

# AML/CFT

Anti-money laundering and countering financing of terrorism

# Enhanced Customer Due Diligence Guideline

September 2020



## Structure of the Enhanced Customer Due Diligence guideline

	Introduction	Page 3
	Terms used in this enhanced CDD guideline	Page 4
Part 1	Enhanced customer due diligence	Page 5
Part 2	Enhanced CDD and identity requirements	Page 12
Part 3	Circumstances when enhanced CDD applies	Page 14
Part 4	Source of Wealth and Source of Funds	Page 18
Part 5	Enhanced CDD and Politically Exposed Persons	Page 21
Part 6	Table of Abbreviations and Acronyms	Page 22

## Introduction

1. This guideline assists you to conduct **enhanced customer due diligence (enhanced CDD)** on your customers under the **Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the Act)**.
2. The Act sets out a number of specific situations in which enhanced CDD is required. In addition, enhanced CDD is required when you consider, based on your **money laundering and terrorism financing (ML/TF) risk assessment (risk assessment)**, that the level of risk involved means that enhanced CDD should apply.
3. Enhanced CDD requires the collection and verification of the same identity information that is required for standard customer due diligence. However, when undertaking enhanced CDD, you may need to use increased or more sophisticated measures to do this. In most, but not all, cases enhanced CDD also requires the collection and verification of information relating to the **source of wealth (SoW)** or **source of funds (SoF)** of your customer.
4. This guideline does not address enhanced CDD requirements for wire transfers and correspondent banking relationships.
5. Your **AML/CFT programme (programme)** must outline how your business will determine when enhanced CDD is required for a customer and when other types of customer due diligence are permitted.
6. A risk-based approach allows you some flexibility in the steps you take when conducting enhanced CDD. Your risk assessment and programme will determine the amount of time and effort you spend on enhanced CDD.
7. A risk-based approach does not stop you from engaging in transactions/activities or establishing business relationships with higher risk customers. Rather, it should help you to effectively manage and prioritise your response to ML/TF risks.
8. Examples provided in this guideline are suggestions to help you meet your obligations under the Act. They are not exhaustive and are illustrative in nature.
9. This guideline has been produced by the AML/CFT supervisors under section 132(2) of the Act. It cannot be relied on as evidence of complying with the requirements of the Act. This guideline does not constitute legal advice.
10. Section 57(2) of the Act requires you to have regard to this guideline, it is important that you have read and taken this guidance into account when developing your AML/CFT programme. After reading this guideline, if you still do not understand any of your obligations you should contact your AML/CFT supervisor or seek legal advice.
11. Where AML/CFT guidance material is referenced, it can be accessed at the following websites:

**Department of Internal Affairs:**

<http://bit.ly/2gQ3lev>

**New Zealand Police Financial Intelligence Unit:**

<http://bit.ly/2zpmWPJ>

**Reserve Bank of New Zealand:**

<http://bit.ly/2n6RYdp>

**Financial Markets Authority:**

<http://bit.ly/2hV45oJ>

## Terms used in this enhanced CDD guideline

12. The Act does not define the terms set out below. For the purposes of this guideline, the following definitions apply.

**“Reasonable steps”**: Refers to an objective view of what actions would be proportionate and suitable given the risks involved and the obligations of the Act. For instance, the level of identity verification you undertake on your customer.

**“Material change”**: ML/TF risk is not static and a customer’s ML/TF risk profile can change quickly. A material change is an event, activity, or situation that you identify during interactions with your customer (or via ongoing customer due diligence and account monitoring) that could change their level of ML/TF risk. This may result in the need for enhanced CDD.

**“Risk-based approach”**: Refers to the proportionate AML/CFT measures that you implement in response to identified risks. An effective risk-based approach (sometimes called RBA) allows you to exercise informed judgement when conducting enhanced CDD on your customers. Under a risk-based approach, there is no such thing as “zero risk”.

**“According to the level of risk”**: Consistent with a risk-based approach, this refers to your assessment of ML/TF risk associated with your customer.

**“Inherent risk”**: This is the assessed ML/TF risk before any AML/CFT controls and measures are in place.

**“Residual risk”**: This is the assessed ML/TF risk after AML/CFT controls and measures have been put in place.

13. All footnote references refer to the AML/CFT Act 2009 unless stated otherwise.

14. On 1 July 2018, **suspicious transaction reports (STRs)** were replaced by **suspicious activity reports (SARs)**. We use the acronym SAR to denote both types of reporting for the purposes of this guideline.

## Part 1: Enhanced customer due diligence

### What is enhanced CDD?

15. **Customer due diligence (CDD)** is a cornerstone of your programme. CDD is the process through which you develop an understanding of your customers and the ML/TF risks they pose to your business.
16. In some higher ML/TF risk circumstances an increased level of CDD is required. This is known as **enhanced CDD**, “**ECDD**” or “**EDD**”. As part of standard CDD, you **must** obtain sufficient information to determine whether you require enhanced CDD on your customer.<sup>1</sup>
17. Enhanced CDD has two core requirements over and above standard CDD:
  - You may need to use increased or more sophisticated measures to obtain and verify your customer’s details, their beneficial ownership structure, and the details of representatives and other key persons. You **must** take reasonable steps to do this according to the level of risk involved.<sup>2</sup> (This is covered in Part 2 of this guideline.)
  - You should usually obtain and verify information relating to the **source of wealth (SoW)** or **source of funds (SoF)** of your customer.<sup>3</sup> The circumstances in which you need to do this are detailed within the Act.<sup>4</sup> You **must** take reasonable steps to do this according to the level of risk involved.<sup>5</sup> (This is covered in Part 4 of this guideline.)
18. You **must** base your programme on your risk assessment. Your programme **must** contain your enhanced CDD procedures, policies and controls that manage and mitigate the ML/TF risks presented by your customers.<sup>6</sup>

### Why is enhanced CDD required?

19. Enhanced CDD is required for certain types of customers and some transactions or activities. This includes situations where you consider (based on your risk assessment) that the level of risk involved is such that enhanced CDD should apply.<sup>7</sup>
20. For instance, enhanced CDD helps you:
  - Determine whether complex beneficial ownership structures are legitimate and intended to facilitate business or if they are deliberately complicated to hinder investigation and conceal the identity of the beneficial owners.<sup>8</sup>
  - Determine whether a customer’s SoW or SoF are legitimately derived, or intended for legitimate use, or whether there are reasonable grounds to suspect it may be the proceeds of crime.
  - Distinguish between a customer that has a higher risk profile but is not involved in ML/TF, as opposed to a customer whose transactions or activities may be linked to ML/TF.

---

1 Section 17(b)

2 Sections 16(1) and 24(1)(b)

3 Sections 23(1)(a), 26(2)(b) and 26(3)

4 Section 22

5 Sections 23(1)(a), 24(1)(b), 26(2)(b) and 26(3)

6 Sections 57(1)(c) and 57(1)(j)

7 Section 22(1)(d)

8 Section 5

- Comply with the requirement that SARs are reported to the **New Zealand Police Financial Intelligence Unit (FIU)**.

## When is enhanced CDD required?

21. There are various circumstances set out in the Act where enhanced CDD is required. These circumstances may apply to a customer that is seeking to conduct an occasional transaction or activity with you, or a new customer you are establishing a business relationship with. You should usually conduct enhanced CDD on your customer before any activities or transactions have commenced. Exceptions can apply – see paragraphs 47-49.
22. Enhanced CDD may also be required at subsequent points during a business relationship as part of your ongoing CDD and account monitoring procedures.<sup>9</sup>

## When must enhanced CDD be conducted for new customers?

23. You **must** conduct enhanced CDD when taking on certain types of new customer. This includes establishing a business relationship with a customer or if a customer seeks to conduct an occasional transaction or activity.
24. Customers that **must** have enhanced CDD are:<sup>10</sup>
  - A trust or another vehicle for holding personal assets
  - A non-resident customer from a country that has insufficient AML/CFT systems or measures in place
  - A company with nominee shareholders or shares in bearer form
  - A politically exposed person (PEP)
  - A customer seeking to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose
  - Any other customer or circumstances that you assess (based on your risk assessment and standard CDD) to be of high ML/TF risk<sup>11</sup>
  - A business relationship with a customer that involves new or developing technologies, or new or developing products, that might favour anonymity
  - A customer seeking to conduct an occasional transaction or activity through the reporting entity that involves new or developing technologies, or new or developing products, that might favour anonymity.
25. Unless you have doubts about the adequacy or veracity of the information, data and documents that you have obtained and verified relating to your customer, you are not required to conduct enhanced CDD again.<sup>12</sup> However, enhanced CDD could be required again as a result of any material changes in your business relationship with your customer or due to ongoing CDD and account monitoring.

---

<sup>9</sup> Section 31

<sup>10</sup> Section 22

<sup>11</sup> Section 22(1)(d)

<sup>12</sup> Section 11(4)

## When must enhanced CDD be conducted again?

26. As part of your ongoing CDD and account monitoring processes you **must** regularly review your customer's details, account activity and transaction behaviour.<sup>13</sup> This is to ensure that it is consistent with your knowledge and understanding of their business and risk profile, as well as their business relationship with you. You should be more frequent and thorough in your scrutiny of a higher risk customer's transactions and activities than those of a lower risk customer.
27. You **must** have regard to your customer's ongoing level of ML/TF risk,<sup>14</sup> which will determine if enhanced CDD is required. If, as part of your ongoing CDD, you identify any of the following situations you should conduct enhanced CDD:
- A review of a high-risk customer's account activity and transaction behaviour shows that their level of ML/TF risk remains high
  - A review of a low- or medium-risk customer's account activity and transaction behaviour shows that their level of ML/TF risk has increased since your previous assessment
  - When you consider, based on your risk assessment and programme that the level of risk involved is such that enhanced CDD should apply to a particular situation.<sup>15</sup>
28. You **must** conduct enhanced CDD where your customer seeks to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose.<sup>16</sup>
29. As a general principle, you should review CDD (including enhanced CDD) for higher risk customers more regularly than for lower risk customers. For example, you may wish to review higher risk customers CDD on a regular basis. For low- to medium-risk customers you may want to design review processes based on longer periods of time or where there are opportunities to update CDD information – for example, during face-to-face interactions with your customer. The final decision will be yours to make based on your risk assessment and programme.

## When must enhanced CDD be conducted for existing customers?

30. An existing customer is a customer that you have a business relationship with at the time your obligations under the Act come into effect.<sup>17</sup>
31. Customers **must** be subject to ongoing CDD and account monitoring.<sup>18</sup> Where there has been a material change in the nature and purpose of an existing customer's business relationship with you, and you consider that you have insufficient information about them, then CDD **must** be undertaken. This includes enhanced CDD where required by the Act or specified in your risk assessment or your programme.

---

13 Section 31

14 Section 31(3)(b)

15 Section 22(1)(d)

16 Section 22(1)(c)

17 Section 5

18 Section 31

## When must SoW or SoF information be obtained?

32. SoW or SoF information is required when you conduct enhanced CDD in accordance with sections 22(1) and 22(2) of the Act. This includes most cases of enhanced CDD, such as when you are dealing with a Trust, a Politically Exposed Person (PEP), or higher risk circumstances.
33. SoW or SoF information is not required when you conduct enhanced CDD in accordance with sections 22(3)-(5) of the Act. This includes circumstances such as for wire transfers, correspondent banking relationships and those involving new or developing technologies, or new or developing products that might favour anonymity.

## What does “according to the level of risk” mean?

34. When conducting enhanced CDD, you **must** verify the information provided to you by the customer using documents, data or information issued by a reliable and independent source. You **must** take reasonable steps to verify the information provided to you by the customer according to the level of risk involved.
35. “Reasonable steps” does not mean “no steps”. The Act is founded on a risk-based approach where there is no such thing as zero risk. For instance, verification **must** be carried out on the SoW or SoF of trusts even if you assess them as presenting lower ML/TF risk (family trusts for example). Your risk assessment and programme will direct the degree of your verification measures.
36. This means that you have some flexibility in the level of validation and corroboration that you undertake. You can use your judgement on the level of verification you use depending on the situation, customer, activity, or transaction. However, the steps that you take should be objective, appropriate for your business and proportionate with the level of ML/TF risk.

## How important is “nature and purpose” for enhanced CDD?

37. When on-boarding a customer, you **must** obtain information on the nature and purpose of the proposed business relationship.<sup>19</sup> The information you obtain on the nature and purpose of the proposed business relationship will help you determine whether your customer requires enhanced CDD, and it will help you with your ongoing CDD and account monitoring.
38. Information on the nature and purpose of the business relationship could include the reason the customer would like a particular product or service, the estimated total dollar value that may be received per annum, or the expected outgoings. It could also include information on the expected pattern, level, and type of activity (i.e. transaction volumes and frequency).
39. Your procedures, policies and controls should set out how you define and collect the nature and purpose of the proposed business relationship. For instance, you could include specific nature and purpose questions in your customer on-boarding form requesting this mandatory information or you could have nature and purpose as part of your scheduled ongoing CDD requirements.

---

<sup>19</sup> Section 17(a)



## What does “material change” mean for enhanced CDD purposes?

40. Your ongoing CDD and account monitoring should identify if there is material change in the nature and purpose of your customer’s business relationship with you. A material change could present an increase in ML/TF risk.
41. Such material change could include circumstances where your customer asks for new and higher risk products or services, or if they are creating new corporate or trust structures. On the other hand, it could be if your customer starts undertaking unexpected and unexplained activity in overseas locations. Alternatively, the volume or size of your customer’s transactions or activities may increase beyond what is reasonably expected.
42. For example, you may have a local customer who requested straightforward transactional services from you at on-boarding, so you assessed them as low-risk and conducted standard CDD. However, ongoing CDD and account monitoring identifies that this customer has moved to a higher risk jurisdiction and there has been an unexpected increase in transaction volume and/or value. In these circumstances, you may now require enhanced CDD as part of your ongoing CDD.

## What if you cannot complete enhanced CDD?

43. If you are not able to complete enhanced CDD for a customer, you must not carry out any occasional transaction or activity for them, nor establish a business relationship with them.<sup>20</sup> If you already have a business relationship with the customer, this **must** be terminated.<sup>21</sup>
44. This prohibition applies to circumstances where a customer fails or refuses to provide the relevant information, data, or documents that you have requested. This also applies if the information, data, or documents that the customer provides are inadequate, or if you have reasonable grounds to believe they are fraudulent.
45. As part of your programme, you should include your procedures, policies and controls for situations when enhanced CDD, or any other type of CDD, cannot be conducted.<sup>22</sup> This should cover the following situations:
  - When enhanced CDD is unable to be conducted at on-boarding
  - When the business relationship has been established and enhanced CDD was incorrectly conducted during on-boarding
  - When enhanced CDD could not be conducted following a review during ongoing CDD and account monitoring
  - When enhanced CDD cannot be conducted after a material change in the business relationship.
46. If you are unable to conduct enhanced CDD, you **must** consider whether to submit a **suspicious activity report (SAR)**.<sup>23</sup> It will be useful to record your enhanced CDD efforts during this time and include those in your SAR.<sup>24</sup>

<sup>20</sup> There are limited circumstances where the verification aspects of enhanced CDD can be completed after forming a business relationship.

<sup>21</sup> Section 37

<sup>22</sup> Your programme could also describe how you request, receive, and follow up on enhanced CDD requirements that are not met.

<sup>23</sup> Section 37(1)(d)

## Can you delay identity verification during enhanced CDD?

47. You can complete verification of customer identity for both standard CDD and enhanced CDD after you form a business relationship.<sup>25</sup> However, this should be the exception rather than part of your regular business activity. You can use delayed verification when it is essential not to interrupt normal business practice **and** verification is completed **as soon as practicable** once the business relationship has been established.
48. In addition to the above, you **must** effectively manage the ML/TF risks through transaction limitations and account monitoring or through other appropriate risk management procedures. For instance, limiting or stopping your customer's ability to withdraw funds until enhanced CDD has been conducted. Your programme should provide detail on your procedures, policies, and controls in relation to delayed verification.
49. You should not use delayed verification or exception policies to circumvent enhanced CDD procedures. This is particularly important if you have a suspicion of ML/TF or you become aware of anything that causes you to doubt the identity or intentions of your customer or their beneficial owner.

## What enhanced CDD record keeping do you need to do?

50. Your programme **must** have procedures, policies and controls for record keeping.<sup>26</sup> In relation to enhanced CDD, you **must** keep copies of all the information, data or documents you have used to verify your customer's identity and details, their beneficial ownership (if applicable) and their SoW or SoF (if applicable).<sup>27</sup>
51. You should keep written notes or findings that justify the level of verification you undertook and the reasons behind your AML/CFT decisions. For example, you should record the reasons why you delayed your enhanced CDD verification of a customer, or why you escalated a transaction monitoring alert to an SAR after conducting enhanced CDD. This could be part of a formal decision log or contained in your SAR procedures.
52. Your record keeping should be clear and logical so that another party reading the notes can understand the risk-based decision that you made. This is important for supervisory and audit purposes.
53. Record keeping is an essential part of the audit trail for the detection, investigation, and confiscation of criminal or terrorism property/funds. Record keeping helps investigating authorities to establish a financial profile of persons of interest and to trace criminal or terrorism property/funds. It also helps the Court to examine past transactions to assess whether property/funds are connected to criminal or terrorism-related offences.

---

24 To reduce ML/TF risk when you terminate a relationship where funds or other assets have been received, you should return the funds or assets to the source from which they were received. In general, this means that the funds or assets should be returned to your customer, but this may not always be possible. Where your customer requests that money or other assets be transferred to third parties, you should assess whether this provides grounds for suspicion of ML/TF and submission of a SAR.

25 Sections 16(3) and 24(3)

26 Section 57(1)(e)

27 Section 50 (3)(a)

## Do you need enhanced CDD as part of your training?

54. Training is an important part of your AML/CFT system and **must** be part of your programme.<sup>28</sup> Well-designed enhanced CDD procedures, policies and controls may be compromised if you (or your staff) are not adequately trained.
55. Your training should incorporate when and how enhanced CDD will be undertaken, including on-boarding customers, conducting ongoing CDD and submitting SARs. In addition, your enhanced CDD training should also look at what reliable and independent sources of information you can use to verify customer identity, beneficial ownership, and SoW or SoF. Your training should also cover recognised methods and trends in ML/TF that could be deterred or detected by enhanced CDD, as well as any new and emerging techniques.

## Can you conduct enhanced CDD via a third party?

56. The Act allows for CDD, including enhanced CDD, to be undertaken for you by a third party. This may be a member of your designated business group, your agent or other reporting entities or persons in another country when certain conditions are met. The Act requires that the third-party consents to conducting the CDD for you and to providing you all relevant information.<sup>29</sup>
57. If a third party is undertaking CDD (including enhanced CDD) for you this **must** be considered in your risk assessment and the procedures, policies and controls included in your programme. Liability for carrying out CDD (including enhanced CDD) remains with you unless certain conditions are met.<sup>30</sup>

---

28 Section 57(1)(b)

29 Section 32-34

30 Section 33(3)(a)

## Part 2: Enhanced CDD and identity requirements

### Obtaining and verifying identity information

58. When conducting enhanced CDD on a customer, you **must**<sup>31</sup> obtain the same identity information that is required for standard CDD. This includes the customer's full name, date of birth and address (if an individual) or company identifier or registration number and registered office (if not an individual) and any other information prescribed by the Act or regulations.
59. You **must** take reasonable steps to verify that information, data, or documents are from reliable and independent sources.<sup>32</sup> As you are conducting enhanced CDD, you may need to use increased or more sophisticated measures to do this than you would for standard CDD.
60. To help you determine the level of enhanced CDD verification required for customers that are individuals, you should refer to the **Amended Identity Verification Code of Practice 2013 (IVCOP)** guidance material, and its **explanatory note**. The IVCOP provides suggested best practice to verify the identity of individuals that are low- or medium-risk customers.

### Persons acting on behalf of a customer and beneficial owners

61. You **must** identify and verify the identity of any person acting on behalf of the customer and any beneficial owner(s) of the customer. In relation to a person acting on behalf of the customer, and according to the level of risk involved, reasonable steps **must**<sup>33</sup> be taken to verify the information collected so that you are satisfied who the person is *and* that they have the authority to act.
62. In relation to the beneficial owner(s) of the customer, and according to the level of risk involved, reasonable steps **must**<sup>34</sup> be taken to verify the information collected so that you are satisfied that you know the identity of the beneficial owner(s).

### Exception handling procedures

63. To comply with the IVCOP, you **must** have appropriate exception handling procedures in place, for circumstances when a customer demonstrates they are unable to satisfy the requirements of the IVCOP.<sup>35</sup> **However, this does not apply to enhanced CDD due to the higher risk of ML/TF.**

### Enhanced CDD and beneficial owner

64. A core requirement of enhanced CDD is to identify and verify your customers' beneficial ownership arrangements to ensure that you fully understand them. It is crucial to know who the beneficial owner(s) are so that you can make appropriate decisions about the level of ML/TF risk presented by your customer.

---

31 Section 23

32 Section 13

33 Section 16(1)(c)

34 Section 16(1)(b)

35 Point 4 IVCOP

- 
65. If you want to do business with a customer, you **must** identify and verify the identity of the beneficial owner(s).<sup>36</sup> You should establish and understand the customer's ownership structure at each layer. The beneficial owner is not necessarily one individual; there may be several beneficial owners in a structure. Where there are complex ownership layers with no reasonable explanation, you should consider the possibility that the structure is used to hide the beneficial owner(s). If so, enhanced CDD may be required.
66. Refer to **Beneficial Ownership Guideline** material for further information on beneficial ownership.

---

<sup>36</sup> Section 11 – Except in circumstances where simplified CDD applies.

## Part 3: Circumstances when enhanced CDD applies

67. This section provides information on the different types of circumstances and customers for whom enhanced CDD is required. This applies equally to business relationships with a customer and occasional transactions and activities.

### Trusts

68. You **must** conduct enhanced CDD on a trust or another vehicle for holding personal assets.<sup>37</sup> The requirement for enhanced CDD on trusts recognises the potential use of trusts to disguise the criminal origin of funds or the true ownership and effective control of the trust. This is particularly the case where ownership and control arrangements are sophisticated or complex. Your risk assessment and programme will determine the level of enhanced CDD you conduct on these entities and the assessed ML/TF risk associated with them.
69. For instance, your risk assessment may assess the level of inherent ML/TF risk presented by a domestic ‘family’ trust as lower than the risk presented by an overseas trust from a jurisdiction with weak AML/CFT measures or high levels corruption. You will still need to conduct enhanced CDD, including verification of SoW or SoF, on the family trust but it will not need to be as in-depth as with the overseas trust. The level of enhanced CDD you decide to undertake should be proportionate to the risks involved.
70. You **must** take reasonable steps, according to the level of risk involved, to verify the identity of any beneficial owners of your customer.<sup>38</sup> This includes instances where the beneficial owner of your customer may be an individual behind another legal arrangement<sup>39</sup> or a company.
71. For a customer that is a trust, you **must** obtain the name and date of birth of each beneficiary of the trust.<sup>40</sup> There is no requirement to verify this information. However, if the customer is a discretionary trust or a trust with more than 10 beneficiaries, you **must** instead obtain a description of each class or type of beneficiary.<sup>41</sup> If the trust is a charitable trust, you **must** also obtain the objects of that trust.<sup>42</sup>
72. To identify the SoW or SoF of a trust you will need to identify the individual(s) who are the settlor(s), and the origin of the settlor’s wealth. For example, the settlor may have inherited family wealth, accumulated business earnings, or received funds from the sale of property. You will also need (if relevant) to identify the source of any income that the trust is receiving. For example, it may be income from an underlying company or simply a monthly deposit from a family bank account. See Part 4 for more information.
73. Further information can be found in the **Beneficial Ownership Guideline**, the **CDD fact sheet on trusts** and the associated “**Clarification of the position**” document.

37 Sections 22(1)(a)(i) and 22(1)(b)(i)

38 Section 16(1)(b) and 24(1)(a)

39 Section 5

40 Section 23(2)(a)

41 Section 23(2)(b)(i)

42 Section 23(2)(b)(ii)

## Countries with insufficient AML/CFT measures

74. If your customer is non-resident and from a country with insufficient AML/CFT measures and/or higher ML/TF risks you **must** undertake enhanced CDD.<sup>43</sup> To help you to determine which countries have insufficient AML/CFT measures in place, you should refer to the **Countries Assessment Guideline** published by the AML/CFT supervisors, as well as other guidance material such as those published by FIU, Ministry of Justice, and the Financial Action Task Force (FATF).

## Companies with nominee shareholders

75. You **must** conduct enhanced CDD on a customer that is a company with nominee shareholders.<sup>44</sup> The use of nominee shareholders makes it more difficult to identify the beneficial owners of a company, increases the complexity of the company structure and adds another level of obfuscation. This increases the ML/TF risk and enhanced CDD measures are necessary.

## Companies with shares in bearer form

76. Shares in bearer form present a high risk of ML/TF. You **must** conduct enhanced CDD on a customer that is a company with some or all of its shares in bearer form.<sup>45</sup> A higher risk of ML/TF exists when a company has some, or all, of its capital in the form of bearer shares. It is often difficult to identify the beneficial owners of a company with bearer shares because they are not registered with any authority. Instead, ownership is based on the customer who physically holds the share document. This means that any transfer of ownership is not registered or regulated. Companies that issue bearer shares are often in higher risk jurisdictions.

## Complex or unusual transactions

77. You **must** conduct enhanced CDD on a customer if they conduct:

- A transaction that is complex
- A transaction that is unusually large
- An unusual pattern of transactions that have no apparent or visible economic or lawful purpose.<sup>46</sup>

78. Adequate and effective CDD provides context and helps you understand the types of transactions that your customer should be conducting. It also helps you identify complex and unusual transactions or patterns of transactions, and the situations when you need to conduct enhanced CDD.

79. Your account monitoring is also a vital element in identifying these types of transactions. Whether an automated or manual system is used, this should generate ML/TF alerts for review and examination. You should base your thresholds and scenarios for these alerts on your risk assessment and you should detail your procedures, policies, and controls in your programme.

---

<sup>43</sup> Sections 22(1)(a)(ii) and 22(1)(b)(ii)

<sup>44</sup> Section 22(1)(a)(iii)

<sup>45</sup> Section 22(1)(a)(iii)

<sup>46</sup> Section 22(1)(c)

## Assessed risk for a particular situation

80. You **must** conduct enhanced CDD when you consider the level of risk in a particular situation is such that enhanced CDD should apply.<sup>47</sup>
81. This requirement applies to any other situation where there is ML/TF risk not otherwise or specifically identified in the Act. The situations where these ML/TF risks arise should be based on the findings of your risk assessment and they will be particular to your business. The situations may arise from a combination of vulnerabilities associated with the size, nature and complexity of your business, your types of customers, your products and services and your methods of delivery, as well as the types of institutions and countries that you deal with.
82. In relation to the countries you deal with, it is important to understand that the risks associated with a country are wider than having insufficient AML/CFT measures in place. Country risk can result from:
- Ineffective AML/CFT measures
  - High levels of organised crime
  - Perceived levels of bribery and corruption
  - Association with TF
  - Conflict zones and their bordering countries
  - Production and/or transnational shipment of illicit drugs.
83. The **Countries Assessment Guideline** will assist you in determining when enhanced CDD may be required due to country risk. The guideline refers to information sources that can help you in assessing country risk, including, but not limited to:
- FATF identification of jurisdictions with strategic AML/CFT deficiencies
  - FATF mutual evaluation reports
  - Basel AML Index
  - United Nations Office on Drugs and Crime reports
  - Transparency International Corruption Perceptions Index
  - Reliable and independent media sources.
84. While your risk assessment is the starting point to identify situations where there is ML/TF risk, other indicators may only be identifiable as you administer your programme. This will include your customer's behaviour, the CDD or enhanced CDD you have conducted, your account monitoring and the wider AML/CFT environment. Your risk assessment and programme **must** also have regard to supervisory AML/CFT guidance.<sup>48</sup>

---

<sup>47</sup> Section 22(1)(d)

<sup>48</sup> Sections 58(2)(g) and 57(2)



## Suspicious activity reports (SARs)

85. As soon as practicable after you become aware that you must report an SAR, you **must** conduct enhanced CDD.<sup>49</sup> You will need to ensure that in conducting the enhanced CDD you do not tip off the customer that you will be submitting an SAR. Unlawful disclosure of SARs (and prescribed transaction reports) is an offence.<sup>50</sup>
86. Conducting enhanced CDD in these circumstances could include asking your customer further questions about their activity or transactions and confirming the nature and purposes of the business relationship. Such enquiries, when conducted properly and in good faith, do not constitute tipping off. It may be the case that after conducting enhanced CDD you determine that your customer's activity is no longer suspicious, and a SAR will not be required.
87. Maintaining clear and logical records of decisions made, by whom, and the reasons for them will help you demonstrate your appropriate handling of unusual or suspicious activities.

## New and developing technologies and products

88. New and developing technologies and products can present unknown ML/TF risks and vulnerabilities, and new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity.
89. Where you have a customer who wants to establish a business relationship, or conduct an occasional transaction/activity, involving new and developing technology and products that might favour anonymity, you **must** take additional enhanced CDD measures to mitigate and manage these ML/TF risks.<sup>51</sup> It is for you to determine what measures are required according to the level of risk involved.
90. Your risk assessment should consider whether your business is, or may be, exposed to customers involved in new and developing technologies and products. Your programme should then detail the procedures, policies, and controls that you will implement for this type of customer and technology.<sup>52</sup>

---

49 Section 22A(2)

50 Section 94

51 Section 22(5)

52 Section 30

## Part 4: Enhanced CDD and SoW and SoF

91. In many cases, SoW or SoF information and documents required for enhanced CDD will be readily available and quickly provided by your customer. In other cases, you may need to inquire further into complex ownership or control structures, or you may need to examine the origins of your customer's wealth in detail.
92. There are several different forms of enhanced CDD established by the Act,<sup>53</sup> and establishing your customer's SoW or SoF is not always a requirement of enhanced CDD. Reporting entities should determine the requirements of enhanced CDD as it applies to their customer's circumstances.<sup>54</sup> In the circumstances where it applies, you **must** collect information relating to the SoW or SoF of your customer<sup>55</sup> and you **must**, according to the level of risk involved, take reasonable steps to verify<sup>56</sup> that information. Your programme should set out how you will do this.
93. For instance, a high-risk, overseas customer will require greater effort and more comprehensive investigation to verify SoW or SoF information than a low-risk, domestic customer. **Even for low-risk customers you must conduct some verification measures.**

### What is the difference between SoW and SoF?

94. Your customer's SoW is the origin of their entire body of assets. This information gives an indication of the amount of wealth your customer would be expected to have and a picture of how they acquired it.
95. Your customer's SoF is more narrowly focused. It is the origin of the funds used for the transactions or activities that occur within the business relationship with you. This also applies for an occasional transaction or activity.
96. In circumstances where you are establishing or updating your customer's risk profile you may need to collect and verify information regarding their SoW. However, when enhanced CDD is triggered by circumstances involving transactions or activities, you may need to focus more specifically on the SoF.
97. It is important to remember that your customer's SoW and SoF do not exist in isolation of each other. In a situation where an individual transaction is disproportionately large compared to your knowledge of a customer's wealth, this should trigger a more detailed examination of that transaction or activity. It is for you to determine when to examine your customer's SoW, when to examine their SoF, or when to examine both.

### How do you obtain and verify information about SoW or SoF?

98. You should ask your customer to provide you information about their SoW or SoF and record this information.<sup>57</sup> You **must** take reasonable steps, according to the level of risk involved, to verify this information using reliable and independent sources.

---

53 Sections 23-30  
54 Section 22  
55 Section 23(a)  
56 Section 24(1)(b)  
57 Section 23

99. Where you identify that the origin of your customer's funds or wealth has come from their beneficial owner(s), it may be necessary, according to the level of risk involved, for you to extend your level of verification to include the SoW or SoF of these persons. However, you should not obtain and verify SoW or SoF for every beneficial owner where they have nothing to do with the "customer's" SoW or SoF.
100. To help you verify information about SoW and SoF, you may be able to use publicly available information on the internet, or other commercially available databases. However, in many situations, it will be necessary for your customer to provide you with documents issued by third parties that support their financial position. In higher risk circumstances, it may be necessary to seek further information, either from your customer or directly from the relevant third party.
101. You **must**<sup>58</sup> develop an understanding of the size and nature of your customer's overall wealth and, importantly, how it was acquired. This does not require you to verify their entire financial history or identify every asset that they hold. They may have multiple income streams and assets making this extremely difficult.
102. It may be useful to establish the different categories of income or assets that make up their total wealth. Examples could include their various investments, salary, family income or different types of commercial activity. Where there are multiple categories or income streams, you should focus your verification on the larger of them, as well as those that are the most complex or obfuscated. Once categorised and examined, it should be easier to understand your customer's overall level of wealth.
103. It is not expected that every part of the SoW will be accounted for. However, you **must** be satisfied that the nature and size of your customer's wealth matches what you know about them.

### **How do you determine SoF?**

104. Verifying your customer's funds should be a more granular process. The information, data, or documents that you use should be specific to the business relationship or to their activities and transaction behaviour. This is important when your verification relates to a specific transaction, or sequence of transactions, that your customer is involved in. This also applies to any occasional transaction or activity that you conduct for a customer.

### **What documents can verify SoW or SoF?**

105. When you verify SoW or SoF information, you should use data or documents issued by a credible and reliable source such as a multi-national company, a reputable third-party commercial provider, or a government department from a low-risk country with sufficient AML/CFT measures.
106. The types of data and documents that you use for verification will vary depending on the circumstances and the information that the customer provides to you. The following documents, data, or information could be considered reliable and independent:

---

<sup>58</sup> Sections 23(1)(a) and 24(1)(b)

- Government-issued or registered documents or data
- Full bank and other investment statements
- Full payslip or wage slip or other documents confirming salary
- GST number and IRD statement of earnings from the most recent year (for sole traders)
- Inheritance (stamped grant of probate, stamped grant of letters of administration)
- Audited financial accounts from a chartered accountant or Charities Services
- Letter from an agent of the customer confirming they have knowledge of and established business relationships with the customer
- A copy of a will
- Sales and purchase agreements.

107. For customers who conduct their business activities with you there should be a range of documents you can use to verify how funds have been acquired. Depending on the type of business, this could include contractual agreements, sales and purchase records or import and export related documents for the shipment of goods.

108. Documentation accepted to verify SoW or SoF should depend on the level of ML/TF risk presented by the customer. The higher the risk, the more comprehensive and reliable documents you obtain should be. For instance, we would expect certified copies or originals to be sighted, or verification via other reliable measures such as disclosure registers, for higher risk customers. However, in other circumstances such as in low risk situations or if the original document was only ever signed electronically, you may be able to rely on a copy received by email. You may also need to exercise caution with documents signed by relationship managers that have a vested interest in on-boarding or retaining a customer. In addition, you should be wary of documents that appear fraudulent or altered.

### **Additional notes regarding SoW or SoF**

109. You are, of course, able to conduct your own research to supplement the information and documents that your customer provides you regarding their SoW or SoF. This could be at on-boarding, during ongoing CDD or prior to submitting an SAR. Sources could include:

- Internet
- Trusted intermediaries
- Reliable media
- Publicly available databases
- Professional third-party providers.

110. An accurate understanding of a customer's SoW or SoF is best achieved when it occurs in conjunction with the identification of beneficial owners, and with comprehensive information obtained on the nature and purpose of a business relationship.

## Part 5: Enhanced CDD and Politically Exposed Persons (PEPs)

111. A PEP is a person who in the last 12 months has held a prominent overseas position. The term PEP includes their relatives and close associates, which are sometimes called RCAs. It also includes people who have beneficial ownership of legal entities or arrangements existing to benefit PEPs.
112. You **must** as soon as practicable after establishing a business relationship (or occasional activity or transactions) take reasonable steps to determine if your customer, or their beneficial owner, is a PEP.<sup>59</sup>
113. You **must** ensure that you have adequate and effective procedures, policies, and controls to identify customers that are PEPs. This will depend on the size, nature and complexity of your business and the likelihood of having a PEP as a customer.
114. You **must** conduct enhanced CDD on a customer who is a PEP.<sup>60</sup> In addition, your senior management (if applicable) **must** approve continuing the business relationship with a PEP.<sup>61</sup> You **must** obtain and take reasonable steps to verify the PEP's SoW or SoF.<sup>62</sup>
115. According to the level of risk involved, it may be appropriate, as part of your enhanced CDD, to use internet/media searches and publicly available reports to check if your customer is a PEP, especially when they are from a country with high levels of bribery, corruption, and organised crime. With larger or more complex businesses, you may want to consider using the services of a third-party provider and commercially available databases to screen for PEPs.
116. For ongoing CDD and account monitoring of a higher risk PEP, you may need to undertake ongoing media monitoring or increase transaction monitoring activity. You may wish to conduct more frequent enhanced CDD reviews and submit quicker, more thorough SARs.
117. Key enhanced CDD questions to consider are:
- Is the PEP's transaction/activity in line with expectations?
  - Is the PEP's identity data, address, employment, SoW or SoF and relatives and close associates' status up to date?
  - Are there any unexplained changes to the PEP's details?
  - If the PEP's net worth has grown substantially in a short amount of time, do you have a clear explanation for the sudden growth?
  - Have you sought clarification from the PEP where necessary and updated their details?

---

<sup>59</sup> Section 26

<sup>60</sup> Section 22(2)

<sup>61</sup> Section 26(2)(a)

<sup>62</sup> Section 26(2)(b)

## Part 6: Table of Abbreviations and Acronyms

AML/CFT	Anti-money laundering and countering financing of terrorism
AML/CFT supervisors	The Department of Internal Affairs, the Financial Markets Authority, and the Reserve Bank of New Zealand
The Act	AML/CFT Act 2009
CDD	Customer due diligence
FATF	Financial Action Task Force
FIU	New Zealand Police Financial Intelligence Unit
IVCOP	Amended Identity Verification Code of Practice 2013
ML	Money laundering
PEP	Politically exposed person
Programme	AML/CFT programme
RBA	Risk-based approach
RCA	Relative and close associate
Risk assessment	AML/CFT risk assessment
SAR	Suspicious activity report
SoF	Source of funds
SoW	Source of wealth
STR	Suspicious transaction report
TF	Terrorism financing

## Revision History

Dec 2017	Original Version
Mar 2019	Updated Version
Sep 2020	<ul style="list-style-type: none"> <li>• Structure table moved to front of document.</li> <li>• Updated wording in paragraphs 9 &amp; 10 – there is no substantial meaning change.</li> <li>• Addition of section ‘When must SoW or SoF information be obtained?’ (paragraphs 32 &amp; 33) – following paragraphs renumbered accordingly.</li> <li>• Update to paragraphs 17 &amp; 21 – replacement of ‘must’ with ‘should usually’.</li> <li>• Addition of bullet point on ‘new or developing technologies’ to paragraph 24.</li> <li>• Deletion of bullet point on ‘material change’ from paragraph 27.</li> <li>• Replaced ‘should’ with ‘must’ in paragraph 50 (previously 48) in relation to keeping copies of documentation.</li> <li>• Rewording of paragraphs 70 &amp; 71 (previously paragraphs 68 &amp; 69). There is no substantial meaning change.</li> <li>• Addition of sentence to paragraph 108 (previously paragraph 106) relating to electronic copies of documents.</li> </ul>