AML/CFT

Anti-money laundering and countering financing of terrorism

Enhanced Customer Due Diligence Guideline

April 2024

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Reserve Bank of New Zealand
Te Pūtea Matua

Te Tari Taiwhenua
Internal Affairs

Structure of the Enhanced Customer Due Diligence guideline

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 you to obtain and verify 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 cases, enhanced CDD also requires you to obtain and verify information relating to the **source of wealth (SoW)** and/or **source of funds (SoF)** of your customer. In some situations, additional measures may also be required.

4. This guideline does not address enhanced CDD requirements for wire transfers and correspondent banking relationships under sections 22(3)-(4) of the Act.

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, mitigate and prioritise your response to ML/TF risks.

8. This guideline is based on the requirements of the Act and has been produced by the AML/CFT supervisors under section 132(2) of the Act. This guideline does not constitute legal advice.

9. 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.

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 guideline 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 Guidelines are referenced, they can be accessed at the following websites:

Department of Internal Affairs:	http://bit.ly/2gQ3Iev
New Zealand Police Financial Intelligence Unit:	http://bit.ly/2zpmWPJ
Reserve Bank of New Zealand:	http://bit.ly/2n6RYdp
Financial Markets Authority:	https://bit.ly/3fjcKlD

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 extent 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. (Refer to paragraph [27] for the circumstances in which ECDD is required).[1]

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.[2] (This is covered in Part 2 of this guideline).
    - You should obtain and verify information relating to the **source of wealth (SoW)** and/or **source of funds (SoF)** of your customer.[3] The circumstances in which you need to do this are detailed within the Act.[4] You **must** take reasonable steps to do this according to the level of risk involved.[5] (This is covered in Part 4 of this guideline).

18. 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. (For further information regarding SoW refer to Part 4 of the guideline).

19. 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.

20. 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.[6]

Why is enhanced CDD required?

21. 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.[7]

[1] Section 17(b) and 22
[2] Sections 16(1) and 24(1)(a)
[3] Sections 23(1)(a), 24(1)(b), 26(2)(b) and 26(3)
[4] Section 22
[5] Sections 24(1)(b), 26(2)(b) and 26(3)
[6] Sections 57(1)(c) and 57(1)(j)
[7] Section 22(1)(d)

22. 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.
    - Determine whether a customer's SoW and/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.
    - Comply with the requirement that SARs are reported to the **New Zealand Police Financial Intelligence Unit (FIU).** A SAR must be submitted to the FIU, as soon as practicable, but no later than three working days after there are reasonable grounds for forming suspicion.

When is enhanced CDD required?

23. 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 [56] to [58].

24. Enhanced CDD may also be required at subsequent points during a business relationship as part of your ongoing CDD and account monitoring procedures.[8]

25. There are also certain circumstances in which enhanced CDD is required when there are grounds to report a suspicious activity. This is covered in Part 5 of the guideline – see page 26.

When must enhanced CDD be conducted for new customers?

26. 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.

27. Customers that **must** have enhanced CDD are:[9]
    - 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[10]
    - A company with nominee shareholders or shares in bearer form
    - A politically exposed person (PEP)

[8] Section 31
[9] Section 22
[10] Refer to Countries Assessment Guideline and paragraphs [86] to [87]

- 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[11]
- A business relationship with a company with 1 or more nominee directors[12]
- A business relationship with a limited partnership with a nominee general partner[13]
- A business relationship with a customer that involves new or developing technologies, or new or developing products, that might favour anonymity[14]
- 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.

28. Unless you have doubts about the adequacy or veracity of the information, data and documents that you have previously obtained and verified relating to your customer, you are not required to conduct enhanced CDD again.[15] 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.

When must enhanced CDD be conducted again?

29. As part of your ongoing CDD and account monitoring processes you **must** regularly review your customer's details, account activity and transaction behaviour.[16] 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.

30. You **must** have regard to your customer's ongoing level of ML/TF risk,[17] 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.[18]

[11] Section 22(1)(d)
[12] Regulation 12(a)– AML/CFT (Requirements and Compliance) Regulations 2011. Refer to the Companies CDD Guideline for further information on complying with these regulations.
[13] Regulation 12(b)– AML/CFT (Requirements and Compliance) Regulations 2011. Refer to the Limited Partnerships CDD Guideline for further information on complying with these regulations.
[14] Section 30
[15] Section 11(4)
[16] Section 31
[17] Section 31(3)(b)
[18] Section 22(1)(d)

31. 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.[19]

32. 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?

33. An existing customer is a customer that you have a business relationship with at the time your obligations under the Act come into effect.[20]

34. Customers **must** be subject to ongoing CDD and account monitoring.[21] Where there has been a material change in the nature and purpose of an existing customer's business relationship with you (refer to paragraphs [46] to [49]), 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.

When must SoW and/or SoF information be obtained and verified?

35. SoW and/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.

36. You are required to have procedures, policies and controls in your programme to differentiate when you obtain and verify information regarding the SoF of the customer or the SoW of the customer, or alternatively both the SoF and the SoW of the customer.[22] Note in some circumstances, you may also be required to obtain and examine other information when conducting enhanced CDD, for example regarding the purpose of a transaction.[23]

37. SoW and/or SoF information is not required when you conduct enhanced CDD in accordance with section 22(5) of the Act. This includes circumstances involving new or developing technologies, or new or developing products that might favour anonymity.

What does "according to the level of risk" mean?

38. 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

[19] Section 22(1)(c)
[20] Section 5
[21] Section 31
[22] Regulation 15H AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)
[23] Regulation 12AB AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)

independent source. You **must** take reasonable steps to verify the information provided to you by the customer according to the level of risk involved.

39. "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. Your risk assessment and programme will direct the degree of your verification measures.

40. 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. You must keep appropriate records to document the reasons and conclusions for your decisions (see paragraph [61]).

How important is standard CDD for determining if enhanced CDD is required?

41. Standard CDD assists you to establish your customer's risk profile.[24] For legal persons and legal arrangements, developing a clear understanding of the underlying persons that own or control them is a key part of this.[25]

42. When on-boarding a customer, you **must** obtain information on the nature and purpose of the proposed business relationship.[26] For a customer ordinarily eligible for standard CDD, you must also obtain sufficient information to determine whether the customer should be subject to enhanced CDD.[27]

43. Your conduct of standard CDD at on-boarding, including the information you obtain regarding the nature and purpose of the proposed business relationship, will help you determine whether your customer requires enhanced CDD and the extent of this enhanced CDD. It will also help you with your ongoing CDD and account monitoring.

44. 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).

45. Your procedures, policies and controls should set out the steps you take for standard CDD, including how you define and obtain information on 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. You could have nature and purpose as part of your scheduled ongoing CDD requirements.

[24] Effective 1 June 2025, a new regulation 12AC of the AMLCFT (Requirements and Compliance) Regulations 2011 will explicitly require a reporting entity to risk-rate a new customer and record this rating. This needs to be reviewed as part of ongoing CDD and account monitoring.
[25] Refer to the supervisors' guidelines for different types of legal person and legal arrangement.
[26] Section 17 (a), Section 25
[27] Section 17 (b)

What does "material change" mean for enhanced CDD purposes?

46. 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.

47. 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, frequency or size of your customer's transactions or activities may increase beyond what is reasonably expected.

48. 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 must now require enhanced CDD as part of your ongoing CDD.

What if you cannot complete enhanced CDD?

49. 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.[28] If you already have a business relationship with the customer, this **must** be terminated.[29]

50. 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.

51. 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.[30] 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

[28] There are limited circumstances where the verification aspects of enhanced CDD can be completed after forming a business relationship.
[29] Section 37
[30] Your programme could also describe how you request, receive, and follow up on enhanced CDD requirements that are not met.

- Ensuring you give the customer sufficient (and reasonable) time to provide the required documents within a business relationship.

52. If you are unable to conduct enhanced CDD, you **must** consider whether to submit a **suspicious activity report (SAR)**.[31] It will be useful to record your enhanced CDD efforts during this time and include those in your SAR.

What is the timeframe to terminate the business relationship if enhanced CDD cannot be completed?

53. The Act does not specify a timeframe if you cannot conduct CDD and are required to terminate a business relationship (under section 37 of the Act).

54. However, the AML/CFT supervisors consider that this should be as soon as practicable, taking into consideration the nature and complexity (including liquidity) of the product or service you are providing to the customer. In some circumstances, it may not be possible to immediately cease the business relationship due to another contractual agreement.[32] That said, the supervisors consider that the termination process should commence as soon as you determine you are unable to complete CDD. You must keep records to document the termination process, including your communications with the customer and the reasons behind your AML/CFT decisions[33] – see paragraph [60].

55. The High Court[34] has held that when you terminate a relationship where funds or other assets have been received, you should return the funds or assets to the customer. In general, this means that the funds or assets should be returned to your customer even if the funds were received from a third party, unless the customer directs the funds to be paid to the source. Where your customer requests that money or other assets be transferred to third parties, you should assess whether this in itself provides grounds for submission of a SAR.

Can you delay identity verification during enhanced CDD until after you have established the business relationship?

56. You can complete verification of customer identity for both standard CDD and enhanced CDD after you form a business relationship.[35] 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.

57. 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, restricting deposits, limiting or stopping your customer's ability to process transfers until enhanced CDD has been conducted. Your

[31] Section 37(1)(d)
[32] Section 9 states the Act has effect despite anything to the contrary in any contract or agreement. No person is excused from compliance with any requirement of this Act or regulations by reason only that compliance with that requirement would constitute breach of any contract or agreement.
[33] Section 51(1)(c)
[34] *Arjang v NF Global Limited [2021] NZHC 395* at paragraphs [53] and [55]
[35] Sections 16(3) and 24(3)

programme should provide detail on your procedures, policies, and controls in relation to delayed verification.

58. 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?

59. Your programme **must** have procedures, policies and controls for record keeping.[36] 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 and/or SoF (if applicable).[37] You must keep your records for a minimum of five years after an occasional transaction or occasional activity has been completed or a business relationship has ended (whichever is later).[38]

60. 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.

61. 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.

62. 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.

Do you need enhanced CDD to be part of your training?

63. Training is an important part of your AML/CFT system and **must** be part of your programme.[39] Well-designed enhanced CDD procedures, policies and controls may be compromised if you (or your relevant staff[40]) are not adequately trained.

64. 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

[36] Section 57(1)(e)
[37] Section 50
[38] Section 49-52
[39] Section 57(1)(b)
[40] Section 57(1)(b) requires your programme to include adequate and effective procedures, policies and controls for training on AML/CFT matters for senior managers, the AML/CFT compliance officer, and any other employee that is engaged in AML/CFT related duties.

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?

65. The Act allows for CDD to be undertaken for you by a third party. This can include enhanced CDD. 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.[41] Liability for carrying out CDD (including enhanced CDD) remains with you.

66. 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.

[41] Section 32-34

Part 2: Enhanced CDD and identity requirements

Obtaining and verifying identity information

67. When conducting enhanced CDD on a customer, you **must**[42] 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.

68. You **must** take reasonable steps to verify that information, data, or documents are from reliable and independent sources.[43] 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.

Amended Identity Verification Code of Practice 2013

69. The **Amended Identity Verification Code of Practice 2013 (IVCOP)** provides suggested best practice and a 'safe harbour' for verifying the name and date of birth of individuals that are low- or medium-risk customers. The supervisors consider that you may also find the IVCOP instructive as guidance for verifying the name and date of birth of high-risk individuals (when you are conducting enhanced CDD).

70. For example, you could use the IVCOP as your starting point for high-risk customers. It may be that the risk relating to a particular customer does not relate to the accuracy of their biographical information (i.e. you are satisfied you have verified their true name and date of birth). In this situation, you may not need to undertake any further verification steps over and above those set out in the IVCOP. Your AML/CFT resource can be then applied to other aspects of enhanced CDD, such as the examination of the SoW and/or SoF.

71. However, in other circumstances, risks relating to the person's biographical information (i.e. the risk this person is using a false identity) may be integral to the assessment they are high risk. For this type of situation, you should consider what additional, increased or more sophisticated measures are required to verify the name and date of birth. This could include sighting additional identity documents or if onboarding the customer remotely, obtaining certified copies of documents or taking additional identity authentication steps. In some circumstances, it may be necessary to require them to attend a branch in person with their original identity documents.

72. **Note**: The IVCOP states that you must have appropriate exception handling procedures in place, for circumstances when a customer demonstrates they are unable to satisfy its requirements.[44] These exception handling procedures should not apply if you are using the IVCOP as your starting point for verifying the name and date of birth of high-

[42] Section 23
[43] Section 13
[44] Point 4 IVCOP

risk customers. Note also that the 'safe harbour' provided by the IVCOP does not apply in relation to high-risk customers.

73. For further information relating to name and date of birth verification, refer to **the Amended Identity Verification Code of Practice 2013** and its August 2023 **Explanatory Note and Guideline.**

Persons acting on behalf of a customer and beneficial owners

74. 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**[45] be taken to verify the information obtained so that you are satisfied who the person is *and* that they have the authority to act.

75. In relation to the beneficial owner(s) of the customer, and according to the level of risk involved, reasonable steps **must**[46] be taken to verify the information obtained so that you are satisfied that you know the identity of the beneficial owner(s).

Enhanced CDD and beneficial owner

76. A core requirement of enhanced CDD is to identify and verify your customers' beneficial ownership arrangements to ensure that you 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.

77. If you want to do business with a customer, you **must** identify and verify the identity of the beneficial owner(s).[47] 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.

78. Refer to **Beneficial Ownership Guideline** material for further information on beneficial ownership.

[45] Section 16(1)(c)
[46] Section 16(1)(b)
[47] Section 11 – Except in circumstances where simplified CDD applies.

Part 3: Circumstances when enhanced CDD applies

79. 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

80. You **must** conduct enhanced CDD on a trust or another vehicle for holding personal assets.[48] 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.

81. 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 of corruption. You will still need to conduct enhanced CDD, including verification of SoW and/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.

82. You **must** take reasonable steps, according to the level of risk involved, to verify the identity of any beneficial owners of your customer.[49] This includes instances where the beneficial owner of your customer may be an individual behind another legal arrangement[50] or a company.

83. For a customer that is a trust, you **must** also obtain the name and date of birth of each beneficiary of the trust.[51] There is no requirement to verify this information. However, if the customer is a discretionary trust, a charitable trust or a trust with more than 10 beneficiaries, you **must** instead obtain a description of each class or type of beneficiary.[52] If the trust is a charitable trust, you **must** also obtain the objects of that trust.[53]

84. To identify the SoW and/or SoF of a trust you will need to identify 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. This could also include identifying the underlying individual(s) if the settlor(s) is not a natural person. 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.

[48] Sections 22(1)(a)(i) and 22(1)(b)(i)
[49] Section 16(1)(b) and 24(1)(a)
[50] Section 5
[51] Section 23(2)(a)
[52] Section 23(2)(b)(i)
[53] Section 23(2)(b)(ii)

85. Further information can be found in the **Beneficial Ownership Guideline and** the **Guideline: CDD for trusts**.

Countries with insufficient AML/CFT measures

86. If your customer is non-resident from a country with insufficient AML/CFT measures and/or higher ML/TF risks you **must** undertake enhanced CDD.[54] 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).

87. Note that a country that is subject to a FATF call for action **must** always be considered a country with insufficient AML/CFT systems or measures in place.[55]

Companies with nominee shareholders

88. You **must** conduct enhanced CDD on a customer that is a company with nominee shareholders.[56] 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

89. 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.[57] 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.

Unusually large, complex or unusual pattern of transactions

90. You **must** conduct enhanced CDD on a customer if they seek to 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.[58]

91. 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

[54] Sections 22(1)(a)(ii) and 22(1)(b)(ii)
[55] Regulation 15 AML/CFT (Requirements and Compliance) Regulations 2011
[56] Section 22(1)(a)(iii) and 22(1)(b)(iii)
[57] Section 22(1)(a)(iii) and 22(1)(b)(iii)
[58] Section 22(1)(c)

and unusual transactions or patterns of transactions, and the situations when you need to conduct enhanced CDD.

92. 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. Your monitoring rules for thresholds and other scenarios should be commensurate with the types of customers you deal with, the products and services you offer and the size and value of transactions you undertake. You should be able to justify the rationale behind your rules set based on your ML/TF risks.

Assessed risk for a particular situation

93. You **must** conduct enhanced CDD when you consider the level of risk in a particular situation is such that enhanced CDD should apply.[59]

94. 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.

95. 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.

96. 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

[59] Section 22(1)(d)

- Transparency International Corruption Perceptions Index
- Reliable and independent media sources.

97. 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 material.[60]

Companies with nominee directors

98. You **must** conduct enhanced CDD on a customer that is a company with one or more nominee directors.[61] Companies that have these arrangements present a higher ML/TF risk making enhanced CDD necessary. The use of nominee directors makes it more difficult to identify the beneficial owners of the company and increases the complexity of the company's structure.

Limited partnerships or overseas limited partnerships with nominee general partners

99. You **must** conduct enhanced CDD on a customer that is a limited partnership or an overseas limited partnership with a nominee general partner.[62] Limited partnerships which have these arrangements present a higher ML/TF risk. While there are legitimate reasons for using nominee general partners, these arrangements are sometimes misused to disguise beneficial owners and facilitate money laundering and other types of criminal offending.

Grounds to make a suspicious activity report (SAR)

100. For an existing customer or a customer engaging in an occasional transaction or activity, you **must** conduct enhanced CDD as soon as practicable after you become aware that you must report an SAR.[63] In this circumstance, the supervisors' view is that conducting enhanced CDD prior to submitting the SAR would strengthen the quality and usefulness of the SAR (see paragraph [139]).

101. You **must** also conduct enhanced CDD in any circumstances ordinarily eligible for simplified CDD **if** there are grounds to report a SAR. This includes when establishing a business relationship or conducting an occasional transaction or activity for one of the usually lower risk types of customers (as specified in section 18(2) of the Act). This also includes circumstances (as specified in section 18(3) of the Act) when a new person purports to acts on behalf of a customer that you have already established a business relationship with.

[60] Sections 58(2)(g) and 57(2)
[61] Regulation 12(a)– AML/CFT (Requirements and Compliance) Regulations 2011
[62] Regulation 12(b)– AML/CFT (Requirements and Compliance) Regulations 2011
[63] Section 22A(2)

102. For further information regarding the relationship between enhanced CDD and suspicious activity reporting, see Part 5 below.

New or developing technologies or products

103. New or developing technologies or 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.

104. Where you have a customer who wants to establish a business relationship, or conduct an occasional transaction or activity, involving new or developing technology or products that might favour anonymity, you **must** take additional enhanced CDD measures to mitigate and manage these ML/TF risks.[64] It is for you to determine what measures are required according to the level of risk involved.

105. Your risk assessment should consider whether your business is, or may be, exposed to customers involved in new or developing technologies or products. Your programme should then detail the procedures, policies, and controls that you will implement for this type of customer and technology.[65]

106. Effective 1 June 2024, if you are introducing a new or developing technology or a new or developing product (including a new delivery mechanism), there is an explicit requirement that you **must** update[66] your risk assessment before doing so.[67] This ensures that any new or evolving risks are fully examined, with mitigating steps as required taken before the new or developing technology or product is launched. Note that in practice, these steps should align with your existing procedures, policies and controls to keep your risk assessment (and in turn AML/CFT programme) up to date. The supervisors do not consider that creates additional or wider obligations relating to risk assessments.

[64] Sections 22(5) and 30
[65] Section 57(1)(i)
[66] This could include assessing the risks and updating the relevant section of your risk assessment relating to the new or developing technology or the new or developing product (including the new delivery mechanism).
[67] Regulation 13E AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)

Part 4: Enhanced CDD - SoW, SoF and additional measures

107. As set out in Part 3 of this guideline, there are various circumstances in which enhanced CDD obligations relating to SoW and/or SoF are required.[68] Where this applies, you **must** obtain information relating to the SoW and/or SoF of your customer[69] and you **must**, according to the level of risk involved, take reasonable steps to verify[70] that information.

108. Reporting entities should implement procedures, policies and controls for enhanced CDD that are appropriate to the product or service provided, the level of ML/TF risk and the customer's circumstances.[71] Your programme should set out how you will do this.

109. Effective 1 June 2024, your AML/CFT programme **must** differentiate when you will obtain and verify information regarding the customer's SoW or the customer's SoF, or alternatively both the customer's SoW and their SoF.[72] Note in some circumstances, you may also be required to implement additional enhanced CDD measures if examining SoW and/or SoF is not sufficient to manage and mitigate the ML/TF risks.[73]

110. 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.

111. For instance, an overseas customer with a complex ownership structure and multiple assets or income streams will require greater effort and more comprehensive investigation to verifiy SoW and/or SoF information than a customer with a simple ownership structure and financial arrangements.

Do I obtain and verify the SoW, the SoF or both?

112. In circumstances where you are establishing or updating your customer's risk profile you may need to obtain and verify information regarding their SoW. As set out in paragraph [18] above, 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.

113. However, when enhanced CDD is triggered by circumstances involving transactions or activities, you may need to focus more specifically on the SoF. As set out in paragraph [19] above, 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.

114. It is also 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

[68] Section 22(1) and (2)
[69] Section 23(1)(a)
[70] Section 24(1)(b)
[71] Section 22
[72] Regulation 15H AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)
[73] Regulation 12AB AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)

disproportionately large compared to your knowledge of a customer's wealth, this should trigger a more detailed examination of that transaction or activity.

115. It is for you to determine when to examine your customer's SoW, when to examine their SoF, or when to examine both. Your programme **must** contain procedures, policies and controls that set out how you differentiate and the respective circumstances in which you will obtain and verify the SoW, the SoF or both.[74]

116. **Note**: The supervisors acknowledge it may not be possible to document every different scenario in your AML/CFT programme in which you will examine SoW versus SoF, or both. Furthermore, that a case-by-case determination depending on the identified risk may be preferable in some circumstances. Therefore, your AML/CFT programme could consider the types of situations in which SoW or SoF (or both) will be examined, and how you will differentiate in practice. The key consideration when determining whether SoW or SoF (or both) should be examined is which of them best enables you to effectively mitigate the ML/TF risks. You are not able to simply 'choose' the option that is the easiest to fulfil.

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

117. You should ask your customer to provide you information about their SoW and/or SoF and record this information.[75] You **must** take reasonable steps, according to the level of risk involved, to verify this information using reliable and independent sources.

118. 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 and/or SoF of these persons. However, you need not obtain and verify SoW or SoF for every beneficial owner where they have nothing to do with the "customer's" SoW or SoF.

119. 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.

120. You **must**[76] 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.

121. 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

[74] Regulation 15H AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)
[75] Section 23
[76] Sections 23(1)(a) and 24(1)(b)

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.

122. 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?

123. 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?

124. When you verify SoW and/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.

125. 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:

- 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.

126. 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.

127. 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 and SoF

128. You are, of course, able to conduct your own research to supplement the information and documents that your customer provides you regarding their SoW and/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.

129. An accurate understanding of a customer's SoW and/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.

Additional enhanced CDD measures may also be required

130. In some circumstances, obtaining and verifying information relating to the customer's SoW and/or SoF may not be sufficient to manage and mitigate the ML/TF risk. For these situations, you **must** carry out additional enhanced CDD measures before establishing, and during a business relationship.[77]

131. There are four additional enhanced CDD measures prescribed in regulations. You should consider which one or a combination of the following is appropriate in the given circumstances:

(a) obtaining further information from the customer in relation to a transaction; or

(b) examining the purpose of a transaction; or

(c) enhanced monitoring of a business relationship; or

(d) obtaining senior management approval for transactions or to continue the business relationship.

132. For example, the examination of the purpose of a particular transaction may be necessary to understand if it represents a ML/TF risk. This could include asking the

[77] Regulation 12AB AML/CFT (Requirements and Compliance) Regulations 2011 (effective 1 June 2024)

customer for further information about it, such as to explain who the beneficiary is, their relationship to this person and the reason for the transaction.

133. If the explanation provided is not adequate, it may be necessary to require documentation from the customer (for example an invoice) to corroborate the information they have provided. Another control in your AML/CFT programme could be to obtain approval from your senior management to proceed with the transaction.

134. In other situations, such a decision to on-board a customer assessed as higher risk, it may be necessary to conduct an enhanced level of monitoring for the duration of that business relationship. This could include much more regular reviews and scrutiny of transactions and activities. Again, you could implement a control that senior management approval is obtained to establish or continue the business relationship.

135. Note the four additional enhanced CDD measures in regulations is a non-exhaustive list. There may be other enhanced measures you can take that are more appropriate and/or necessary to mitigate the ML/TF risks faced by your business.

136. Your additional enhanced CDD measures, and the circumstances in which you utilise them, should be detailed in your AML/CFT programme.

Part 5: Enhanced CDD and suspicious activity reporting

137. The relationship between enhanced CDD, the prohibitions if CDD cannot be conducted (see paragraphs [53] to [55] above) and suspicious activity reporting (including timeframes) is one of nuance that needs to be managed.

138. This is particularly so when enhanced CDD is triggered within a business relationship, such as by a particular transaction, pattern of transactions, or other high-risk situation.[78] This includes for existing customers (pre-Act customers), for whom there is also a specific requirement to conduct enhanced CDD when the reporting entity becomes aware a SAR must be reported.[79]

139. It is important to remember that:

- Enhanced CDD – This is a key part of determining whether there are grounds to submit a SAR. It enables you to differentiate between an activity that appears high-risk, but is actually legitimate, versus an activity or transaction that requires a SAR. Enhanced CDD also ensures that any resulting SAR can be of the highest quality and use to law enforcement agencies.

  Note: In some circumstances, the requirement for enhanced CDD will be identifiable upfront and prior to the transaction. In other circumstances, the requirement for enhanced CDD may only be identifiable post-transaction (for example if transaction monitoring software detects a sequence of transactions as unusual requiring examination). Similarly, it may not always be practicable to complete enhanced CDD prior to submitting the SAR.[80]

- Prohibitions – A purpose of the Act is to deter ML/TF. The prohibitions in the Act if CDD cannot be conducted (including enhanced CDD) are preventive. [81]

- Non-disclosure – The non-disclosure provisions prevent disclosure of a SAR and any information that will identify, or is reasonably likely to identify, the existence of a SAR, or a person that has handled, prepared or made a SAR.[82]

140. There is **no exemption** from conducting enhanced CDD on the basis that it could inadvertently 'tip off' the customer of a pending law enforcement interest in them (i.e. that a SAR is going to be submitted). The only exception to this is if a person is subject to a Commissioner's order, a production order, or a chief executive of Customs order, for which there is an exemption in place.[83]

141. Conducting enhanced CDD in high-risk circumstances could include asking your customer further questions about their activity or transactions, the source of funds and confirming the nature and purposes of the business relationship. Depending on the

[78] Section 22(1)(c) or (d)
[79] Section 22A. Note that section 22(1)(c) or (d) also applies to existing customers.
[80] Enhanced CDD, once completed, may necessitate an update of the original SAR or submission of a further SAR.
[81] Section 37
[82] Section 46
[83] Regulation 24AC AML/CFT (Exemptions) Regulations 2011. Note: members of the Financial Crime Prevention Network also have an exemption from enhanced CDD in certain circumstances under Part 17 of the AML/CFT (Class Exemptions) Notice 2018.

situation, you may also need (to take reasonable steps) to obtain documents from the customer to verify the source of funds information.

142. Such enquiries, when conducted properly and in good faith, do not constitute ‘tipping off’. Indeed, it may be the case that after conducting enhanced CDD you determine that your customer’s activity is not suspicious, and a SAR will not be required.

143. 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.[84]

[84] Section 51(1)(c)

Part 6: Enhanced CDD and Politically Exposed Persons (PEPs)

144. A PEP is a person who in the last 12 months has held a prominent overseas function. 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.

145. 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.[85]

146. 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.

147. You **must** conduct enhanced CDD on a customer who is a PEP.[86] In addition, your senior management (if applicable) **must** approve continuing the business relationship with a PEP.[87] You **must** obtain and take reasonable steps to verify the PEP's SoW or SoF.[88]

148. 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.

149. 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.

150. 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?

[85] Section 26
[86] Section 22(2)
[87] Section 26(2)(a)
[88] Section 26(2)(b)

Part 7: 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	• Structure table moved to front of document. • Addition of section 'When must SoW or SoF information be obtained?' • Various other changes for clarification purposes without substantial meaning changes.
Oct 2022	• Addition of bullet points on 'nominee directors' and 'nominee general partners'. • Addition of sections 'companies with nominee shareholders' and 'limited partnerships with nominee general partner and overseas limited partnerships.
April 2024	• Updated following new regulations 12AA, 12AB, 15, 15H and 15K of the AML/CFT (Requirements and Compliance) Regulations 2011 which impact on enhanced CDD obligations. New/updated paragraphs [18], [19], [36], [87], [116], [130] to [136]. • Inclusion of additional paragraphs [53]-[55] relating to terminating of business relationship if CDD cannot be completed, and a new Part 5 (paragraphs [137] to [143]) relating to the intersection between enhanced CDD and suspicious activity reporting. This follows Recommendation 128 in the 2022 Statutory Review of the Act. • Use of IVCOP as starting point for customers assessed as high risk to verify name and date of birth. New paragraphs [69] to [73]. • Other minor edits to some paragraphs for clarification purposes.

Disclaimer: This guideline has been produced by the AML/CFT supervisors under section 132(2)(c) of the Act. It is intended to assist reporting entities to understand their enhanced customer due diligence obligations under the Act. This guideline does not constitute legal advice.