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

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 and terrorism financing (ML/TF) risk posed by a customer, the business relationship or transaction(s) is high. Where the risk is identified as high, you must apply enhanced customer due diligence (ECDD) procedures to understand, mitigate and manage the ML/TF risks.

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. Your AML/CTF program must also document the range of actions you will take, and the additional information you will collect or verify, for the ongoing due diligence of the customer.

Your ECDD program must be informed by 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 their family members and close associates)
- your products and services
- your business practices and delivery methods/channels, and
- the countries you do business in or with.

Commented [PR1]: "With the customer?" the business relationship reference here can be very broadly defined.

Commented [PR2]: Comment 1: We suggest the use of "must" throughout the guidance be reviewed as there are instances where "might" or "may" would be more appropriate and better aligned with the law. While "must" is appropriate where it reflects a legislative obligation, might or may is preferable where the points are designed to guide the risk based approach.

Governance and oversight

For the board and/or senior management to effectively lead and embed a positive culture of AML/CTF compliance, they must be fully engaged with the AML/CTF compliance and risk management process. This involves much more than just having AML/CTF as a standing agenda item for meetings. The board and senior management are expected to engage, question, challenge and take ownership of any ML/TF risks the business faces and determining the reporting entity's risk appetite. This includes making informed decisions on whether to continue providing designated services to a customer who poses an unacceptable level of risk and any changes to the risk appetite.

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

Commented [PR3]: We note the definition of "senior management" may vary amongst reporting entities, depending on the size/scale/structure of the organisation.

Also, in practice the "senior management" may delegate the authority as per what is permitted within each entity's policy.

Also suggest changing the highlighted reference to and/or as it will depend on the scale and nature of the org and whether the board or senior management are engaged at this level of granularity.

When to apply ECDD

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

Commented [PR4]: May?

- you have determined, having regard to your risk-based systems and controls, that the ML/TF risk is high; or
- you are providing a designated service to a customer who is (or has a beneficial owner who is) a foreign politically exposed person, or
- you have formed a suspicion of ML/TF or other criminal activity, or
- 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 include:

Commented [PR5]: Consider suggesting that the drafting of the first bullet point should align with the Act:

"'complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.' "

- circumstances where you consider the customer's transaction to be overly complex, unusually large or there is an unusual pattern of transactions which has no apparent logical business purpose, lend themselves to anonymity, or

Commented [PR6]: Suggest changing the leading sentence to "Examples of situations which may bring higher ML/TF risk"

customer resident in a higher risk foreign country (e.g. the foreign country has inadequate or insufficient AML/CTF measures)

- you identify that a customer has complex or opaque beneficial ownership structures that serve no logical business purpose
- an existing customer applies for a new product or service and there are indications that the risk associated with an existing business relationship may have increased
- your transaction monitoring program identifies that your customer's behaviour or activity does not match their current ML/TF risk profile
- the service you are asked to provide is for a new customer who is (or has a beneficial owner who is) a foreign politically exposed person (PEP), or family member or close associate of a foreign PEP
- a customer's suspicious activity or behaviour has, or may, lead you to submit an SMR
- a transaction or business relationship involves a person or a company that has a presence in, or is incorporated in, a high risk or prescribed foreign country
- customers are using, or seek to use, new and developing technologies or products that allow the customer a level of anonymity
- where the customer has provided false, misleading or stolen identification documentation or other information as part of the processes in establishing a business relationship.

You may only need to undertake ECDD on a customer once. However, you may need to conduct subsequent ECDD of the customer if you have ongoing concerns about the customer, or in response to material changes in the business relationship with your customer.

How to apply ECDD

Where you have determined that a customer, business relationship, or transaction presents a high ML/TF risk, you must apply ECDD measures that are appropriate and proportionate to the ML/TF risk you have identified.

Commented [PR7]: Increased to make it high risk? Increased risk is relative and does not in itself warrant ECDD.

Also is this intended to cover situations where a customer applies for a new product, and when processing that request the RE realises the customers existing relationship is higher risk than previously thought? Or is it because the new product inherently changes the risk profile?

Would be great to clarify with an example.

Commented [PR8]: this scenario may not necessarily mean that the customer's ML/TF risk rating should be high, without further investigation. If this scenario specifically is covering for suspicious activity or behaviour identified, bullet point 6 on SMR lodgement covers this.

Commented [PR9]: The other bullet points appear to cover the scenarios where there is suspicious activity. This appears to be a catch all.

Commented [PR10]: Suggest removal of "may" here is too broad, suggest deletion.

Commented [PR11]: Suggest this bullet point is amended to align with 15.9(4) by removing the references to "business relationship" and to "high risk [country]" and keeping it limited to wording in 15.9(4).

Commented [PR12]: 1. This is an indicator only of channel risk, but does not indicate necessarily overall high ML/TF risk; and
2. What does "a level of" mean in practice?
3. Can AUSTRAC provide an example of new and developing technologies they are trying to capture?

Commented [PR13]: This appears to be a scenario where the customer could and should be exited and not retained with ECDD. Welcome AUSTRAC clarity here as a circumstance for offloading.

Also could this be expanded to where a customer refuses to provide information requested.

Commented [PR14]: Consider if a couple of examples would assist here e.g. one where ECDD is only required once and another where ongoing ECDD is required.

Commented [PR15]: Referring to the highlighted para, suggest a reference to the AML/CTF Rules 15.9 for customer, business relationship or transaction may present high ML/TF risk, and since "must" has been used, the wording should be more in line with the requirement in the legislation.

Commented [PR16]: Suggest reference in this paragraph to "business relationship *with a customer*"

You must be able to demonstrate and record that the ECDD measures undertaken were considered to be appropriate to the ML/TF risk posed and that the extent of the ECDD measures you apply was considered is proportionate to the ML/TF risks

For example, if a customer conducting large cash transactions is identified as posing a higher level of ML/TF risk, it would not be appropriate 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 will provide you with a 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, and clarity about whether the purpose of the business relationship and the customer's reasons for conducting the transaction are legitimate.

Carrying out ECDD also allows you to decide on reasonable grounds whether a suspicious matter report (SMR) should be provided to AUSTRAC. Accordingly, ECDD plays an important role in detecting, disrupting and preventing money laundering and terrorism financing. It also protects your business or organisation from being exploited for criminal purposes.

For example, your ECDD program will assist you to:

- clarify whether complex beneficial ownership structures are legitimate and intended to facilitate business; or whether they are deliberately complex and 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 or if they are derived from the proceeds of crime
- distinguish between customers that have a higher risk profile but are not involved in ML/TF (for example, a foreign PEP), as opposed to customers

Commented [PR17]: Does this mean legal in this context? Or, merely consistent with the usual pattern of customer activity.

Commented [PR18]: Based on the AML/CTF Rules 15.9, ECDD is required to be undertaken after SMR obligation arises.

Commented [PR19]: More that ECDD is to confirm whether the correct beneficial owner is identified. ECDD has no comment to make on the structure of the BO,

Alternatively, suggest this be rephrased to:

"Clarify if there is a legitimate need for the complex beneficial ownership structure, or if it has no obvious purpose other than being opaque in order to conceal the true beneficial ownership".

whose transactions or activities may be linked to ML/TF or other criminal activity
- determine whether there are sufficient grounds to form a suspicion and submit a suspicious matter report (SMR) to AUSTRAC.

Commented [PR20]: Suggest replacing with "reasonable grounds" to align with s 41.

What to include in your ECDD program

Your ECDD program must:

- define the types of customers, designated services, channels and jurisdictions that you consider as posing a higher level of ML/TF risk, and include clear and consistent triggers that prompt the application and implementation of ECDD processes in accordance with the risk-based approach
- specifically identify who in your reporting entity is responsible for carrying out ECDD;
- incorporate 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
- outline the ECDD measures that you will apply
- establish appropriate risk-based systems and controls to consistently apply ECDD and ensure its effective operation through internal reporting and monitoring
- ensure that there are appropriate and effective governance, oversight and approval processes.

Commented [PR21]: As noted in page 1, the following is not explicitly prescribed in the legislation/rules. If these represent regulatory expectations on "good practice" for implementing ECDD, the word "must" should be softened to "may"

Commented [PR22]: Should this be defined under the ML/TF risk assessment?

This is inconsistent to the following stated in page 1 of the draft guidance.

"Your ECDD program must be informed by your approved and current ML/TF risk assessment, which identifies the ML/TF risks posed by....."

Commented [PR23]: We would propose that it is the respective risk assessment(s) that defines the types of customers, designated services, channels, and jurisdictions that a reporting entity considers as posing a higher level of ML/TF risk.

Commented [PR24]: In larger entities, ECDD may be conducted by many different business units. It is unclear for what purpose this would be required other than to identify the executive with overall responsibility.

The steps taken to carry out ECDD measures must be appropriate to the circumstances, and may include a range of measures as outlined in Rule 15.10, including:

- obtain more information
- conduct more detailed analysis of customer information
- verify and re-verify customer and the customer's beneficial owner information
- conduct more detailed analysis and monitoring of transactions both past and future.

Commented [PR25]: As ECDD is a range of measures, this should be changed form 'will apply' to 'may apply'

Commented [PR26]: This may be set out in the AML/CTF Program and not specifically the ECDD Program.

Commented [PR27]: 3rd bullet point below should be amended to 'verify **or** re-verify'

- seek approval from senior management to proceed with or reject the transaction or to continue or terminate the relationship with the customer.

Note: You must document and keep records of the ECDD activities you have carried out, and the outcomes of each assessment. This includes documenting the decisions made by senior management at every stage, including the reasons behind each decision.

Obtain more information

When conducting ECDD, you may need to obtain further information from the customer or a third party. This may 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
- 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 [take reasonable measures to]:
    - 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
    - establishing the source of the customer's funds to ensure it is not acquired from the proceeds of crime
    - taking additional steps to understand the background, ownership and financial situation of the customer, and the parties to the transaction
    - increasing the level of screening of 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 be already held across your organisation, for example, a credit assessment report

Commented [PR28]: Whilst we acknowledge that a similar position has been taken by AUSTRAC under current ECDD guidance in relation to Senior Management approval for transactions, is the intention of this dot point to extend rule 15.10(7) to Rule 15.10(6)?
i.e., There is no requirement, under rule 15.10(7), for Senior Management approval of "considering whether a transaction or particular transactions should be processed"

Commented [PR29]: We seek confirmation that this is a legislative requirement justifying a "must" here. While REs will in practice do this, there does not appear to be a legislative basis. We suggest that wherever must is used, that a legislative provision is referenced.

Commented [PR30]: Consider moving the reference re "seeking independent, reliable sources to verify this information" under the heading "Verify-re-verify customer and beneficial owner information" (pg. 7) as it appears to be more aligned to rules15.10(3) and 15.10(4)

Commented [PR31]: It might be clearer here to exclude the second part of this sentence on whether it is not acquired from the proceeds of crime because the RE responsibility is to establish the source of funds and report where REs suspect the funds are acquired from the proceeds of crime. Whether funds are proceeds of crime is a matter for law enforcement, and not something an RE can "ensure."

- taking additional steps to assess and be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship
- requesting additional information or a more detailed explanation from the customer where the activity is inconsistent with the customer's existing risk profile

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

Commented [PR32]: Suggest the following amendments to the bullet points to prevent duplication and focus on the objective of this measure:
- assess and be satisfied that **information and activity** relating to the customer is consistent with the purpose and intended nature of the business relationship
- requesting additional information or a more detailed explanation from the customer where information or activity is inconsistent with the **purpose and intended nature of the business relationship**

Commented [PR33]: Suggest changing "high risk foreign country" to "prescribed foreign country" to align with R15.9(4)

More detailed analysis of customer information

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

Verify and re-verify customer and beneficial owner information

Commented [PR34]: Or?

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, Customer identification.

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, including:

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

Seek approval from senior management

Your ECDD program must include policies and procedures outlining where senior management approval is required in relation to the following situations where it involves high risk customers:

- 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
- process a transaction for/relating to a high risk customer on an account.

The reasons and the outcomes, including who made the decisions, must be clearly documented.

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

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

Commented [PR35]: "Must" comment as per earlier noted. If a legislative requirement then would be good to align with the relevant legislative provisions. Otherwise, should be softened to "may"

Also, senior management approval is one of the ECDD measures in section 15.10, however, we understand reporting entities may take a risk based approach to determine which ECDD measures to apply as appropriate. Section 15.9 states the scenarios when the reporting entities must apply the ECDD, which are
• Customer assessed as high risk
•Customer/BO who is identified as foreign PEP
• SMR obligation has arisen
•Transactions involve party in a prescribed country.

Commented [PR36]: Whilst we acknowledge that a similar position has been taken by AUSTRAC under current ECDD guidance in relation to Senior Management approval for transactions, is the intention of this dot point to extend rule 15.10(7) to Rule 15.10(6)?
i.e., There is no requirement, under rule 15.10(7), for Senior Management approval of "considering whether a transaction or particular transactions should be processed"

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

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 that you appropriately record where these outcomes occur.

If you are unable to conduct ECDD you should also consider whether to submit an SMR to AUSTRAC and engage with senior management in this matter.

Commented [PR37]: Could this be expanded on? What are the circumstances where AUSTRAC considers an RE is unable to conduct ECDD (i.e. tipping off concerns? Customer refusal to provide further information?)

When to conduct ECDD again?

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

You should ensure that the monitoring and analysis of customer transactions is proportionate to the ML/TF risk that has been identified. It is necessary that you 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 that 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 that the ML/TF risk profile has increased since the last assessment, e.g. where your customer asks for new and higher risk products or services.

Commented [PR38]: To high-risk?

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, you should consider whether subsequent ECDD is required.

ECDD and suspicious matter reports

You must apply ECDD procedures where a customer's activity or behaviour form the grounds for suspicion following which you will submit an SMR. Submitting a 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 systems and controls.

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 that you do not disclose any information about the report.

Under the AML/CTF Act, it is a criminal offence to tell the customer or any person other than AUSTRAC that 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 that 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 circumstances to the tipping off offence where a disclosure is made to State and Territory police and other Australian law enforcement agencies.

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 that 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 consider that applying a specific ECDD measure 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. Where you decide not to perform a particular ECDD measure, to avoid tipping off a customer, you should document the reasons for this decision.

Once you form a suspicion about a customer, be discreet when conducting ECDD. You must not disclose that you have submitted, or are obliged to submit, an SMR to AUSTRAC, or any information from which it could be reasonably inferred that you intend to or have submitted an SMR.

Commented [PR39]: Is there any additional guidance that AUSTRAC can provide on the types of questions that may risk tipping off or alternatively, questions that an entity could ask without risk of tipping off.

Record keeping

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

involved at each stage of the process and any outcomes.

Commented [PR40]: We seek confirmation that this is a legislative requirement justifying a "must" here. While REs will in practice do this, there does not appear to be a legislative basis. We suggest that wherever must is used, that a legislative provision is referenced.

You must also keep records on any findings that 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 it was decided to escalate a transaction monitoring alert to an SMR after conducting ECDD.

You should accurately document all decisions by senior management 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 lodge an SMR.

Self-assessment questions – ECDD

Commented [PR41]: The start of the document does not describe as self-assessment? Seems odd introducing it near the end of the doc.

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 risks that are 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?
- When was the last time your ECDD processes and procedures were independently reviewed?

Commented [PR42]: As part of the independent review of the Part A program, or is this a separate process?

Examples of good and bad practices

Good practices	Bad practices
• The ECDD program is approved by the board and/or senior management and clearly documents the business's specific processes and procedures to be followed and the roles and responsibilities of staff and senior management, and includes a mechanism for regular independent reviews.	• The business does not have a documented set of procedures or processes for undertaking ECDD and 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 senior management sign-off.
• The AML/CTF compliance officer has oversight of all 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 higher risk customers.

Commented [PR43]: should this be part of the Part A program for the independent review, rather than documented separately under ECDD?

Commented [PR44]: This should be "and/or" as it will depend on the size and nature of the organisation whether it is appropriate for both board and senior management for signing-off.

Commented [PR45]: What does oversight mean here? If we are referring to a general understanding of high risk customers, is that sufficient? For large entities with thousands of high risk customers, oversight of specifics of each customer is not possible.

It might also be useful to refer here to a team that is delegated this oversight function

• Your business establishes the legitimacy of, and documents, the source of wealth and source of funds used in high risk business relationships.	• No distinction is made between conducting source of wealth 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 customer on boarding.
• The reporting entity has kept records and can provide evidence that 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 considers the credit risk of the customer has been considered but not the ML/TF risk.
• For a customer that the reporting entity has ongoing concerns about, it agrees to increase ECDD measures undertaken and gather new information about the	• For a customer that the reporting entity poses ongoing concerns, the same ECDD measure is conducted each time, despite it not gathering any new or

Commented [PR46]: Reporting entity's responsibility is to establish the source of funds and report where REs suspect the funds are acquired from the proceeds of crime and Whether funds are proceeds of crime is a matter for law enforcement, and not something an RE can "ensure."

Commented [PR47]: If there is ongoing concern (which could result in SMR), should reporting entity also consider whether to cease the customer relationship?

Commented [PR48]: Undertake additional ECDD measures?

customer, proportionate to the risks posed.	additional information about the customer or preventing their activity.

Related pages

- AML/CTF programs overview
- Customer identification: Know your customer (KYC)
- Money laundering/terrorism financing risk assessment
- Transaction monitoring
- 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

Australian Government
AUSTRAC

Proposed updated guidance on Employee due diligence and Employee AML/CTF risk awareness training

Page title	Employee due diligence
Format	Web content
Audience	All reporting entities

Employee due diligence

Employee due diligence means screening your employees to make sure they do not pose a money laundering or terrorism financing (ML/TF) risk to your business.

Commented [PR1]: This description appears to be too narrow. It would be clearer and more accurate to reword this paragraph/section to refer to 'EED Program' and provide a brief summary of the applicable AML/CTF Rule requirements i.e. screening, re-screening and consequences for employees.

Screening your employees involves checking their background in order to determine their suitability for the role, making sure they are who they say they are and confirming the information they have provided is true and correct. It is expected that you will engage employees who possess the necessary skills, knowledge and expertise to carry out any anti-money laundering and counter-terrorism financing (AML/CTF) functions or responsibilities effectively.

Commented [PR2]: It is not clear how this refers to the applicable screening EDD requirement and appears to instead refer to general suitability.

You must have an employee due diligence (EDD) program in place which documents your risk-based systems and controls for how you will screen and rescreen employees who may be in a position to facilitate an ML/TF offence in connection with the provision of a designated service.

Your EDD program must also document the steps you will take in circumstances where an employee fails to comply with your AML/CTF program.

Identifying roles that pose a risk to your business

As part of your EDD program, you must have a process to review all roles within your business to ascertain which positions pose a risk to your business and can facilitate a ML/TF offence. This will enable you to identify where you should apply your EDD processes.

You can ask prospective and existing employees to provide you with the necessary information to assist you in assessing their suitability for the role. For example, this can take the form of a questionnaire requiring the prospective or existing employee to declare that the information they have provided to you is true and correct.

You should review and independently verify the information provided by the prospective or existing employee.

Your EDD program is an important component of Part A of your AML/CTF program. It must be based on the ML/TF risk assessment of your business or organisation and the employees' roles. AUSTRAC expects that you consider the risks identified in your ML/TF risk assessment and relate these risks to the roles performed by your employees. Your AML/CTF program must explain the processes, systems and controls you have established to mitigate and manage risk, including how you will screen your prospective employees, which roles you will screen and when and how you will re-screen an existing employee.

Which employees to screen and re-screen

At a minimum, you must screen or re-screen any employee whose role may put them in a position where they could facilitate ML/TF. Screening and re-screening processes and frequency should be risk-based and not prescriptive.

Depending on the structure of your business, this will include board members (directors), executives, senior managers, officers, and contractors.

This also includes:

Commented [PR3]: We suggest this should align with the rules and simply state:

... have appropriate risk based systems and controls to ascertain .. whether, and in what manner, to screen prospective employees (or those being promoted or transferred).

Commented [PR4]: For the existing employees, can AUSTRAC please clarify if this is more for the scenario where existing employees moving to a new role that requires re-perform the suitability assessment.

Commented [PR5]: It is not clear how this refers to the applicable screening/re-screening EDD requirements and appears to instead refer to general suitability.

Commented [PR6]: On a risk basis?

Commented [PR7]: While this may be best practice, it is not in the rules and suggest it be rephrased to reflect this as best practice rather than mandatory.

Commented [PR8]: Suggest that this section state that 'employee' is not defined in the AML/CTF Act or Rules and that the Guidance is providing possible examples. We do not suggest a definition is required, but it is important to note.

We also suggest that all references to non-employees (i.e., board members, executives, consultants, senior managers, officers, contractors, etc) be removed to avoid confusion. The AML Rules are limited to "employees" and it depends on the particular legal engagement whether a person is an "employee"

Commented [PR9]: In the AML/CTF Rules Part 8.3 and Part 9.3, it is for reporting entity to apply risk based approach, to determine, whether to, and in what manner to, screen and re-screen prospective and existing employees.

Commented [PR10]: Does the reference to board members include non-executive directors?

employees (including executive directors and senior managers), officers, and contractors
prospective employees who, if employed, may be in a position to facilitate a ML/TF offence
existing employees whose role or duties may enable them to facilitate the commission of a money laundering or financing of terrorism offence
existing employees prior to being transferred or promoted to a position which may enable them to facilitate a ML/TF offence.

How to screen employees

To screen both prospective and existing employees you should consider the following steps:

identify and verify their identity
confirm their employment history and qualifications (for example through original or certified documents, written references or referee reports)
undertake character and background checks to confirm their employee history and past conduct
consider reviewing a licence that may have been issued to them by another government agency in Australia which involves a Fit and Proper Person (FPP) test and where you can confirm the check has been conducted to a suitable level
decide whether they are suitable for the position and assess whether they pose a risk to your business or organisation, and
consider requesting that they conduct a National Police Check.

Employee self-disclosure of material changes to their circumstances

As part of your EDD program, you may consider requiring employees to self-disclose material changes in their circumstances that may have an impact on their suitability for their current role. This may include, for example, circumstances where the employee is being investigated, charged or prosecuted for a criminal offence, if there

have been significant changes in their financial arrangements or where they are proposing to undertake secondary employment.

You may also consider adopting a regular review process where the employee is asked to provide a self-attestation or submit updates concerning any material changes to their circumstances since their initial or last EDD assessment.

National Police Checks

If you are considering requesting prospective or existing employees to undertake a National Police Check, it is strongly recommended you access the Australian Federal Police National Police Checks web page. This provides employers and applicants with further details on how to obtain a National Police Check through the AFP, including fees, an application completion guide, and frequently asked questions covering consent and the Commonwealth Spent Convictions Scheme.

The Australian Criminal Intelligence Commission also maintains a list of Accredited bodies to assist you to apply for and submit a National Coordinated Criminal History Check. These accredited bodies are also authorised to submit checks on behalf of organisations to assist these organisations with the screening of their employees (see Legal Entity Customers).

Self-attestation

You can ask prospective and existing employees to provide you with the necessary information to assist you in assessing their suitability for the role. This can take the form of a questionnaire requiring the prospective or existing employee to declare that the information they have provided to you is true and correct.

Commented [PR11]: As per comments above, it is not clear how this refers to the applicable screening/re-screening EDD requirements and appears to instead refer to general suitability.

You should review and independently verify the information provided by the prospective or existing employee.

High-risk roles

Some roles in your business or organisation might pose a higher ML/TF risk than others (for example, roles with duties that might make the employee a target for collusion or coercion by associates involved with criminal groups). You must apply more rigorous checks for these roles.

For example, you might consider checking whether the prospective or existing employee:

- has a criminal record (only in relation to convictions or offences that are relevant to the inherent requirements of the role) by requesting them to conduct and consent to provide you with the outcomes of a National Police Check
- is or has been subject to any regulatory, court or legal action
- has taken advantage of the laws of bankruptcy for their own benefit
- is a director or office bearer of a company by searching the ASIC data base
- can provide details of independent referees for the purposes of character references and background checks
- has lived in high-risk countries or regions
- is a politically exposed person (PEP) or is named on a sanctions list or is the subject of any adverse media reports
- has secondary employment or business interests that may present ML/TF risks.

Having collected and assessed this information, you will need to determine whether the person is suitable for the role in accordance with the risk profile of the position.

Conducting the checks

It is important that the persons you use to conduct background checks on prospective or current employees have the appropriate skills and experience to perform this function. It is also expected that you document the outcomes and decisions made regarding these employee due diligence assessments.

Employees who don't comply with your AML/CTF program

Commented [PR12]: Is the use of 'must' here consistent with the applicable AML/CTF Rules?

The requirement is to have appropriate risk based systems and controls.

Commented [PR13]: General comment - some of these are more conflict of interests than they are relevant to ML/TF risk.

It would be good to clarify which need to form part of EDD and which are just good practice

Commented [PR14]: It is not clear why this is a relevant consideration and therefore suggest it is revised accordingly or omitted.

Commented [PR15]: Suggest this section also refer to third parties and tools that may be utilised by a reporting entity to conduct background checks.

Your EDD program must also set out the steps you will take if an employee fails to comply with your AML/CTF program.

This might include mandatory training to refresh their knowledge of your AML/CTF program, or disciplinary action, depending on the seriousness of the breach. Disciplinary action might range from formal warnings to dismissal.

You must also document the outcomes of any procedures that are applied in the event that an employee fails to comply with your AML/CTF program.

Review of your employee due diligence processes

You should ensure that your EDD processes are reviewed regularly, including independent reviews.

Any changes made to EDD processes should be documented and include the reasons for the change and the senior manager responsible for approving the revisions.

Self-Assessment Questions

These questions have been developed as a guide only to assist you in determining whether your business is complying with its obligations.

- What is your approach to the screening of employees in accordance with your EDD obligations?
- Do the screening processes and management of different employees (including members of the board and senior management) reflect the ML/TF risks to which their role is exposed?
- How do you assess the effectiveness of your EDD processes?
- How often are your EDD processes reviewed and updated and do you record and document any changes or revisions?

Examples of good and bad practices

Commented [PR16]: Consider if the EDD Program can simply rely / cross reference HR policies that address this.

The Rules state that EDD program 'must establish and maintain' a system for employee who fail to comply.

Not a specific Part A requirement to set it all out in the EDD program.

Commented [PR17]: When it comes to dismissing employees for breaches of the AML/CTF program, how can REs deal with such employees where an SMR obligation arises.

There are also circumstances where an employee is dismissed as a customer of the RE for transactional behaviour where an SMR is required.

There are difficulties in both instances in relation to tipping off that we welcome guidance on.

Commented [PR18]: Is the use of 'must' here consistent with the applicable AML/CTF Rules?

Commented [PR19]: Should these questions also cover the other applicable EDD requirements for re-screening and consequences for employees?

Commented [PR20]: If our screening identifies a 'negative' response to any of the questions, irrespective of the risk rating of the role, would this still be relevant for AML/CTF purposes? For example, a role may not be a customer facing role, i.e. does not permit access to customer records, however the employee has a criminal record. The role itself may not be susceptible to the commission of a ML/TF offence and hence not rated as 'high'. In this scenario what would be the risk for ML/TF?

Commented [PR21]: Suggest dot point is revised in line with comments above regarding 'employee'.

Good practices	Bad practices
Temporary employees are subject to the same levels of employee due diligence processes as permanent employees.	Failure to assess all positions in the business to determine the risks posed to the reporting entity and the level and frequency of the EDD processes that should apply to each position.
Employees employed in higher-risk roles are subjected to higher levels of employee due diligence.	The conduct of EDD is a one-off process and fails to identify changes that could affect an individual's suitability for the role.
Where employment agencies are used, periodically satisfies itself that the agency is adhering to the agreed EDD processes.	Only screening employees in senior management and board roles while failing to screen operational employees.
A robust framework is maintained to ensure any employee's non-compliance with internal AML/CTF policies or processes is managed and resolved.	Not subjecting staff to re-screening when they move into a higher ML/TF risk role.
Records are maintained for decisions made and actions taken in accordance with EDD program.	There is no clear documented audit trail of reviews and changes or enhancements to your EDD processes.

Commented [PR22]: The contractor may subject to the same levels of EDD as permanent employee, where applicable.

For example, a contractor may not have a permanent employee record for the ABA check.

Commented [PR23]: Is this consistent with the applicable AML/CTF Rules?

Employee due diligence examples

Medium-risk role example

An **administrative officer** may have some opportunity to facilitate the commission of a ML/TF offence by, for example:

- having access to, and the ability to amend, customer information and transaction and account data
- being responsible for uploading and processing payments, including cash transactions
- performing customer due diligence processes.

Noting the above, you may determine this role poses a medium risk to your business. For a medium risk, your EDD checks may involve:

- reference checks from previous employers a character reference
- if appropriate, consider requesting the prospective or existing employee to conduct a National Police Check
- a bankruptcy search.

Higher-risk role example:

A **manager** may have significant opportunity to facilitate a money laundering or financing of terrorism offence by, for example:

- having authorisation over the investment and release of funds corresponding directly with potential or existing customers
- having the authority to change processes, such as temporary exemptions or a manual work-around to protocols
- managing and authorising outsourcing or contracting arrangements
- having access to highly sensitive business or customer information.

Noting the above, you may determine this role poses a high risk to your business. For a high risk employee, your EDD checks may be expanded to include:

- a sanctions and Politically Exposed Person (PEP) check (such as a World-Check or equivalent)
- an ASIC company directorship check, and
- a check to determine if they have been or are subject to disciplinary action by a regulatory agency.

These examples of EDD measures are not intended to be exhaustive.

Employee AML/CTF risk awareness training program

You must provide anti-money laundering and counter-terrorism financing (AML/CTF) risk awareness training for your employees to ensure that your employees understand and are aware of:

- your business's obligations under the AML/CTF Act and Rules
- the consequences of non-compliance with the AML/CTF Act and Rules
- the type of ML/TF risk the business might face and the consequences of such risk the business's AML/CTF processes and procedures that employees must carry out.

Part A of your AML/CTF program must include processes, systems and controls to provide tailored ML/TF risk awareness training for employees and to help you make sure your business isn't used to support illicit or criminal activity.

You should:

regularly review your training program to ensure it covers changes to ML/TF risk or the level of ML/TF risk your business faces

ensure that it reflects the current AML/CTF legal framework document any recommended enhancements arising from the review processes.

Your AML/CTF risk awareness training program

Your AML/CTF risk awareness training program must be documented and provide details on how your employees are trained on:

- your obligations under the AML/CTF Act and Rules
- the consequences of not complying with your obligations under the AML/CTF Act trends, methodologies and techniques of money laundering and terrorism financing relevant to your business and the designated services you provide the type of ML/TF risks your business may reasonably face and the consequences of these risks insights into your ML/TF risk assessment including the vulnerabilities of your business' products and services how you meet your obligations, including your systems and controls to identify, mitigate and manage these risks the roles and responsibilities of relevant persons in your organisation concerning the operation and maintenance of your AML/CTF program and risk assessment, including the AML/CTF compliance officer how to identify suspicious activity and transactions and prepare and submit suspicious matter reports (**SMRs**) relevant industry guidance.

Who needs training and how often?

You should give all your employees regular AML/CTF risk awareness training, including board members, directors, operational staff contractors and consultants who are involved in providing designated services to your customers.

Commented [PR24]: It is not clear if the use of 'must' here is intended to also capture the following dot points. If so, this section should be redrafted to use 'must' only in relation to the applicable AML/CTF Rules requirements.

Commented [PR25]: Welcome further clarity here - We assume this includes a range of FCC staff, including front-line staff, back office consultants - but it would be good to make this clear.

The content and frequency of the training will depend on their roles in the organisation and the ML/TF risks your business may face.

Employees should be aware of the changing behaviours, techniques and practices used by money launderers and those engaged in terrorism financing, including having knowledge of relevant risk assessments and risk profiles. This information can be incorporated into training materials, including special purpose training provided when you introduce a new product, service or technology. You should also take into account any changes to the AML/CTF regulatory framework including the AML/CTF Act, Rules and Regulation and any enforcement updates from AUSTRAC that may be relevant to your business.

Training may also be triggered by certain events, such as:

- employees moving between jobs or responsibilities
- new methodologies or indicators relevant to your business emerge, including new information about ML/TF risks in your sector
- failure by employees to comply with your AML/CTF program
- feedback or guidance issued by AUSTRAC on ML/TF risk in your sector, e.g. AUSTRAC Financial crime guides
- feedback from AUSTRAC on your business's AML/CTF compliance.

Program logistics

Your written program must detail how you will run your AML/CTF risk awareness training program for employees. It should include:

- which employees need training, such as new employees, employees being promoted or transferred, senior managers, consultants and new directors
- what the training intends to achieve
- the frequency of the training
- the delivery methods of the training
- relevant training and completion dates

Commented [PR26]: Is this best practice or an obligation at law? It would be good as a general practice to ensure the language is clear throughout on this point.

Commented [PR27]: We query need to specify the delivery method in the Program, particularly given delivery methods change from time to time and might result in needing board approval for a change in delivery method.

Commented [PR28]: It is not clear what this means. It might be too much detail to include what the training modules are in the program.

whether and how employees are to be assessed following the completion of the AML/CTF risk awareness training.

Types of training

You can determine the types of training you provide for employees based on your ML/TF risks.

Options may include:

- online training courses
- in-house or external training with an instructor
- on-the-job training, especially if the risks are specific to a certain role
- induction training for new employees and existing employees who take on new roles or positions
- regular communication to employees via email, notices or bulletins about any changes or updates to your ML/TF risk systems, controls and procedures, including appropriate follow-up with employees to ensure that the information has been read and understood.

Self-Assessment Questions

These questions have been developed as a guide only to assist you in determining whether your business is complying with its obligations.

- Do your employees have access to training on an appropriate range of ML/TF crime risks?
- How do you ensure that training is of a consistent quality and reflects current trends?
- Is the training tailored to particular roles?
- How do you assess the effectiveness of your training?

Examples of good and bad practices

Good practices	Bad practices
Tailored training is in place to ensure that employees' technical knowledge is adequate and up to date. Employees have easy access to policies and procedures.	Training materials and logs are not kept up to date and are not accessible to employees.
Training covers practical examples, uses actual case studies and provides information on how to comply with policies.	Training is provided by an external provider who has no understanding or knowledge of the specific risks, systems and controls relevant to the business.
Training covers the consequences of non-compliance with processes and policies.	Training is not tailored and does not include the specific ML/TF risks identified by the reporting entity
Refresher training is provided to ensure that employees remain up to date with changes to ML/TF risks, policies and procedures, and changes to the legal framework.	Training is too broad/high level or is not role-specific, so staff are unclear what ML/TF risks and AML/CTF policies and procedures relate to their role.
Training includes some form of testing on completion and the results are used to assess individual training needs.	Training is infrequent and refresher training provides no new information or content each time.

Related legislation

Part 8.2 of the of the AML/CTF Rules (latest version) – AML/CTF risk awareness training program (standard programs)
Part 9.2 of the of the AML/CTF Rules (latest version) – AML/CTF risk awareness training program (joint programs)