign PEP
- you have formed a suspicion of ML/TF or other criminal activity for the purposes of section 41 of the AML/CTF Act, or

Commented [A12]: Senior management is a concept that is not defined by the AML/CTF Act. Given the Act requires risk-based systems and controls, the definition of senior management should be designed by each reporting entity to appropriately fit that entity's risk-based systems and controls. We therefore suggest not including definitions of senior management in this guidance but rather leaving it to a reporting entity to establish what is appropriate for that particular entity.

Further, we do not think that "SMO" (taken from section 1.2.2 of the AML/CTF Rules) is an appropriate definition for senior management. The definition of SMO is predominantly used in the Rules when determining the identity of a customer's beneficial owner (eg: Part 4.12). It is not used in Chapter 15 of the Rules in the context of who from a reporting entity is "senior management" for ECDD purposes.

Commented [A13]: Can AUSTRAC please confirm if this is actually a legal requirement?

We recognise boards and senior management are tasked with ongoing oversight, but there is no specific obligation for the board or senior management to set the appetite.

Is AUSTRAC intending to introduce new obligations with this guidance?

Commented [A14]: Is the Part A guidance going to cover AUSTRAC's expectations, particularly for entities with multiple systems and controls?

Commented [A15]: Perhaps clarify that this is for 'financial crime risks'? There are many types of business risk appetite; credit risk, market risk etc.

Commented [A16]: This definition is generally applicable to senior managing official within an entity which could be a customer of a reporting entity. Is AUSTRAC suggesting Reporting Entities applying the same definition to determine the "senior management" who should be making the decision on the business relationship and whether to proceed with a transaction relating to high risk customers?

We think it is arguable whether this definition is appropriate from 2 perspectives:

1) From an operational perspective, depending on the size/structure of the reporting entity, it may be challenging to have senior managing official directly engaged for making decision on high risk customer, due to the volume of high risk customer profiles as well.

2) Whether this type of decision really need to be made by the senior managing officials (EXCOs) of the reporting entity who may likely not be close to the customer risk profiles, and impossible to be, again due to the volume of high risk customers. Or the Senior Managing Official should be expanded to capture other non EXCO senior management that have the knowledge/experience and ...

Commented [A17]: Initial review of Insights Paper did not yield details on *delegation.* Recommend that links to other sources observe consistency to the subject matter at hand.

- you are entering into, or proposing to enter into, a transaction and a party to the transaction is physically present in, or is a corporation incorporated in, a prescribed foreign country.

Examples of high ML/TF risk situations may include:

- Complex, unusually large transactions or unusual patterns of transactions, which have no apparent economic or visible lawful purpose and if a suspicion arises as a result. For example, this may include circumstances where you consider the customer's transaction to be inconsistent with their known profile because it is overly complex, unusually large, or involves a transaction or series of transactions with a customer who resides in a prescribed or higher risk foreign country (e.g. the foreign country has inadequate or insufficient AML/CTF measures.
- You identify a customer has complex or opaque beneficial ownership structures which serve no logical business purpose and if a suspicion arises as a result. For example, the customer has an extensive network of companies or trusts which are inconsistent with their business activity, or the corporate structure includes entities which are registered in recognised secrecy or tax haven jurisdictions.
- An existing customer applies for a new product or service and when processing the request, you identify the customer's risk rating should be high. For example, the customer conducts transactions to jurisdictions you have assessed as posing a higher ML/TF risk, or the customer has been identified as a foreign PEP.
- Your transaction monitoring program identifies some anomalies concerning your customer's behaviour and activity. Further investigation reveals a marked increase in their ML/TF risk profile because (a) the value of the customer's transactions have significantly increased and they involve parties that the customer has had no recent known history and if a suspicion arises as result, or because (b) they involve prescribed jurisdictions.
- The service you are asked to provide is for a new customer who is (or has a beneficial owner who is) a foreign PEP, or family member or close associate of a foreign PEP.
- You have submitted a suspicious matter report (SMR) due to a customer's suspicious activity or behaviour.
- You enter into, or propose to enter into a transaction where the other party to the transaction is physically present in, or is a corporation incorporated in, a prescribed foreign country (for example, the Democratic People's Republic of Korea).
- The customer appears to have provided false, misleading or stolen identification documentation or other information as part of the processes in establishing a business relationship and if a suspicion arises as a result.

Commented [A18]: Suggested mark-up has been added to clearly align with 15.9(3) of the Rules.

Commented [A19]: Suggested mark-up has been added to clearly align with 15.9(3) of the Rules.

Commented [A20]: Given there isn't an accredited list of tax haven jurisdictions, suggest changing this to "jurisdictions which have inadequate or insufficient measures in terms of beneficial ownership measures".

Commented [A21]: Suggested mark-up has been added to clearly align with 15.9(1) of the Rules where a customer's overall risk rating becomes high. "Higher than currently assessed" may reference moving an overall customer's risk rating from low to medium, which may not necessarily trigger ECDD alone under R15.9.

Commented [A22]: It may be relevant to include an example that incorporates the use of cash as an elevating risk factor.

Commented [A23]: This point has been marked up, as it doesn't quite align with the other risk situations. Planning to submit may not be an example of a high risk situation if it has been determined that a reasonable suspicion has not been formed?

Common practice is that ECDD is only conducted from reported SMRs, not from potentially submitting an SMR.

Commented [A24]: Suggested mark-up has been added to clearly align with 15.9(3) of the Rules.

Note: A number of the scenarios outlined above may also form the 'reasonable grounds' for suspicion which would require you to submit an SMR (under section 41 of the AML/CTF Act).

You may only need to undertake ECDD on a customer once. However, having regards to the circumstances and your business' risk appetite, you may need to conduct subsequent ECDD if you have ongoing concerns about the customer's behaviour or activity, or in response to material changes in the business relationship. If the customer remains high risk, it is best practice to periodically conduct ECDD in order to monitor and consider changes in risk.

If you or anyone in your business or organisation suspects on reasonable grounds that a customer is not who they claim to be, or the designated service relates to any one of the following: terrorism financing, money laundering, an offence against a Commonwealth, State or Territory Law, proceeds of crime or tax evasion, you must submit an SMR within the required timeframes, regardless of whether you have completed ECDD (as outlined in section 41 of the AML/CTF Act.)

Once ECDD has been completed you may decide to submit further SMR(s), particularly where you identify any additional information, including documentation that enhances your suspicion.

Undertaking ECDD may, for example, identify:

- the assessed ML/TF risk exceeds your approved risk appetite and applying appropriate systems and controls does not mitigate and manage the level of assessed ML/TF risk, or
- continuing the relationship may impact on your reputation and standing.

When these circumstances arise, you may consider engaging senior management, to enable them to make a risk-based decision to either continue the customer relationship, withdraw the designated service from the customer or terminate the relationship altogether.

There are other situations where you may decide to terminate the relationship with the customer, regardless of any ECDD obligation, including forming a suspicion that the customer may be engaged in money laundering and terrorism financing or related activities. You should document the decisions and reasons in all of these circumstances.

How to apply ECDD

Commented [A25]: Hyperlink to below section on 'ECDD and suspicious matter reports'

Commented [A26R25]: This comment is provided by AUSTRAC.

Commented [A27]: We wish to confirm if this already covers the above last bullet, ***"The customer appears to have provided false, misleading…"***

Commented [A28]: If this paragraph is intended to reference ECDD measure 15.10(6) of the Rules, then suggest changing to "may" and removing the reference to "board" as 15.10(6) is only mandatory for foreign PEPs (per R15.11) and it does not refer to board (only senior management).

Commented [A29]: Note reference to Board and/or senior management.

It would be useful if AUSTRAC would clarify if a Reporting Entity can reach its conclusion on the appropriate definition of Senior Management, given Reporting Entity's sizes, risks, and remits at this level can vary significantly. The categorisation with Board indicates a very senior role making these decisions which is not feasible in a large REs (e.g., ADIs), especially given the large number of ECDD cases.

Commented [A30]: AUSTRAC may consider including exceptions for staff safety.

Where you have determined a customer, the business relationship with a customer, or transaction/s presents a high ML/TF risk (as set out in paragraph 15.9 of the AML/CTF Rules) you must apply ECDD measures which are appropriate and proportionate to the ML/TF risk you have identified.

Once you have determined that you need to undertake ECDD, you must undertake measures which are appropriate to the circumstances (as per paragraph 15.10 of the AML/CTF Rules).

You should demonstrate why the ECDD measures undertaken were considered to be appropriate to the ML/TF risk posed and document this in your business records.

For example, if a customer conducting large cash transactions is identified as posing a higher level of ML/TF risk, with activity that is inconsistent with their recent transaction history – and if as a result a suspicion arises, it would be inappropriate to only undertake customer identification and verification measures. A more prudent option would be to consider and assess the customer's source of funds.

- The benefits of ECDD

Your ECDD program should provide you with a deeper and greater understanding of your customers and their assessed ML/TF risk. In particular, undertaking ECDD can provide you with more certainty about the identity of the customer and/or beneficial owner(s), and clarity about whether the purpose of the business relationship and the customer's reasons for conducting the transaction are consistent with their assessed risk profile.

Carrying out ECDD plays an important role in detecting, disrupting and preventing money laundering and terrorism financing and can protect your business or organisation from being exploited for criminal purposes. Information obtained from carrying out ECDD can help you identify suspicious activity, or determine whether a transaction or behaviour is suspicious, which would require you to submit an SMR to AUSTRAC.

For example, your ECDD program should assist you to:

- clarify if there is a need for a complex beneficial ownership structure or if it has no obvious business purpose other than being opaque in order to conceal the true beneficial ownership and control of the customer
- clarify and determine whether a customer's source of wealth and funds are legitimate and can be established using reasonable measures
- distinguish between customers that have a high risk profile but are not involved in ML/TF (for example, a foreign PEP), as opposed to customers whose

Commented [A31]: Hyperlink to the section above which specifies these circumstances per para 15.9 of the Rules.

Commented [A32R31]: This comment is provided by AUSTRAC.

Commented [A33]: Hyperlink to 'Record keeping' section belowe

Commented [A34R33]: This comment is provided by AUSTRAC.

Commented [A35]: Operationalising this may prove too much of a burden to justify ECDD application to each individual case. Recommend removing sentence, as a result. However, clarity welcomed on whether applicable to individual cases or as a broad framework.

Commented [A36]: It may be relevant to include an example that incorporates the use of cash as an elevating risk factor.

Commented [A37]: Suggested mark-up has been added to clearly align with 15.9(3) of the Rules.

Commented [A38]: ECDD is triggered by a suspicion arising (15.9(3)) of the Rules. If a suspicion arises, it would trigger ECDD and the reporting entity would complete that ECDD and possibly update an SMR if additional information becomes available as part of ECDD.

Commented [A39]: Added reference to "reasonable measures" in line with 15.10(1) & (2) of the Rules.

Commented [A40]: Mentions highest/higher interchangeably - specificity on application of gradings would help.

transactions or behaviours may be linked to ML/TF or other criminal activity, and

- consider whether there are sufficient grounds to form a suspicion and if so, submit an SMR to AUSTRAC (under section 41 of the AML/CTF Act). Once any suspicion has been formed you must submit the SMR within the required timeframes, regardless of whether the ECDD has been completed. In these circumstances you can submit a further SMR where you have identified any additional information which supports your suspicion.

Commented [A41]: AUSTRAC should consider and/or? If not, does this infer all instances of ECDD require an SMR?

What to include in your ECDD program

Your ECDD program should be informed by your approved and current ML/TF risk assessment.

Having regard to paragraphs 15.9 and 15.10(1) to (7) of the AML/CTF Rules, it is best practice for your ECDD program to include:

- triggers when ECDD is required, for example, as a consequence of changes in the customer's risk profile, activity or behaviours, or where the customer engages with a higher risk product or service
- the ECDD measures that you may apply to mitigate and manage the risks; and
- appropriate risk-based systems and controls.

It is best practice for your ECDD program to:

- define the types of customers, designated services, channels and jurisdictions that you assess as posing a high level of ML/TF risk leveraging your approved and current ML/TF risk assessment
- include clear and consistent triggers that prompt when to apply and implement ECDD processes in accordance with the risk-based approach;
- identify who in your reporting entity is responsible for carrying out ECDD assessments
- establish appropriate risk-based systems and controls to consistently apply ECDD and ensure its effective operation through internal reporting and monitoring, and
- ensure that there are appropriate and effective governance, oversight and approval processes consistent with your AML/CTF program, that enables you to demonstrate the actions you have taken. This includes provision for reporting to the board and/or senior management and operational areas, where appropriate.

Commented [A42]: AUSTRAC should consider rewording to ECDD/SMR are triggered by the four scenarios in the 15.9 of the Rules.

The steps taken to carry out ECDD must be appropriate to the circumstances, including a range of measures as outlined in Paragraph 15.10 of the AML/CTF Rules, namely:

- obtaining more information
- conducting more detailed analysis of customer information
- verifying or re-verifying a customer's identity and the customer's beneficial owner information
- conducting more detailed analysis and monitoring of transactions
- seeking approval from senior management to continue a business relationship with a customer or whether a designated service should continue to be provided to a customer..

Commented [A43]: The requirement in 15.10(6) of the Rules is to seek senior management approval on whether a designated service should continue to be provided to a customer.

Obtain more information

When conducting ECDD, you may need to obtain further information from the customer or a third party to ensure an appropriate and proportionate response to understanding the nature and character of the ML/TF risk. This can include:

- Clarifying or updating existing customer or beneficial owner information already collected from the customer and seeking additional independent, reliable sources to verify this information. For example, this may include asking the customer to provide additional information through their advisers, explanatory correspondence on letterhead, certified financial statements or tax returns.
- Obtaining further customer identification (also known as know your customer, or "**KYC**") information or beneficial owner information, where appropriate, including on the source of the customer's funds and wealth. For example, this might include taking reasonable measures such as:
    - making inquiries about how the customer or beneficial owners acquired their wealth, in order to be satisfied it is legitimate and not based on the proceeds of crime
    - taking reasonable measures to establish the source of the customer's funds. For example, this can include assessing, where applicable, whether the customer has a profile on social media which may contain details of their employment and other useful background information
    - where applicable, taking additional steps to understand the background, ownership and financial situation of the customer, and other parties to a transaction, and
    - increasing the level of screening through reliable sources such as reputable media, watch lists, and public data bases (e.g. sanctions lists).
- Clarifying the nature of the customer's ongoing business relationship by:
    - considering information which may already be held across your organisation, for example, information contained in a credit assessment report

Commented [A44]: We note, 15.10(1) & (2) of the Rules require taking reasonable measures to ***identify*** as opposed to ***establishing*** SOW/SOF.

- assessing and ensuring you are satisfied the information and activity relating to the customer is consistent with the purpose and intended nature of the business relationship, and
- requesting additional information or a more detailed explanation from the customer (or their advisers) where the activity is inconsistent with the purpose and intended nature of the business relationship.

- For customers who are identified as posing a high risk which may include due to their connection to an identified prescribed foreign country, in line with best practice, you should consider obtaining:
  - additional information on the customer and the ultimate beneficial owner(s)
  - additional information on the intended nature of the business relationship
  - information on the source of wealth and source of funds of the customer and the customer's beneficial owner, and
  - details of the purpose and reason for the transactions.

Commented [A45]: Amended to align with 15.9(1) of the Rules.

Commented [A46]: Clarity should be given where '**best practice**' is called out in this Guidance, that it **aligned** to the Act and/or Rules and not necessarily requiring a reporting entity to implement additional frameworks to comply.

More detailed analysis of customer information

You may also decide to undertake a more detailed analysis of the customer's KYC information. This involves, where appropriate, taking *reasonable measures* (meaning measures which are practical and necessary in line with your identified ML/TF risks) to determine the source of the customer's (and beneficial owner's) funds and wealth.

Commented [A47]: Amended to align with 15.0(2) of the Rules.

Verify and/or re-verify customer and beneficial owner information

You may decide it is appropriate to re-verify customer and/or beneficial owner information, consistent with your obligations under Part B of your AML/CTF program and customer identification procedures.

If you decide to re-verify customer information as part of ECDD, you must ensure your checks are based on reliable and independent documentation or electronic data.

More detailed analysis and monitoring of transactions

You may decide to examine and monitor the customer's past and future transactions where appropriate, including:

Commented [A48]: May not be relevant to examine all the factors in the list.

- the purpose and reason for transactions
- the nature of specific transactions
- their types and frequency
- whether the transactions are suspicious, or
- the expected nature and levels of your customer's transactions, including any future transactions.

Seek approval from senior management

You may decide it is appropriate to seek senior management approval to determine whether to:

- continue a business relationship with a high risk customer, including foreign PEPs and family members or associates of the PEP
- continue providing designated services to a high risk customer
- Your ECDD program should include policies and procedures outlining in what circumstances senior management approval will be required.

Note: In accordance with best practice, AUSTRAC expects that you document and keep records of the ECDD activities you have carried out, and the outcomes of each assessment. This includes documenting senior management decisions at every stage, including the reasons behind each decision.

Commented [A49]: Can we please clarify the interpretation of change? Does it mean that reporting entities may determine to seek senior management approval, when appropriate, which does not have to be all the cases for high risk customers and/or transactions involving high risk customers. Recognising for large REs, this may be very difficult on the volume of these matters, and for delegation.

We would appreciate further clarification from AUSTRAC on the definition of the "senior management".

Commented [A50]: This expectation is linked to a best practice section. However, there is no requirement in the link provided or the Rules to maintain records of each assessment at every stage.

If you cannot complete ECDD or mitigate or manage the ML/TF risk

There may be circumstances where you carried out, or attempted to carry out, your ECDD measures, but you are still not satisfied you have sufficiently mitigated and managed the ML/TF risk, and the customer or their activities remains high risk. In these circumstances, you will need to consider what additional steps are necessary in order to mitigate and manage the risk posed.

Commented [A51]: Please confirm, is this paragraph intended to cover situations where the customer becomes an unacceptable risk rather than a high-risk which is manageable?

This may involve deciding whether it is appropriate to proceed or not with a transaction, reconsider the customer's risk rating or cease providing designated services to the customer.

Accordingly, your ECDD program should outline the relevant procedures, policies, systems and controls (including the role of senior management), to be applied in situations when ECDD, or customer identification and verification obligations, cannot be successfully conducted. It is important you appropriately record where these outcomes occur.

If you are unable to successfully conduct ECDD you should also consider whether there are sufficient grounds to form a suspicion and submit an SMR to AUSTRAC, and engage with senior management. This may include circumstances where a suspicion arises due to a combination of factors such as:

- relevant information is not able to be obtained from customer or third party searches do not yield any results when conducting ECDD
- the customer was unknown or was a non-account customer and left the premises before ECDD could be conducted, and
- the customer refused to provide further information when conducting ECDD.

Commented [A52]: Please confirm if this list is intended to be cumulative (i.e., all the factors occur in one scenario)?

When to conduct ECDD again

As part of your ongoing customer due diligence and transaction monitoring processes, and consistent with your risk-based approach, you must regularly review your customer's details, account activity and transaction behaviour. The purpose of these regular reviews is to ensure the customer's transactions and activity remain consistent with your knowledge and understanding of the customer, their business and risk profile, and their business relationship with you.

In order to ensure the monitoring and analysis of customer transactions is proportionate to the ML/TF risk which has been identified, it is necessary for you to review the activity and transactions of a higher risk customer on a more regular basis.

In determining whether to apply subsequent ECDD, you should consider your customer's current level of ML/TF risk. For example, subsequent ECDD may be appropriate in the following situations:

- a review of a high-risk customer's KYC information, account activity and transaction behaviour reveals their level of ML/TF risk remains high
- a review of a low or medium risk customer's KYC information, account activity and transaction behaviour reveals the ML/TF risk profile has increased to high risk since the last assessment, for example, where your customer asks for new and higher risk products or services.

However, the same scenarios could also result in a customer's risk no longer being high – in which case, it is not necessary to conduct subsequent ECDD.

Whenever there is a material change in the nature and purpose of your customer's business relationship which changes the customer's risk profile to high ML/TF risk, you should consider whether subsequent ECDD is required.

Commented [A53]: Can AUSTRAC please provide examples, outside transaction monitoring and OCDD, how this could be achieved.

Commented [A54]: Amended to align with R15.9(1)

ECDD and suspicious matter reports

In accordance with paragraph 15.9(3) of the AML/CTF Rules, you must apply ECDD when a suspicion is formed for the purposes of section 41 of the AML/CTF Act.

ECDD should commence, *where possible*, prior to the SMR being submitted.

Submitting an SMR to AUSTRAC does not manage the ongoing risk of a customer or alter the fact that a customer is or will remain a higher risk, unless you apply your AML/CTF systems and controls.

You must submit an SMR within the required timeframe regardless of whether the ECDD has been completed. If appropriate, you may submit subsequent SMRs containing additional information identified relevant to the initial SMR.

Tipping off

When conducting ECDD, in circumstances where grounds for a suspicion have been formed (or an SMR has been provided to AUSTRAC), care must be taken when communicating with your customers or any third parties to ensure you do not disclose any information about the report.

Commented [A55]: Please consider noting that ECDD records should not include content that could be considered 'tipping off' if a customer (or other third party) sought access to these records.

Under the AML/CTF Act, it is a criminal offence to tell the customer or any person other than AUSTRAC you have formed a suspicion about their activity or have submitted an SMR to AUSTRAC. It is also an offence to provide any information which may reasonably cause the person to reasonably infer a suspicion has been formed or an SMR submitted. This is referred to as 'tipping off'.

The tipping off offence is not intended to stop you from conducting ECDD on a customer once you have formed a suspicion. In most circumstances, you should be able to perform ECDD as part of your AML/CTF program without tipping off the customer.

Read more about your tipping off obligations, including the limited exceptions to the tipping off offence including where a disclosure is made to State and Territory police and other Australian law enforcement agencies.

Call out box

Asking the customer for more information, including about their identity or the source or destination of their funds, is not considered 'tipping off' and can often be managed in a way which avoids alerting the customer. However, when you form a suspicion about a customer, you should identify any risk of tipping off before performing ECDD and consider ways to manage that risk.

If you cannot apply a specific ECDD measure because it would tip off the customer, you can still perform a range of alternative ECDD measures, including the use of in-house or third party information sources, or confirming whether the customer has a presence on social media channels. Where you decide not to perform a particular ECDD measure to avoid tipping off a customer, in line with best practice, you should engage with senior management or a delegate and document the outcomes and reasons for this decision.

Commented [A56]: We suggest adding a delegate as engaging with senior management to whether or not to perform a certain ECDD measure is not covered under the Rules, and will depend on the organisations risk based systems and controls.

Once you form a suspicion about a customer, be discreet when conducting ECDD. You must not disclose you have submitted, or are obliged to submit, an SMR to

AUSTRAC, or any information from which it could be reasonably inferred you intend to or have submitted an SMR.

Record keeping

It is best practice to maintain records of what ECDD measures you have undertaken, including when the measures were undertaken, the reasons for each decision, and any outcomes.

You should also keep copies of all the information, data and documents you have used to verify (where verification is applicable) your customer's identity and details, their beneficial ownership (if applicable) and their source of wealth and funds.

It is also recommended that you keep records of any findings which justify the level of verification you completed and the reasons behind your decisions. For example, you should record the reasons why you decided to delay undertaking ECDD on a customer, or why you decided to escalate a transaction monitoring alert to an SMR after conducting ECDD. This information can be used to demonstrate: the processes, considerations and outcomes arising from conducting ECDD, whether you have formed a suspicion, that you can apply appropriate measures to mitigate and manage the ML/TF risk, or the basis of withdrawing designated services to the customer.

You should document all senior management decisions concerning the outcomes of your ECDD assessments and the reasons behind each decision. This includes those situations where the ECDD conducted provided you with no further information or clarity, or information legitimising your customer's activity, or resulted in a decision not to submit an SMR.

Self-assessment questions

These self-assessment questions are not exhaustive but have been developed to assist and guide you in meeting your obligations.

- How do your ECDD measures and processes differ from standard customer identification and verification?
- How effectively are the risks flagged during the customer identification and verification process followed up and resolved?
- Do you have clearly documented guidelines indicating which ECDD measures would be appropriate in certain situations, or in relation to certain ML/TF risks?

- Are your ECDD processes adequately documented, including your decision making process, review process and outcomes?
- Do your processes and policies clearly set out the responsibilities, including decision-making, of staff and senior management concerning your ECDD obligations?
- How is ECDD information gathered, analysed, used and stored? Is this also documented?
- Do you have clearly documented guidelines on your processes where attempts to undertake ECDD cannot be completed, or where ECDD undertaken did not satisfy you that the ML/TF risk posed was mitigated or managed?
- What involvement does senior management have in continuing or discontinuing relationships with high risk customers? What information do they receive to inform any decision-making in which they are involved?
- Has your board and/or senior management signed off on your ECDD program and are they required to approve of any revisions and updates?
- In accordance with your AML/CTF program requirements, when was the last time the independent review included an assessment of your ECDD processes and procedures?

Examples of good and bad practices

Good practices	Bad practices
• The ECDD program, as part of your Part A program, is approved by the board and/or senior management and clearly documents the business's requirements to be followed and the roles and responsibilities of staff and senior management, and includes a mechanism for regular independent reviews in accordance with the Part A AML/CTF program obligations.	• The business does not have a documented set of requirements for undertaking ECDD and the ECDD program only comprises the cut and pasting of relevant AML/CTF Rules (in particular, 15.9 and 15.10). It does not outline the detailed processes and procedures, roles and responsibilities and has not been submitted for board and/or senior management sign-off.
• The AML/CTF compliance officer has a general awareness and understanding of high-risk customers and reports regularly to senior management, consistent with the ECDD program obligations.	• Senior management do not take responsibility for making decisions to continue or terminate relationships with high risk customers.
• Your business establishes and documents, the source of wealth	• No distinction is made between conducting source of wealth

Commented [A57]: Amended to align with 15.9 of the Rules .

and source of funds used in high risk business relationships, and where a suspicion is formed, submit an SMR.	checks and source of funds checks.
• Where the ML/TF risk of the customer is identified as being high, the reporting entity uses a range of internal and external resources, including staff knowledge, to collect more information in order to make an informed decision.	• No distinction is made between conducting ECDD on a customer deemed to pose a higher risk, compared to the standard checks conducted for low/medium risk customers at on boarding.
• The reporting entity has kept records and can provide evidence it has collected, assessed and documented ECDD outcomes involving higher risk customers, including decisions made to continue or terminate the customer relationship by senior management.	• There is no record of decisions, including those by senior management, to continue or terminate the relationship with the customer.
• The reporting entity can clearly demonstrate an assessment of ECDD information and its impact on the customer's ML/TF risk.	• The reporting entity considers the credit risk of the customer but not the ML/TF risk.
• For a customer which the reporting entity has ongoing concerns about, it undertakes further ECDD measures and gather new information about the customer, proportionate to the risks posed. If there is an ongoing concern, and depending on the circumstances, the reporting entity considers whether an SMR needs to be submitted or whether to cease the relationship with the customer.	• For a customer which the reporting entity has ongoing concerns about, the same ECDD measure is conducted each time, despite it not gathering any new or additional information about the customer or preventing their activity.

Commented [A58]: Adding *'has'* to make narrative more accurate.

Examples

High risk jurisdictions

A reporting entity's transaction monitoring program identifies a customer receiving a transaction from a jurisdiction identified as high risk in the reporting entity's ML/TF risk assessment and a suspicion arises. Given the suspicion formed, the reporting entity's ECDD obligation is triggered, and the compliance officer considers which ECDD measure is most appropriate in the circumstances. The compliance officer decides to conduct more detailed analysis on the customer's transactions, with a particular focus on any previous transactions involving high risk jurisdictions, to determine the purpose or reason for the particular transaction. After examining the customer's past transactions, the compliance officer decides this transaction is inconsistent with the customer's usual behaviour and transaction history, and determines this to be suspicious, requiring an SMR to be provided to AUSTRAC. The compliance officer prepares and submits the SMR, including details of the suspicious transaction, the analysis conducted, and the reasons why this transaction is suspicious. The compliance officer recognises that submitting the SMR does not mitigate or manage the high risk of the transaction, and decides to enhance the monitoring and scrutiny of the customer's future transactions.

Commented [A59]: Amended to align with 15.10(3) of the Rules.

Pubs and clubs

A cashier attendant at a registered gaming club observes a customer approaching other patrons on the gaming floor and attempting to purchase their winning electronic gaming machine tickets. The cashier identifies this as suspicious and reports the behaviour to the manager on duty. After reviewing CCTV surveillance footage, the duty manager confirms the behaviour is suspicious, triggering the reporting entity's ECDD obligation. The duty manager considers which ECDD measure is most appropriate to the circumstances and decides to obtain more information about the customer's identity. In order to avoid alerting the customer of the suspicion and obtain the required additional information, the duty manager reviews additional CCTV footage to determine the customer's entry time, to corroborate with the identification the customer used to enter the premises. They search social media to collect additional information on the customer. The duty manager then completes and submits an SMR to AUSTRAC, including details of what the cashier observed; what was observed on CCTV; details of the identification the customer presented on arrival; and, the outcomes of social media searches. The duty manager also includes this information in a shift report, which is shared with the reporting entity's compliance officer. The compliance officer identifies that the venue has previously submitted SMRs on the customer for the same behaviour, and determines that this falls outside of the reporting entity's approved risk appetite. The compliance officer, being in a senior management position, determines it is appropriate to terminate the relationship with the customer, and issues a venue ban should the customer return. The compliance

officer briefs the board and other senior management on this decision, recording the agreed outcome and rationale.

Superannuation account activity inconsistent with customer profile

Transaction monitoring identifies a large non-concessional contribution deposited into a customers' superannuation account. The superannuation fund undertakes a review of information already held on the customer and assesses the contribution amount to be inconsistent with their known profile which it decides requires further investigation. The superannuation fund determines it is appropriate to obtain further KYC information and contacts the customer asking for further information about the source of the funds. The customer advises their employer sent the funds as a paid bonus, which the customer corroborates by providing a pay slip. The superannuation fund determines this is not suspicious and therefore does not warrant an SMR being reported to AUSTRAC. The superannuation fund keeps a record of the rationale for this decision, including the customer-provided information.

Related pages

- AML/CTF programs overview
- Customer identification: Know your customer (KYC)
- Money laundering/terrorism financing risk assessment
- Transaction monitoring
- Source of Funds/Source of Wealth
- Suspicious Matter Reporting
- Tipping off
- Politically exposed persons

Related legislation

Section 36 of the AML/CTF Act (latest version) – Ongoing customer due diligence

Parts 15.8 to 15.11 of Chapter 15 of the AML/CTF Rules (latest version) – Enhanced customer due diligence

Section 41 of the AML/CTF Act – Reports of suspicious matters

Proposed new web content

Page title	Glossary
Format	Web content – new glossary term to be added to: https://www.austrac.gov.au/glossary/r
Audience	All reporting entities

Risk appetite

Risk appetite is the level of risk a reporting entity is willing to accept in the pursuit of its broader economic, commercial and operational objectives, and before any action is determined to be necessary in order to reduce the risk. The board and/or senior management of a reporting entity are responsible for determining the approved ML/TF risk appetite of the business.

The ISO Guide 73:2009 Risk Management – Vocabulary defines risk appetite as the '… amount and type of risk that an organization is willing to pursue or retain'.

A risk appetite can allow reporting entities to determine how much of a risk they are willing to take (including financial and operational impacts) in order to innovate in pursuit of their defined objectives.