AML/CFT

Anti-money laundering and countering financing of terrorism

AML/CFT Programme Guideline

October 2024

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

Reserve Bank of New Zealand
Te Pūtea Matua

Te Tari Taiwhenua
Internal Affairs

Contents of the AML/CFT programme guideline

Introduction

1. This guideline assists you to establish, implement and maintain an **anti-money laundering and countering financing of terrorism compliance programme (AML/CFT programme)** under the **Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the Act)**.

2. Your AML/CFT programme is your framework to combat the money laundering (ML) and terrorism financing (TF) risks that your business faces. Your AML/CFT programme must include adequate and effective procedures, policies and controls to detect ML/TF through your business, and to manage and mitigate the risk of it. Your AML/CFT programme must be in writing.[1]

3. The foundation of the Act is that it is risk-based. Your AML/CFT programme must be based on an ML/TF risk assessment.[2] This must be in writing and identify the ML/TF risks you face in the course of your business. Your risk assessment must also enable you to determine the level of risk involved so that you can effectively apply the requirements of the Act.[3]

4. While the Act contains various mandatory requirements, your AML/CFT programme can otherwise be proportionate to the risks that your business faces.

5. A risk-based approach does not stop you from providing higher risk products or services; nor from establishing business relationships with higher risk customers or conducting certain transactions or activities. Rather, a risk-based approach requires you to identify and understand the circumstances in which your risks are higher. You should then apply most of your AML/CFT resource to these situations. For low-risk customers or situations, the application of your AML/CFT resource can be less extensive.

6. This guideline has been produced by the AML/CFT supervisors under section 132(2) of the Act. It provides an overview of the requirements of an AML/CFT programme. It is supported by other guidelines relating to specific obligations under the Act. This guideline does not constitute legal advice.

7. 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.

8. 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 or reviewing your AML/CFT programme. After reading this guideline, if you still do not understand

[1] Section 57
[2] Section 57
[3] Section 58

any of your obligations you should contact your AML/CFT supervisor or seek legal advice.

9. All footnote references refer to the Act, unless stated otherwise.

10. Where AML/CFT Guidelines are referenced, they can be accessed at the following websites:

    - Financial Intelligence Unit (FIU): http://bit.ly/2zpmWPJ
    - Department of Internal Affairs (DIA): http://bit.ly/2gQ3Iev
    - Reserve Bank of New Zealand (RBNZ): http://bit.ly/2n6RYdp
    - Financial Markets Authority (FMA): http://bit.ly/2hV45oJ

Terms used in this guideline

11. 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 (and/or through ongoing customer due diligence and account monitoring) that could change their level of ML/TF risk. This may result in the need for additional customer due diligence (CDD) measures, including enhanced CDD.

    "Risk-based approach": Refers to the proportionate AML/CFT procedures, policies and controls that you implement in response to identified risks. An effective risk-based approach (sometimes called RBA) allows you to exercise informed judgement when meeting your AML/CFT obligations, including when conducting 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 procedures, policies and controls are in place.

    "Residual risk": This is the assessed ML/TF risk after AML/CFT procedures, policies and controls have been put in place.

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

Part 1: Establishing your AML/CFT programme

Purpose of the Act

13. The purposes of the Act are:

    - to detect and deter money laundering and terrorism financing;
    - to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force (FATF); and
    - to contribute to public confidence in the financial system.

Why must you have an AML/CFT programme?

14. The Act improves New Zealand's safety by making it harder for criminals to profit from their offending. It also provides a mechanism for potential criminal activity to be reported and then investigated, for tackling organised crime and depriving criminals of assets amassed from illegal activity. Similarly, by making it harder to finance terrorism, the Act disrupts terrorist activities, both in New Zealand and worldwide.

15. To do this, the Act requires financial institutions, casinos and designated non-financial businesses or professions (DNFBPs)[4] to establish, implement and maintain an AML/CFT programme. These businesses are known as "reporting entities". Further information regarding AML/CFT programme requirements are set out in Parts 2 to 8 of this guideline. Note that dealers in certain high-value items also have some limited obligations as reporting entities under the Act.[5]

16. All countries are exposed to illicit international and domestic money flows. The Act is an important part of New Zealand's implementation of the FATF international standards for combating money laundering, terrorism financing and proliferation.[6] The FATF 40 Recommendations and 11 Immediate Outcomes are the global standard for AML/CFT.

17. Compliance with and demonstrated effective use of the FATF standards are important for New Zealand's international reputation. New Zealand was last evaluated on these standards and outcomes in 2020.[7] The next evaluation is likely to be conducted in 2028 or 2029.

[4] Law firms, incorporated conveyancing firms, conveyancing practitioners, accounting practices, trust and company service providers and real estate agents within the meaning of s5(1) of the Act.

[5] Effective 11 May 2023, it became an offence under section 67A of the Act to buy or sell motor vehicles, boats, precious metals or stones, jewellery or watches for a cash transaction (or a series of related cash transactions) of NZ$10,000 or more. This means that only art and artefact dealers conducting cash transactions of NZ$10,000 or more have requirements as "high-value dealers" under the Act. For further information on their obligations, please contact the DIA.

[6] http://www.fatf-gafi.org/

[7] https://bit.ly/3M8VD2c

What is money laundering?

18. Money laundering is the process that criminals use to "clean" the money or assets generated from criminal activity.

19. Money laundering is not restricted to money and may include any property derived from criminal activity. Money laundering involves converting the money or assets from one form to another, disguising the ownership of it, or otherwise taking steps to conceal its origin.[8]

20. Money laundering enables criminals to enjoy the proceeds of their crimes or to set up or invest it in further criminal activity. Crimes may include drug dealing, fraud, tax evasion, theft, human trafficking, cybercrime, environmental crimes, and corruption. In the context of the relationship to money laundering, these crimes are known as "predicate offences".

21. Money laundering may be carried out by the person(s) that committed the predicate offence. This is known as self-laundering. Alternatively, money laundering may be conducted by a third party on their behalf, including by local or foreign businesses engaged by the offender.

Impact of money laundering

Money laundering is not a victimless crime. It enables and is the driver of the predicate crimes that cause significant harm to our communities. This impacts across New Zealand's health, justice, mental health and welfare systems.

Terrorism financing

22. Terrorism financing is the process by which terrorists fund either terrorist acts or ongoing operations to perform terrorist acts. Terrorists need financial support to carry out their activities and to achieve their goals.[9]

Proliferation financing

23. Proliferation financing (PF) is the act of raising or providing funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of weapons of mass destruction (whether nuclear, chemical or biological). This includes financing their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes).

Supervisors' view:

While the Act does not contain explicit requirements that you manage and mitigate

[8] Money laundering is an offence under s243 of the Crimes Act 1961.

[9] Terrorism financing is an offence under s8 of the Terrorism Suppression Act 2002.

your proliferation financing risks, the supervisors note that discharging your AML/CFT obligations may assist you to do so. Furthermore, to the extent that proliferation financing involves criminal activity generating income (for example cyber-crimes), the requirements of the Act directly apply.

What do you have to do?

24. The steps you must take under the Act are:

    - appoint an AML/CFT compliance officer (**compliance officer**).[10]
    - after undertaking a risk assessment, establish, implement and then maintain a written AML/CFT programme to manage and mitigate your ML/TF risks (based on your risk assessment).[11]
    - Your AML/CFT programme must include procedures, policies and controls to comply with all requirements of the Act – customer due diligence (including account monitoring), reporting requirements and record keeping.[12] A requirement of your AML/CFT programme is that it sets out what you need to, or will continue to do, to manage and mitigate your ML/TF risks.[13]
    - Your AML/CFT programme must also include your procedures, policies and controls for monitoring and managing compliance with your AML/CFT programme, including any functions you outsource to agents or other third parties, and for training and vetting staff.[14]

What are "procedures, policies and controls"

25. These terms are not defined in the Act. However, for the purposes of this guideline and your AML/CFT programme, they should be considered as:

    - **Procedures** set out the day-to-day operations of your business.
    - **Policies** set out expectations, standards, and behaviours in your business.
    - **Controls** are tools that management use in your business to ensure compliance with policies and procedures.

26. In practice, there should be an overlap between your procedures, your policies and your controls. You also have flexibility regarding the approach you take to develop and implement them. Considerations include:

    - The approach you take should be determined by the size, nature and complexity of your business and what works best to manage and mitigate your ML/TF risks.

[10] Section 56(2). For further information relating to the role of the compliance officer, refer to Part 7 of this guideline.
[11] Section 56(1)
[12] Section 57(1). These requirements are covered in Parts 2 to 5 of this guideline.
[13] Section 57(1)(f)
[14] Sections 57(1)(a)(b)(k) and (l). Also Reg.15G of the AML/CFT (Requirements and Compliance) Regulations 2011. These requirements are covered in Part 7 of this guideline.

- If you are a small business providing a low-risk product or service, you may only need simple procedures, policies and controls proportionate to this low risk. However, large businesses with complex risks, products, services and/or types of customers will require much more detailed and comprehensive AML/CFT programmes.
- You may include all procedures, policies and controls in the one primary AML/CFT programme document which is readily accessible by all employees that need to access it. Alternatively, different components of your AML/CFT programme could be held or set out in subsidiary documents, such as standard operating procedures for different business units or products and services.
- Maintaining version control, including any dates of reviews, any changes and version numbers, of your AML/CFT programme and ensuring your documented procedures, policies and controls accurately reflect your business practices prevents failure in your AML/CFT controls.
- Your AML/CFT procedures, policies and controls will function most effectively and efficiently when aligned with your wider customer onboarding and other business processes.

Your AML/CFT programme must be based on your risk assessment

27. You **must** base your AML/CFT programme on your risk assessment. Your risk assessment is the foundation document of your entire AML/CFT programme.

28. Your risk assessment must identify the ML/TF risks you face in the course of your business. Your risk assessment must also enable you to determine the level of risk involved so that you can apply the relevant requirements of the Act.[15] As part of your risk assessment, you must consider the nature, size and complexity of your business, the products and services you offer, the methods by which you deliver them, your types of customers and the countries and institutions you deal with, and guidance material produced by AML/CFT supervisors or the FIU.

29. The procedures, policies and controls in your AML/CFT programme must then respond to the risks identified in your risk assessment. One common way to approach this is for your risk assessment to consider your inherent risk, i.e. the assessed ML/TF risk before you implement your AML/CFT obligations. Your AML/CFT programme then comprises the procedures, policies and controls that you need to mitigate these risks, which results in your residual risk.

30. Your higher areas of residual risk are where you should more intensely direct your AML/CFT controls and resource. For example, if you rated a particular type of customer as “high risk” in your risk assessment, your AML/CFT programme should

[15] Section 58(3)

have procedures and controls to identify this type of customer and conduct enhanced CDD as part of your onboarding process.

31. Similarly, there should be procedures and controls in place to identify and respond to particular types of transactions (for example over a particular threshold or patterned), or other activities your risk assessment identifies to be higher risk. This could be for a new customer, or for a customer you have an established business relationship with (including a customer not previously displaying any higher risk indicators).

32. When developing your AML/CFT programme, it is also important to understand that each risk you identify in your risk assessment does not operate in isolation, but in combination with other risks. Where there are two or more higher risk indicators (often referred to as "red flags") together, your level of ML/TF risk compounds.

33. Your risk assessment must be kept up to date, effective and respond to any new or evolving ML/TF risks you face. For further information regarding your risk assessment, refer to the *Risk Assessment Guideline*.

Other AML/CFT programme requirements

34. Other legal requirements for your AML/CFT programme include:

- Your AML/CFT programme's procedures, policies and controls **must** be both **adequate** and **effective**.[16] "Adequate" means your procedures, policies and controls must be adequately designed to meet all requirements of the Act. "Effective" means that those procedures, policies and controls must manage and mitigate your ML/TF risks and operate effectively in practice.
- You **must** review your AML/CFT programme to ensure it is up to date, identify any deficiencies in its effectiveness, and make any changes identified as being necessary.[17]
- Your AML/CFT programme **must** be independently audited by an appropriately qualified person every three years, unless you are notified by your AML/CFT Supervisor that a four-year timeframe applies. An independent audit may also be required at any other time at the request of your AML/CFT supervisor.[18]
- You **must** prepare and submit an annual report to your AML/CFT supervisor.[19] This must be in the prescribed form and at a time appointed by the supervisor. Refer to the *User Guide: Annual AML/CFT Report*.

Supervisors' view:

Your AML/CFT programme should be specific to your business. While use of a

[16] Section 57(1)

[17] Section 59(1). Refer Part 8 of this guideline

[18] Sections 59(2) and 59A. Also Reg.13 of the AML/CFT (Requirements and Compliance) Regulations 2011. Also refer Part 8 of the guideline

[19] Section 60. Refer Part 4 of this guideline

template may be a good starting point to develop your AML/CFT programme, the supervisors consider that generic procedures, policies and controls not based on your risk assessment and/or not tailored to your ML/TF risks are unlikely to comply with the Act.

Using guidance for your AML/CFT programme

35. You **must** also consider any applicable guidance material produced by your AML/CFT supervisor or the FIU. This includes:
    - The National Risk Assessment (NRA) and FIU guidance material.[20]
    - Sector risk assessments (SRAs) and guidelines produced by the AML/CFT supervisors.
    - Any sector or other specific guidelines by your AML/CFT supervisor.

36. Other guidance you may find useful when developing your AML/CFT programme is published by the FATF, the Asia Pacific Group on Money Laundering (APG)[21] and other overseas AML/CFT agencies such as the Australian Transaction Reports and Analysis Centre (AUSTRAC).[22]

Detecting money laundering and terrorism financing

37. To assist you to develop your AML/CFT programme, it is worthwhile to cover the basics of money laundering and terrorism financing. This will assist you to understand how it might occur through or using your business.

38. Money laundering, in so far as it relates to money, is often conceived to be a three-step process: **placement**, **layering** and **integration**:
    1. **Placement:** This involves introducing criminally derived funds into the financial system. For some predicate offences, including drug offending, the criminally derived funds are likely held and placed into the financial system in cash. For other offences, such as fraud or tax evasion, placement may occur electronically.

       Placement may occur through large transactions deposited directly into an account, or by breaking up large amounts into smaller sums. It could be deposited by an account holder or a third party, in cash or through electronic payments. It may occur via other mechanisms such as purchasing shares or loading credit cards.
    2. **Layering:** Funds are moved or converted into other property to distance or disguise them from the criminal derived source. This may involve breaking the funds up or moving them around in a series of transactions, such as between bank accounts. Funds might be channelled through the purchase and sale of investment

[20] Some FIU guidance material is only accessible by reporting entities registered with the FIU's goAML system.
[21] http://www.apgml.org/
[22] http://www.austrac.gov.au/

instruments or high-value goods or be wired through various accounts across the world. In some instances, a launderer might disguise the transfers as payments for goods or services, giving them an appearance of legitimacy.

3. **Integration:** The funds then emerge from the financial system in a form that appears legitimate. This is the ultimate objective of laundering, the funds can then be used for further criminal activity, for legitimate business or enjoyed as property, such as real estate or high-value assets.

39. While understanding this three-step process is useful, it is also important to note that:

- Money laundering takes many forms and has many typologies, some simple and others complex and they are constantly evolving.
- For the offence of money laundering to occur, it does not require all three steps to be completed. One is often enough.
- The three steps are not always discrete, they can often overlap or be concurrent. Furthermore, in some circumstances (such as electronic payments made as part of frauds, scams and cyber-crimes), the placement stage of money laundering is often inherent to the predicate offending.
- Money laundering does not just occur in relation to money; any property that is the proceeds of crime can be laundered. However, the three-step model is more relevant to money than to other property that is the proceeds of crime.

40. Consequently, your AML/CFT programme should not be restricted to, nor necessarily need to differentiate between, placement, layering and integration. Particularly for a small business with limited products or services or customer numbers, a simpler more holistic approach primarily focussing on whether activities or transactions have a legitimate economic or lawful purpose may be more effective.

41. Relatedly, you should also understand that your suspicious activity reporting obligations (refer paragraphs [93] to [99] below) do not just apply to suspicion of ML/TF. Rather, your reporting obligations apply to circumstances in which there are reasonable grounds to suspect <u>any</u> criminal activity.[23]

42. While money laundering is the process of concealing the illicit origin of proceeds of crime, terrorism financing is the collection or the provision of funds for terrorist purposes. In the case of money laundering, the money or assets are always the proceeds of crime, whereas in the case of terrorism financing, funds can stem from both licit and illicit sources.

43. Therefore, the primary goal of individuals or entities involved in terrorism financing is not necessarily to conceal the source of the funds but to conceal the nature of the funded activity.

[23] Section 39A

Part 2: CDD requirements for a new customer

44. Customer due diligence (CDD) is a cornerstone of your AML/CFT programme.

45. CDD is the process through which you develop an understanding of your customers, and the ML/TF risks they pose to your business. CDD is often referred to as "Know your customer" or "KYC".

46. Those seeking to launder money or finance terrorism generally try to avoid attracting attention by masking their identity and/or the illegal source of their funds (in part or whole). They may also mask their intent to misuse legally obtained funds and/or the identity of the beneficiaries of those funds. Knowing who your customer is (and understanding their financial activities), will make it more difficult for them to conduct illegal activities and transactions through your business.

47. Your AML/CFT programme **must** have procedures, policies and controls to comply with the CDD requirements of the Act.

New customer

48. You must conduct CDD when you establish a **business relationship** with a new customer:[24]

> **Definition of business relationship**
>
> A business relationship is a business, professional or commercial relationship between a reporting entity and a customer that has an element of duration, or is expected to have an element of duration, when contact is established.[25]

49. You must also conduct CDD if a person (who you do not have a business relationship with) seeks to conduct certain types of one off or **occasional transaction or activity**.[26] Further information relating to these "occasional customer" situations are detailed in paragraphs [59] to [70] below.

50. **Note:** In practice, the definition of business relationship is broad,[27] and many reporting entities will have "an element of duration" to their engagement with all their customers. If this applies to you, the "occasional customer" provisions (as set out in paragraphs [59] to [70] below) are not relevant to your business and can be disregarded.

[24] Section 14(1)(a)
[25] As defined in s5(1)
[26] Section 14(1)(b). Reg.15K of the AML/CFT (Requirements and Compliance) Regulations 2011
[27] *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited* [2017] NZHC 2363 at [44]

Types of CDD

51. You are required to conduct either **standard**, **simplified** or **enhanced** CDD depending on the ML/TF risk associated with your customer and the activities or transactions they undertake. In summary:

- **Standard CDD** is likely to apply to most customers. You are required to obtain and verify the full name of the customer, their date of birth (if an individual) or entity identifier or registration number (if not an individual) and address. Any beneficial owner[28] of the customer, and any person acting on behalf of the customer must also be identified and verified.[29]
- **Simplified CDD** only applies for specified types of organisations including government departments, local authorities, and certain listed companies considered to be low risk.[30] For customers eligible for simplified CDD, you are only required to obtain and verify information relating to the person acting on behalf of the customer and their authority to do so.[31]
- **Enhanced CDD** must be conducted in various higher risk situations. In addition to standard CDD requirements, you are required to obtain and verify information relating to the source of wealth or source of funds (or both) of the customer.[32] In some circumstances, additional measures must also be applied if examining the customer's source of funds or wealth is not sufficient to manage and mitigate the ML/TF risks.[33]

  Note: there are further specific enhanced CDD requirements relating to politically exposed persons, wire transfers and new or developing technologies that may favour anonymity.[34] For more detailed information on these requirements, refer to the *Enhanced CDD Guideline* and *Wire Transfers Guideline.*[35]

Check List:

A. You should provide an overview of how your business will address the ML/TF risks identified in your risk assessment and your approach to conducting CDD.

B. You must set out how you will determine when enhanced CDD is required and when simplified CDD is permitted.

[28] As defined in s5(1)

[29] Sections 11, 14-16

[30] Refer to section 18 of the Act for more information

[31] The same process (also known as simplified CDD) may also be conducted within any business relationship when a new person purports to act on behalf of a customer. Refer to section 18(3).

[32] Sections 22(1), 22A, 23 – 24. Also Reg.15H of the AML/CFT (Requirements and Compliance) Regulations 2011

[33] Reg.12AB of the AML/CFT (Requirements and Compliance) Regulations 2011. Additional measures include obtaining further information or examining the purpose of a transaction, enhanced monitoring or obtaining senior management approval for transactions or to continue the business relationship.

[34] Sections 22(2)-(5), 26-30.

[35] Note: Effective 1 June 2024. reporting entities that are intermediary or beneficiary institutions of an international wire transfer have additional procedures, policies and controls that must be included in their AML/CFT programmes (Reg 15E and 15F of the AML/CFT (Requirements and Compliance) Regulations 2011).

C. If your business does not conduct transactions or activities outside of a business relationship, you should clearly state this in your AML/CFT programme, as well as state your controls to ensure this.

A two-step process

52. Conducting CDD is a two-step process:

    1. **Obtaining information** - You must obtain certain information from the customer. As noted in paragraph [51] above, the required information varies depending on the type of customer[36] and whether simplified, standard or enhanced CDD is being conducted.

    2. **Verifying information** - You must then take reasonable steps to verify the information. In most circumstances, the extent of the verification steps you must take is according to the level of risk involved.[37] For a customer determined to be lower risk, the verification you undertake can be less extensive. However, if a customer, transaction or situation is higher risk, the extent of your verification must be robust.

Establishing a business relationship

53. You must conduct CDD (at the required level) before establishing a business relationship with a customer.[38] The Act requires you to carry out CDD on:[39]

    a. your customer
    b. any "beneficial owner" of a customer
    c. any person acting on behalf of a customer

54. As part of conducting CDD, you must also obtain information on the nature and purpose of the proposed business relationship.[40] Effective 1 June 2025, there is also a requirement to risk-rate any new customer when you conduct standard or enhanced CDD.[41]

Supervisors' view:

The supervisors consider an accurate risk-rating of a customer as key to being able to effectively and efficiently discharge your AML/CFT obligations during the subsequent business relationship. Accurate risk ratings inform which of your

[36] Whether an individual, a legal person or a legal arrangement, and depending if a person is acting on behalf of the customer.

[37] Note: There is an exception to this risk-based approach when conducting standard CDD on the customer's name, date of birth and address (if an individual), or name, entity identifier or registration number, address or registered office (if not an individual). Instead, your verification must be to a reasonable level of assurance.

[38] Note that subject to certain conditions, you can delay the verification component of CDD, as long as this is completed as soon as practicable. Refer sections 16 and 24

[39] Unless simplified CDD applies

[40] Sections 17(a), 21 and 25

[41] Reg.12AC of the AML/CFT (Requirements and Compliance) Regulations 2011

customers require more regular review and monitoring, and which require less ongoing scrutiny (refer Part 3 below). This allows the most efficient use of your compliance resource and is central to a risk-based approach.

Note: You have flexibility in the approach you take to risk-rating your customer, for example whether you use a numeric or a simpler low-medium-high scale. You could use an automated solution or you could use a qualitative assessment made by your employee that onboards the customer. Your risk rating process should be based on the findings of your risk assessment.

55. **Standard CDD** (as described in paragraph [51] above) is required for most customers. For a customer that is an individual, the requirements are straightforward.[42] For a customer that is a legal person or legal arrangement,[43] conducting standard CDD is more complex. This is because legal persons and legal arrangements can be used to disguise the criminal origin of funds or assets, who controls them and the reasons that transactions or activities are conducted.

56. By understanding the ownership and control structure of legal persons and arrangements, you can identify the beneficial owner(s) and in turn, determine the level of risk associated with the customer. For further information regarding beneficial ownership and standard CDD requirements for legal persons and legal arrangements, refer to the *Beneficial Ownership Guideline* and the *CDD Guidelines for Companies, Limited Partnerships* and *Trusts*.

57. When conducting standard CDD, you must also obtain sufficient information to determine whether the customer should be subject to enhanced CDD.[44] This is an important part of a risk-based onboarding process. While the information you obtain from your customer does not need to be extensive, it should allow you to identify indicators of higher risk (based on your risk assessment). In practice, obtaining this information can be aligned with the information you obtain regarding the nature and purpose of the proposed business relationship (refer paragraph [54] above). Furthermore, conducting standard CDD may itself identify risk indicators that trigger enhanced CDD.

58. **Enhanced CDD** (as described in paragraph [51] above) is required for any customer you determine to require enhanced CDD (based on your risk assessment and

[42] The *Amended Identity Verification Code of Practice* (IVCOP) provides a "safe harbour" for the verification of an individual's name and date of birth (for persons assessed low to medium risk). For onboarding a customer online, there is a requirement to ensure the person being dealt with is the genuine holder of the identity (being verified) claimed to be. This is known as "binding assurance" or the "linking mechanism". Refer to the *Electronic Verification Explanatory Note* for further information.

[43] A "legal arrangement" means a trust, a partnership (excluding a limited partnership), a charitable entity within the meaning of s4(1) of the Charities Act 2005, an unincorporated society, a fiducie, a treuhand or a fideicomiso (as defined in s5(1) of the Act and Reg.10AAAC of the AML/CFT (Definitions) Regulations 2011).

[44] Section 17(b)

standard CDD conducted).[45] There are also various types of customers for whom enhanced CDD is mandatory if establishing a business relationship:

- 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.[46]
- a company with nominee shareholders or shares in bearer form.[47]
- 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.[48]
- a company with one or more nominee directors.[49]
- a limited partnership with a nominee general partner.[50]
- a politically exposed person (PEP) or where a beneficial owner of a customer is a PEP.[51]
- the involvement of new or developing technologies, or new or developing products, that might favour anonymity, in a business relationship.[52]

Check list:

D. You must set out your procedures for simplified, standard and enhanced CDD respectively, including the information you obtain from the customer and what reliable and independent documents or other sources you use to verify this.

E. You must detail the circumstances in which you conduct each type of CDD for a new business relationship. This should include your risk-based triggers (based on your risk assessment and standard CDD).

F. For enhanced CDD, you must ensure your procedures respond to and are tailored to your higher risks (identified in your risk assessment). This includes identifying when you obtain and verify information relating to the customer's source of wealth or funds (or both), and when further enhanced CDD measures are required.

[45] Section 22(1)(d)

[46] This includes any country identified by the FATF as being a high-risk jurisdiction subject to a call for action. Refer Reg.15 of the AML/CFT (Requirements and Compliance) Regulations 2011.

[47] Section 22(1)(a)(b)

[48] Section 22(1)(c)

[49] Reg.12(a) of the AML/CFT (Requirements and Compliance) Regulations 2011. Refer to the Companies CDD Guideline for further information on complying with this regulation.

[50] Reg.12(b) of the AML/CFT (Requirements and Compliance) Regulations 2011. Refer to the Limited Partnerships CDD Guideline for further information on complying with this regulation.

[51] Sections 22(2), 26

[52] Section 30

Occasional customers

59. As noted in paragraph [50] above, the definition of "business relationship" is broad, and many reporting entities will have "an element of duration" to their engagement with **all** their customers (for example in the financial markets sectors).

60. If so, the provisions of the Act set out from [61] to [70] below relating to "occasional customers" will **not** apply to you. However, in some sectors (for example the money remittance sector, the banking sector relating to payments by third parties) transactions **do occur** with persons outside of a business relationship. These paragraphs are therefore applicable to those customers.

61. You must conduct CDD:

    - if a person (that you do not have a business relationship with) seeks to conduct an occasional transaction or occasional activity through your business.[53]
    - if a person (that you do not have a business relationship with and is not conducting an occasional transaction with you) seeks to conduct a transaction through your business and there are grounds to report a suspicious activity.[54]

      Note: "Occasional transaction" and "occasional activity" are defined terms (as explained further below).

Occasional transactions and activities

62. You must conduct CDD (at the required level) if a person seeks to conduct an occasional transaction or activity.

63. In the same way required for a person establishing a business relationship, you must conduct CDD on your customer, any beneficial owner of your customer and any person acting on behalf of your customer. Similarly, you must conduct either standard, simplified or enhanced CDD (as described in paragraphs [51] above) depending on the type of customer and the level of risk. However, for a person seeking to conduct an occasional activity or transaction:

    - You are not permitted to delay the verification component of CDD until after the transaction or activity.
    - You do not need to obtain information on the nature and purpose of the business relationship, nor sufficient information to determine whether enhanced CDD is required. However, other risk-based enhanced CDD triggers still apply.

[53] Section 14(1)(b).

[54] Reg.15K of the AML/CFT (Requirements and Compliance) Regulations 2011

Note however: there is an explicit requirement to conduct enhanced CDD as soon as practicable after you become aware that you must report a SAR in relation to a person conducting an occasional transaction or activity.[55]

64. **Occasional transactions** are based on thresholds. These range from NZ$1,000 to NZ$10,000 depending on the type of transaction:

- NZ$1,000 or more - for wire transfers (domestic or international), currency exchange, money orders, postal orders, stored value instruments if redeemable for cash, and transactions involving virtual assets.
- NZ$5,000 or more - stored value instruments if only redeemable for non-cash.
- NZ$6,000 or more - for cash transactions in casinos.
- NZ$10,000 or more - for any other cash transaction.[56]

Note: an occasional transaction includes a cash deposit (over the applicable threshold) by a third party (i.e. a person that is not your customer)[57] into an account held by your customer.

65. It is important to understand the definition/threshold of an occasional transaction includes a transaction conducted in "several operations that appear to be linked". This ensures a person is subject to CDD if they conduct two or more related transactions each below the threshold, but that in combination exceed it (for example multiple cash transactions on the same or consecutive days, and/or at different agents or branches). You should have steps in place to detect this.

Supervisors' view:

In practice, the supervisors consider that your procedures, policies and controls to identify persons that have two (or more) linked transactions, each under the applicable threshold, should be risk-based (based on your risk assessment). It is very important to focus on detecting and responding to a person(s) intentionally transacting this way to avoid your CDD requirements.[58] You could consider:

- For in person transactions, review the person's transaction history against timebound rules and parameters, with controls in place to identify linked transactions so that the CDD process can be commenced.[59]
- For automated transactions (for example third party ATM cash deposits), adopt appropriate thresholds/controls to mitigate the risk of linked transactions (that in combination exceed an applicable threshold).

[55] Section 22A(2)

[56] Refer AML/CFT (Definitions) Regulations 2011.

[57] Unless the person's identity and authority to act on behalf of the customer has previously been verified pursuant to s18(3). If so, the person is acting on behalf of your customer and not conducting an occasional transaction.

[58] "Structuring" a transaction to avoid AML/CFT requirements is an offence under s101.

[59] Effective 1 June 2024, Reg.8 of the AML/CFT (Exemptions) Regulations 2011 that exempted requirement to keep records of the parties (i.e. the names) to a transaction (that is not an occasional transaction/within a business relationship) is repealed. Obtaining names (even without verification) will now assist you to identify and respond to potentially linked transactions outside of a business relationship by the same person.

For the types of transactions where the receiving party is your customer, your transaction monitoring could include rules/alerts to identify potentially linked payments by a third party (e.g. multiple cash deposits to the same account in a short period of time).[60] This triggers a further examination and a CDD process on the third party.

66. **Occasional activities** are not threshold based. Instead, they include any activity in the definition of DNFBP (that does not occur within a business relationship).[61] In practice, instances of an occasional activity will be uncommon for most businesses. However, providing a one-off company formation, arranging for a person to act as a nominee director or shareholder or trustee (in the absence of acting as the nominee or trustee) or an ad hoc request to a DNFBP to assist with a financial transaction is likely to meet the definition of an occasional activity.[62]

Element of duration

67. You should also have procedures in place to identify a person transacting occasional transactions or activities with sufficient regularity that you do have a business relationship with them (i.e. there is an element of duration).

68. You should develop appropriate parameters for this in your AML/CFT programme. At the point of determination there is a business relationship, you will then need to ensure you have obtained information on the nature and purpose of the business relationship, and sufficient information to determine if enhanced CDD is required (refer paragraph [57] above).

Check list:

G. If you allow occasional transactions and/or occasional activities, then you must set out your procedures for simplified, standard and enhanced CDD for a person seeking to conduct an occasional transaction or activity, including any differences from the CDD policies in place for new business relationships.

H. You should set out your risk-based occasional transaction and activity procedures for (a) identifying a series of linked operations/transactions that in combination, meet the occasional transaction threshold, and (b) identifying a customer transacting or conducting activities with sufficient regularity that there is a business relationship. Your focus should be persons seeking to intentionally circumvent your CDD requirements.

Other transactions outside business relationship where there is suspicion

69. Some businesses conduct a further type of transaction with a customer. These are lower value transactions that are not conducted within a business relationship and do

[60] Refer footnote 59 above

[61] Regulation 24A of the AML/CFT (Exemptions) Regulations 2011

[62] Refer to the definition of designated non-financial business or profession in s5(1) of the Act.

not meet the definition of occasional transaction. These transactions may range in value up to NZ$10,000 (depending on the type of transaction and applicable occasional transactional threshold – for the thresholds and definition refer paragraph [64] above).

70. You do not normally have any CDD obligation in relation to these transactions as they are typically considered low risk. However, there are some types of higher risk or suspicious transaction that may only be of relatively low value (for example terrorism financing or online child exploitation). When a person seeks to conduct such a transaction and there are grounds to report a suspicious activity, you are required to conduct (at least standard) CDD.[63]

Supervisors' view:

In practice, the supervisors again consider that your procedures, policies and controls to identify such a customer/transaction should be risk-based (based on your risk assessment):

- You should therefore focus on the types of transactions (for example certain international payments, or larger cash transactions, but under an occasional transaction threshold) where the risk is higher.
- Your procedures can be aligned with those in place to identify persons intentionally circumventing your CDD requirements in relation to occasional transactions (refer paragraph [64] above).
- Another important indicator of suspicion for these transactions may be behavioural during any interaction you have with the customer. For example, the customer is nervous, unwilling to provide information or asks about AML/CFT procedures.

Check list:

I. You should align your procedures for identifying persons seeking to conduct a suspicious transaction (that is not within a business relationship or an occasional transaction) with your procedures for detecting persons circumventing your CDD requirements for occasional transactions.

Prohibitions

71. The prohibitions in the Act if CDD cannot be conducted are preventive. If you are not able to complete CDD for a customer, you **must** not carry out any occasional transaction or activity for them, nor establish a business relationship with them. You must also consider if a SAR should be submitted to the FIU.[64]

[63] Reg.15K of the AML/CFT (Requirements and Compliance) Regulations 2011

[64] Section 37. Note that other prohibitions apply to customer anonymity and shell banks.

72. 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.

Check list:

J. You should ensure your procedures, policies and controls for the Act's prohibitions are integrated with your wider CDD obligations, with appropriate escalation, determination and authorisation processes for this to be carried out as soon as practicable.

Part 3: CDD requirements within a business relationship

73. Once you have established a business relationship with a customer, you must conduct risk-based **ongoing CDD and account monitoring.**

74. This is to ensure that the business relationship and the transactions relating to it are consistent with your knowledge about the customer, their business and risk profile, and to identify any grounds for reporting suspicious activity.[65] This may require you to update the CDD information and records you hold for the customer.[66]

75. Ongoing CDD and account monitoring may also trigger **enhanced CDD.** Or enhanced CDD may separately be triggered within a business relationship based on parameters in your AML/CFT programme. Enhanced CDD within a business relationship is required for a higher risk transaction(s), activity, or situation (refer *Enhanced CDD Guideline* and paragraph [83] to [86] below)**.**

76. Your AML/CFT programme **must** have procedures, policies and controls to comply with your CDD obligations within a business relationship. This applies in relation to any customer that you have established a business relationship with under the Act, as well as for any existing customer (who you had a business relationship with at the time your obligations under the Act came into effect).

Ongoing CDD and account monitoring

77. Ongoing CDD requires you, according to the level of risk involved, to regularly review CDD and any other information you hold related to your business relationship with a customer. This includes information you obtained relating to the nature and purpose of the business relationship, and sufficient information to determine if enhanced CDD is required (refer paragraph [54] and [57] above).

78. Account monitoring operates concurrently to ongoing CDD. It requires you, also according to the level of risk involved, to regularly review a customer's account activity and transaction behaviour.[67] For a DNFBP, it also involves reviewing the DNFBP activities that you provide to the customer.[68]

Supervisors' view:

The supervisors consider that your respective procedures, policies and controls (including the parameters you set) for ongoing CDD and account monitoring should be risk-based. Importantly, they should leverage each other. A review of CDD information could trigger review of the customer's transactions, or vice versa.

[65] Section 31
[66] Reg.15J of the AML/CFT (Requirements and Compliance) Regulations 2011
[67] Section 31
[68] Reg.15J of the AML/CFT (Requirements and Compliance') Regulations 2011

Examples of triggers include:

- When your interactions with a customer identify a material change that could increase their risk profile. For example, there is significant change in the products or service you provide or in their personal circumstances, such as they move abroad.
- If your account monitoring rules (see paragraph [79] below) trigger an alert (that is not a false positive) in relation to a customer's transaction(s) or activity.

Risk-based reasons include:

- As part of a scheduled review of a customer that you have previously determined higher risk (e.g. at onboarding or during a subsequent review). Your review of a customer you have assessed as high-risk should be more frequent than a medium risk customer.

Your framework/methodology for determining your risk-based triggers and frequency of your reviews should be documented in your AML/CFT programme.

Note: The supervisors do not consider it necessary for you to review CDD information, activity or transaction behaviour in the absence of a risk-based reason or trigger for doing so. This means you are not expected to conduct ongoing reviews of customers that are clearly low risk, for example based on the product and service provided and/or a customer with a low-risk rating.

79. You can use a manual or electronic system (or a combination of the two) to monitor your customers' transactions and activities. This must enable you to detect complex or unusually large transactions, or unusual patterns of transactions or behaviour, and/or where there are grounds to report a suspicious activity. Your account monitoring will be shaped by the factors considered in your risk assessment. For some businesses, a manual system may be sufficient but not so for others. For example, if you conduct large numbers of transactions, or have a large customer base, a manual system will not allow you to adequately, or effectively, monitor transactions and activities.

Supervisors' view:

Specific to your account monitoring, the supervisors consider that your procedures, policies and controls should be directed at detecting complex or unusually large transactions, or unusual patterns of transactions or behaviour, and/or where there may be grounds to report a suspicious activity. Your monitoring rules should be risk-based and identify those transactions and/or activities that require review, including those circumstances when enhanced CDD is required. When developing your monitoring rules, you should consider:

- How your account monitoring rules address the specific risks identified in your risk assessment.
- Setting appropriate, risk-based rule thresholds and parameters targeting higher-

risk activities, transactions, products, customers and countries.

- Nature and purpose information obtained during CDD (at onboarding or ongoing). This information can be built into the rules themselves and/or used as part of the review into any alerts generated.
- Prioritising your review efforts on those alerts that flag higher-risk activity (although all alerts should be reviewed).
- Including controls to manage circumstances in which the same transaction is flagged multiple times for review.
- Including clear timeframes for when generated alerts should be reviewed, actioned and reported (when necessary).
- Regularly reviewing the effectiveness of your transaction monitoring system, such as the rate of suspicious activity detection, false positives and compliance with timeframes.
- Regularly, and if necessary, updating and refining your transaction monitoring rules to reflect changes in your business, emerging risks and new typologies.
- How you maintain records of your monitoring activity.

Updating CDD information

80. As part of your review of CDD and any other information you hold related to your business relationship with a customer, you may need to update this information (as is necessary to mitigate your ML/TF risks). You must then take reasonable steps to verify the updated information.

81. Your requirement to obtain and verify this updated information is based on the level of risk. Relatedly, in determining the extent to which the information must be updated or verified, you must consider when CDD was last conducted, and the adequacy of the information held.[69] Effective 1 June 2025, there is also a requirement to review (and update), as appropriate, your customer's risk rating (refer paragraph [54] above).

82. Note: the requirement to update CDD information applies both to customers with whom you established a business relationship under the Act, and also to existing (pre-Act) customers. For existing customers specifically, there is also an explicit requirement to conduct CDD if there has been a material change in the nature or purpose of the business relationship and you consider you have insufficient information about the customer.[70]

[69] Reg.15J of the AML/CFT (Requirements and Compliance) Regulations 2011
[70] Section 14(1)(c)

Supervisors' view:

In practice, the supervisors consider that you **only** need to consider updating CDD information (as part of your ongoing CDD and account monitoring) when there is a risk-based reason or trigger for doing so.

Your procedures, policies and controls for determining if you should update CDD information, and then determining what CDD to update, should therefore be directed at understanding your customer's ML/TF risk profile (or any changes to it). For example, if your review identifies inconsistencies between CDD information you've previously obtained/verified and the customer's transactions and activities, you could:

- Obtain updated nature and purpose information on the business relationship.
- Obtain updated or further information to sufficiently determine if enhanced CDD is required (when only standard CDD was conducted previously).
- Obtain and verify updated or further information regarding the customer's source of wealth or funds (or both) (if enhanced CDD was conducted previously).

Additionally, in relation to customers that are legal persons and legal arrangements, you may need to:

- Obtain and verify updated standard CDD information in order to understand changes to the customer's beneficial owner(s), including to identify any material change and/or increase in the customer's risk profile.

Note: The supervisors do not consider it necessary (nor consistent with a risk-based approach) that you regularly reverify a person's biographical information if you have verified this previously (unless there are concerns regarding their identity or it is otherwise necessary, for instance a name change). The expiry of an identity document does not in itself trigger a requirement to update a customer's CDD information.

In circumstances when you review CDD information held for a customer and determine there is no need to update it, this decision should be recorded against the customer's file for future reference.

Enhanced CDD

83. As noted at [75] above, enhanced CDD may also be required within a business relationship. Enhanced CDD is required when:

    - 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.[71]
    - You consider, based on your risk assessment and AML/CFT programme, that the level of risk involved is such that enhanced CDD should apply to a particular

[71] Section 22(1)(c)

situation.[72]

- For an existing (pre-Act) customer, as soon as practicable after you become aware that you must report an SAR.[73]

84. It is important to understand that enhanced CDD may be triggered by ongoing CDD and account monitoring. Or alternatively, it may be triggered separately based on parameters included in your AML/CFT programme (based on your risk assessment). 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.[74]

85. Also note that enhanced CDD 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.

86. For further information regarding enhanced CDD requirements within a business relationship, refer to the *Enhanced CDD Guideline*.

Check list:

K. You should ensure your ongoing CDD and account monitoring procedures, policies and controls (including requirements to update CDD information) are risk-based, clearly documented and reviewed regularly to ensure they are up to date.

L. Whether a manual or automated (or combination) monitoring system is used, you should have clearly documented triggers and/or ML/TF alerts generated for review and examination. Thresholds and scenarios for this should be based on your risk assessment and commensurate with the types of customers you deal with, the products and services you offer, and the value and volume of transactions undertaken.

M. You should set out your procedures, policies and controls for conducting enhanced CDD within a business relationship, whether triggered by ongoing CDD and account monitoring, or based on separate parameters (based on your risk assessment). This includes the circumstances and process to be followed when the requirement for enhanced CDD is identifiable prior to the transaction.

[72] Section 22(1)(d)

[73] Section 22A(2). Refer the definition of "existing customer" in s5(1) of the Act.

[74] Enhanced CDD, once completed, may necessitate an update of the original SAR or submission of a further SAR.

Prohibitions

87. As noted at paragraph [71] above, the prohibitions in the Act are preventive. If you are not able to complete CDD for a customer when it is triggered within a business relationship, the business relationship **must** be terminated. You must also consider if a SAR should be submitted to the FIU.[75]

88. 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.

89. 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). 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 for you to immediately cease the business relationship due to another contractual agreement.[76] That said, the supervisors consider that the termination process should commence as soon as you determine you are unable to complete CDD.

90. The High Court[77] 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.

91. Your procedures, policies and controls to comply with the Act's prohibitions should be documented in your AML/CFT programme.

Check list:

N. You should ensure your procedures, policies and controls for the Act's prohibitions (both for a new customer and within a business relationship) are integrated with your wider CDD obligations, with appropriate escalation, determination and authorisation processes for this to be carried out as soon as practicable.

[75] Section 37. Note that other prohibitions apply to customer anonymity and shell banks.

[76] 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.

[77] *Arjang v NF Global Limited [2021] NZHC 395* at paragraphs [53] and [55]

Part 4: Reporting requirements

92. You are required to submit two types of reports to the FIU under the Act – suspicious activity reports (**SARs**) and prescribed transaction reports (**PTRs**).

Suspicious activity reports

93. Suspicious activity reporting is a key part of your AML/CFT programme.

94. SARs are analysed by the FIU and provide valuable information to assist the New Zealand Police, other law enforcement and security agencies to investigate financial crime. It is important to note the requirement to submit a SAR does not just apply when there is suspicion of money laundering or terrorism financing, it applies to suspicion of any criminal activity.[78]

95. You must submit a SAR when there are reasonable grounds to suspect that a transaction, service, or inquiry, is or may be relevant to the investigation, enforcement or prosecution of crime. This includes if a person seeks to conduct a transaction, but it is not ultimately conducted (for example if the customer refuses to comply with CDD obligations). Similarly, if you propose to provide a service to a person, but this does not occur. Importantly, your SAR obligations apply in relation to any person (i.e. not just a person that is your customer as defined in the Act). For example, it includes a person making payments to your customer through you.

96. The requirement to submit a SAR is based on an objective test. Where an objective observer would conclude that reasonable grounds for suspicion were known to your reporting entity, it is no defence that you did not actually consider the transaction or activity to be suspicious.[79]

97. 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.[80] You should therefore focus time and resource on your suspicious activity reporting procedures, policies and controls to ensure they comply with the Act.

98. While developing the procedures, policies and controls in your AML/CFT programme, it is important to note:

    - You must submit SARs via the FIU's online goAML system.[81]
    - A SAR must be submitted in the prescribed format, contain various details as prescribed by regulations and a statement of the grounds on which the transaction or activity is suspicious.[82]

[78] Section 39A
[79] *Department of Internal Affairs v Ping An Finance (Group) New Zealand Co Ltd* [2017] NZHC 2363 at [64]
[80] Section 41(2)
[81] https://bit.ly/2ygOri3
[82] Section 41

- Urgent SARs can be made orally but you must, as soon as practicable, and within three working days, submit the SAR to the FIU via goAML.
- Non-disclosure provisions prevent you from 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.[83]
- The only circumstance in which you do not have to conduct enhanced CDD when this is triggered is if a person is subject to a Commissioner's order, a production order, or a chief executive of Customs order.[84] Note that neither the Act nor regulations contain any wider 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).
- Conducting enhanced CDD in high-risk circumstances, when conducted properly and in good faith, does 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.

99. In the same way that you are not permitted to disclose information relating to a SAR, your submission of a SAR is afforded the same level of confidentiality and security. Your customer (or any other person reported in your SAR) cannot be told of the existence of the SAR by the Police or any other law enforcement or security agency. Furthermore, this information can only be disclosed in judicial proceedings in limited circumstances where a Judge (or person presiding) is satisfied that the disclosure is necessary in the interests of justice.[85]

Check list:

O. You should ensure you are registered for goAML so you are able to report a SAR when required.

P. You should set out your procedures, policies and controls for examining and conducting enhanced CDD for higher risk transactions, activities or other situations to determine if a SAR is required and your escalation processes.

Q. You should detail who is responsible for authorising and submitting the SAR, how you meet the reporting timeframe and what procedures are in place in the event the usual decision maker(s) is not available.

R. You should set out how you comply with the non-disclosure provisions, ensuring that only officers and employees that need to know about the existence of a SAR as part of their AML/CFT duties are able to access this information.

[83] Section 46. Other than to the FIU, your supervisor; or to be able to meet your AML/CFT obligations, to an officer or employee of your business, to a member of your designated business group or to your lawyer.

[84] Reg.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.

[85] Section 46 to 47

Law firms with legally privileged information

100. Law firms are explicitly excluded from reporting legally privileged information. Legally privileged information is a confidential communication made or brought into existence for the purpose of obtaining or giving legal advice or assistance; or a communication subject to the general law governing legal privilege or that is specified in sections 53-57 of the Evidence Act 2006.[86]

101. It is important to understand that legal privilege does not remove the requirement to submit a SAR. Also note that most information that relates to a suspicious activity is unlikely to be legally privileged. Furthermore, when the circumstances that trigger a SAR are met, all relevant non-legally privileged information set out in the regulations must still be submitted. However, care needs to be taken to ensure that privileged communications are not included.[87]

102. **Note**: In some circumstances, information may cease to be legally privileged at a later date. In these situations, you may be required to submit a new SAR. If in any doubt about filing a SAR because legally privileged information may be involved, you should seek specialist advice.

Prescribed transaction reports

103. PTR obligations were established in 2017 and are also an important part of your AML/CFT programme.

104. Unlike SARs, PTRs are a "bulk" information gathering process that apply to certain types of transaction. Submitting a PTR is not a risk-based requirement. PTRs contribute to the intelligence picture across the entire financial system, providing necessary statistics and useful intelligence on the flow of cash and money in and out of New Zealand. PTRs also make certain ML/TF typologies more difficult to hide, and in turn, improve the detection and disruption of organised crime, fraud, and tax evasion.

105. You must submit a PTR for:

- any domestic **cash transaction (LCT) of NZ$10,000 or more**.

  Note: For an operator of a money or value transfer service (also known as a "money remitter") this includes depositing physical cash into a person's bank account to settle an inbound international wire transfer.[88]

[86] For full definition, refer to section 42

[87] You are never required to provide legally privileged information to your supervisor, another government agency or your auditor.

[88] Reg.9 of the AML/CFT (Prescribed Transactions Reporting) Regulations 2016. The DIA has published guidance for money remitters (https://bit.ly/4bMwlTv)

- an **international wire transfer (IFT) of NZ$1,000 or more**[89] when you are an ordering or beneficiary institution of the wire transfer.

  Note (1): For an operator of a money or value transfer service, an IFT-PTR is also required if you are an intermediary institution of an international wire transfer (of NZ$1,000 or more).[90]

  Note (2): DNFBPs are exempt from the wire transfer provisions. However a DNFBP that makes or receives an international wire transfer of NZ$1,000 or more on behalf of a customer from or into its trust account held with another reporting entity must submit an IFT-PTR.[91]

106. A PTR must be submitted as soon as practicable, but no later than ten working days after the transaction. A PTR must also be submitted using the goAML system, in the prescribed format and contain various details as prescribed by regulations.

107. You should ensure that your procedures, policies and controls enable you to comply with the Act and the PTR regulations, as well as being appropriate to the reporting solution you utilise - whether manual or automated. The FIU has produced a range of guidance material relating to PTR reporting on its website, which will assist you.[92]

108. Note that the same confidentiality and non-disclosure provisions relating to SARs also apply to PTRs (refer paragraph [98] to [99] above).

Annual report

109. You must submit an annual report to your AML/CFT supervisor on your risk assessment and AML/CFT programme[93]. Refer to the *AML/CFT Annual Report Guideline.*

[89] Or equivalent in foreign currency.

[90] Reg.6A of the AML/CFT (Exemptions) Regulations 2011. Refer DIA guidance: https://bit.ly/4bMwlTv

[91] Reg.8 of the AML/CFT (Prescribed Transaction Reporting) Regulations 2016, Reg.15A of the AML/CFT Definitions Regulations 2011. The DIA has published guidance for DNFBPs (https://bit.ly/4aT2VCf)

[92] http://bit.ly/2zkB9RJ

[93] Section 60

Part 5: Record keeping requirements

110. Keeping detailed and accurate records maximises the ability of law enforcement and other agencies to reconstruct transactions and activities and undertake financial investigations and prosecutions (in the event this is required).

111. Maintaining detailed and accurate records is also important for you to be able to effectively implement your AML/CFT obligations, particularly your ongoing CDD and account monitoring requirements (as set out in Part 3 above). Furthermore, it enables you to demonstrate your compliance with your AML/CFT obligations to your supervisor, and the reasons for the decisions you have made.

112. You must retain these records for the following timeframes:

Type of records:	Timeframe:
Identity and verification records – Records reasonably necessary to enable the nature of the evidence used for the purposes of CDD to be readily identified at any time. This should be a copy of the evidence used to verify the person's identity.[94]	At least 5 years from the end of the business relationship (or the completion of the occasional transaction or activity).
Other records relating to business relationship – Records relevant to the establishment of the business relationship, and any other records reasonably necessary to establish the nature and purpose of the business relationship, and activities relating to it. For example, this may include account files, business correspondence and written findings.[95]	At least 5 years from the end of the business relationship.
Transaction records – Records reasonably necessary to enable the transaction to be readily reconstructed at any time, including nature, amount, date and parties to the transaction.[96]	At least 5 years from the completion of the transaction (unless FIU or your supervisor specifies longer).
Suspicious activity reports[97]	At least 5 years after the report is made (unless FIU or your supervisor specifies longer).

[94] Section 50. Note: Only if it is not practicable to retain a copy of the evidence used to verify the person's identity, you are then able to keep any information reasonably necessary to enable the evidence to be obtained.

[95] Section 51(1)(a) and (c). Reg.15N of the AML/CFT (Requirements and Compliance) Regulations 2011.

[96] Section 49

[97] Section 49A

Prescribed transaction reports[98]	At least 5 years after the report is made (unless FIU or your supervisor specifies longer).
Risk assessments, AMLCFT programmes and independent audits[99]	At least 5 years after the date on which they ceased to be used on a regular basis.

113. These records must be kept in a form that is immediately accessible.[100] This enables you to provide them swiftly (in response to a production order or other legal authority) if there is urgent need for them from a law enforcement or other agency.

114. All records must be kept in written form in the English language, or be readily convertible into written form in the English language.[101]

Examining and keeping written findings

115. There are additional record keeping obligations that apply in relation to certain potentially higher risk circumstances.

116. You must examine and keep written findings in relation to the following types of transactions, activities and/or business relationships:

- complex or unusually large transactions.
- unusual patterns of transactions that have no apparent economic or visible lawful purpose.
- any other activity that the reporting entity regards as being particularly likely by its nature to be related to ML/TF.[102]
- business relationships and transactions from or in countries that do not have or have insufficient AML/CFT systems in place.[103]

Supervisors' view:

Examining these types of transactions, activities and business relationships and keeping records of your findings is a key part of a risk-based approach. It ensures:

[98] Regulation 15N of the AML/CFT (Requirements and Compliance) Regulations 2011. The supervisors' view is that records of PTRs should be retained for five years from the date of the report (to align with SAR record keeping requirements).

[99] Section 51

[100] Section 52. Department of Internal Affairs v OTT Trading Group Ltd [2020] NZHC 1663 at [77]

[101] Section 52

[102] Section 57(1)(g)

[103] Section 57(1)(h). There is also a requirement to have additional measures for dealing with or restricting dealings with such countries.

- You are taking steps to understand your customer's activities and determine whether the risk is low, medium or high. This can be reviewed in the event a similar situation arises again in relation to that customer.
- Decisions you make (for example whether to update standard CDD, conduct enhanced CDD, submit a SAR and/or terminate a business relationship), and who makes those decisions, are clear, logical and justifiable.
- You are able to demonstrate appropriate handling of higher risk/suspicious activities to your supervisor and/or the Police or other agency.

Privacy Act 2020

117. In addition to the record keeping requirements under the Act, you also have obligations under the Privacy Act 2020 (Privacy Act).

118. The Privacy Act governs how you collect, store, use and share your customer and other individuals' personal information. It adopts 13 Privacy Principles that should be adhered to. One of these principles (Principle 5) relates to the **Storage and Security of Information**. It states there must be safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information. This principle should be applied to the records you keep (refer paragraph [112] above) as part of your AML/CFT obligations.

119. Note that if the provisions of the two Acts do not fully align, AML/CFT requirements prevail over the requirements of the Privacy Act.[104] In particular, Principle 9 relates to the **Retention of personal information**. It states that an organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used. Your AML/CFT record keeping requirements and timeframes therefore override any case that could be made for disposing of documents, data or information earlier.

120. Further information regarding the Privacy Act is available from the **Office of the Privacy Commissioner**.

Other data security considerations

121. For reporting entities that handle credit cards, it is important to also be aware of the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data. For more information, please refer to the PCI DSS standards.

[104] Section 24 of the Privacy Act

Destruction of records

122. Once the required timeframe under the Act has expired for keeping a record, you are required to take all practicable steps to ensure that the record is destroyed. However, this does not apply where there is a lawful reason for retaining that record. This includes if retention of the record is necessary to comply with the requirements of any other Act, to enable you to carry on your business, or for the purposes of the detection, investigation, or prosecution of any offence.[105]

Check list:

S. You should review and align your AML/CFT record keeping requirements with your obligations under the Privacy Act. You should ensure that your procedures and policies cover how and where you store records, your retention and destruction schedules.

T. You should ensure that all records related to a particular customer are readily accessible/centrally stored for ease of review as part of ongoing CDD and account monitoring requirements. Notwithstanding, there should be controls relating to access of sensitive or confidential information for each customer, such as for copies of previous SARs or written findings of examinations.

[105] Section 54

Part 6: Relying on third parties and outsourcing

123. You are, subject to certain conditions, able to rely on a third party to conduct CDD or carry out other AML/CFT functions on your behalf. The various types of third party you can rely on are:

- a member of your designated business group (**DBG**).
- another reporting entity (or equivalent entity in another country that is supervised or regulated for AML/CFT purposes).
- your agent.

124. Additionally, some businesses utilise third-party software solutions to assist them to meet the requirements of the Act. This does not constitute "reliance" under the Act because you are controlling your use of the software solution.

125. **In all circumstances, you are responsible (and liable) for ensuring that the CDD or other AML/CFT functions conducted by a member of a DBG, another reporting entity (or equivalent) or an agent on your behalf, or through a third-party software solution, comply with the Act**.[106] Requirements relating to reliance on these third parties are set out in the paragraphs below.

Designated business groups

126. In certain circumstances, reporting entities may form a DBG with another reporting entity or entities (or an equivalent entity regulated for AML/CFT purposes in another country with sufficient AML/CFT systems and measures in place).

127. Members of the DBG can then rely on each other to conduct CDD procedures and share parts of their AML/CFT programme. Requirements that can be shared include record keeping, ongoing CDD and account monitoring, suspicious activity and prescribed transaction reporting. It is also possible to share a risk assessment.[107]

128. An annual AML/CFT report must be submitted by all members of a DBG.[108] However, if you share your risk assessment and AML/CFT programme with another member of a DBG, only one of you needs to respond to Part Two of the annual report (on behalf of all DBG members). The other member(s) can leave this blank. All other parts of the annual report must be completed separately.

Supervisors' view:

If you are part of a DBG, your AML/CFT programme should describe its structure and the division of shared and separate AML/CFT obligations where relevant.

[106] There is one exception if you rely on an approved entity pursuant to s33(3A) of the Act. However, at this time there are no prescribed approved entities or approved class of entities.

[107] Section 32

[108] Unless a member of a DBG is not a reporting entity in New Zealand.

129. There are various conditions and eligibility requirements to be able to form a DBG. DBGs are predominantly used by:

- Reporting entities that are companies or limited partnerships with common ownership, or one owns more than 50% of the other.[109]
- For DNFBPs only, a DBG may also be formed by other associated or connected reporting entities that are in the same sector (for example franchisees and/or their franchisor).[110]

130. Note that a DBG can be declined by your supervisor.[111] For further information regarding DBG eligibility, other types of DBG and the application process, refer to the *Designated Business Group Formation* and *Scope Guidelines.*

Other reporting entities (or equivalent in another country)

131. You may also rely on another reporting entity (or equivalent entity in another country) to conduct CDD procedures for you under the Act.

132. The circumstances in which you may rely on another reporting entity (or equivalent) are broader than the availability of a DBG. The intention is that another reporting entity may introduce business to you on behalf of their customer, and to alleviate compliance burden, you are not required to conduct a full CDD process again. However, there are conditions for you to rely on the other reporting entity in this way:[112]

- the other reporting entity must have a business relationship with the customer concerned:
- the other reporting entity must consent to conducting CDD procedures for you and to providing all relevant information to you:
- the other reporting entity must conduct relevant CDD procedures to at least the standard required by the Act and regulations, and must provide you with all the relevant identity information before you establish the business relationship or conduct the occasional transaction or activity for the customer.

  Note: You are required to **obtain** all information required under the Act (whether as part of standard or enhanced CDD) from the other reporting entity. This will assist you with your wider AML/CFT obligations in relation to this customer. It is not permitted for the other reporting entity to merely provide you assurance that CDD has been conducted.

[109] Paragraph (d)(i) of the definition of designated business group in s5(1). Reg.7A of the AML/CFT (Definitions) Regulations 2011

[110] Paragraphs (d)(vi) – (x) of the definition of designated business group in s5(1). The DIA has issued guidance for DNFBPs related to DBG eligibility (https://bit.ly/4c7P.TBy)

[111] Reg.6 of the AML/CFT (Definitions) Regulations 2011

[112] Section 33

- the other reporting entity must, if you need it and request it, also provide you as soon as practicable, but within five working days, copies of all records that were used to **verify** the standard/enhanced CDD information you earlier obtained.[113]

133. As part of implementing your procedures, policies and controls for relying on another reporting entity, you must also:

- take reasonable steps to satisfy yourself that the other reporting entity has record keeping measures to at least the standard of the Act, and is able to provide the relevant verification information as soon as practicable on request, but within 5 working days.[114]
- if the other reporting entity (or equivalent) is in another country, consider the level of risk associated with relying on an entity in that country. You must also establish the other entity is regulated for AML/CFT purposes and is in a country with sufficient AML/CFT systems and measures in place.[115]

Supervisors' view:

Your procedures, policies and controls for satisfying yourself the other reporting entity meets record keeping requirements can be aligned with your process to obtain their consent to conduct CDD for you. In practice, if they are another reporting entity in New Zealand, you already know they have obligations to meet the record keeping requirements of the Act. Whereas for a reporting entity (or equivalent) in another country, you may need to seek their confirmation of this.

If the other reporting entity (or equivalent) is in another country, your assessment of country risk should be conducted as part of your risk assessment. You can establish they are in a country with sufficient AML/CFT systems or measures in place by checking the country is not on the current FATF grey or black list.

Establishing the entity is regulated for AML/CFT purposes can be obtained either from open-source information or by requesting the entity to provide confirmation.

Agents

134. You may also rely on an agent to undertake AML/CFT procedures, policies and controls for you. This includes conducting CDD and account monitoring.[116]

135. "Agent" is not defined in the Act. Instead, the ordinary "principles of agency" apply. Essentially, your agent is an extension of your business in relation to the transactions

[113] Section 33(2)(c)(ii), Reg.14 of the AML/CFT (Requirements and Compliance) Regulations 2011
[114] Reg.13B of the AML/CFT (Requirements and Compliance) Regulations 2011
[115] Section 33. Also Reg.13C of the AML/CFT (Requirements and Compliance) Regulations 2011
[116] Section 34

and activities it carries out for you. An agent is not generally itself captured as a reporting entity under the Act.[117]

136. When you rely on an agent, the AML/CFT functions the agent carries out for you are part of your AML/CFT programme. You are responsible for setting adequate and effective procedures, policies and controls for these functions.[118]

137. As noted at paragraph [125] above, you are also responsible (and liable) for ensuring that the CDD or other function conducted by the agent for you complies with the Act. Your AML/CFT programme must also set out adequate and effective procedures, policies and controls for vetting and training your agents (refer paragraphs [158] to [163] below), and for maintaining a list of agents acting for you.

Supervisors' view:

Depending on how frequently you update your list of agents, you could maintain the list of your agents as part of your AML/CFT programme, as an annex to it, or as a separate document entirely.

138. There are typically two types of agents:

- Networks of agents
- Specialist AML/CFT third-party providers

Network of agents

139. A reporting entity may have a distributed delivery model for its products or services that involves a network of one or more agents.

140. Typically, the agent(s) is a non-financial and/or non-DNFBP business that has entered a commercial arrangement with the reporting entity to be a point of sale (for its product and service).

141. A common example is in the remittance sector where a money remitter may have multiple agents, including a master agent and/or sub-agents (such as dairies or other retailers) contracted to onboard customers and receive funds from them. Other examples include car dealerships and other retailers that act as an agent for non-bank non-deposit taking lenders (such as for car finance or lending on household appliances etc).

[117] There is an exception in the money remittance sector. A business may itself provide a financial service such as currency exchange, but concurrently act as remittance agent for a money remitter. In these situations, the business is not itself captured as a reporting entity in relation to being an agent of the money remitter.

[118] Reg.15G of the AML/CFT (Requirements and Compliance) Regulations 2011

Specialist AML/CFT third-party providers

142. An increasing number of DIA and FMA supervised reporting entities are outsourcing their CDD and accompanying record keeping obligations to specialist AML/CFT providers.

143. These providers offer services to assist reporting entities to comply with the Act.[119] Typically, this occurs as part of a reporting entity's on-boarding procedures for its new customers, particularly customers that are legal persons or legal arrangements.

144. Services provided by the third-party provider may include looking through ownership structures to identify beneficial owners and persons acting on behalf of the customer. The provider then engages with these persons to verify their biographical information (from underlying electronic sources). Other services include obtaining information and undertaking verification of the source of funds or wealth of a customer. At completion, the third-party provider presents the reporting entity with a report detailing its findings.

Supervisors' view:

While AML/CFT third-party providers can provide a useful service, the supervisors are aware some reporting entities take a view that the provider "just takes care of it all" and that all CDD requirements are then met. This is not the case.

As noted at paragraph [125] above, you remain responsible (and liable) for ensuring that the CDD and accompanying record keeping by the third-party provider on your behalf complies with the Act. You should also understand that:

- The CDD you outsource does not exist in isolation from your wider CDD and AML/CFT obligations. This includes the requirement you obtain information on the nature and purpose of a proposed business relationship, and sufficient information to determine if enhanced CDD is required. Furthermore, your standard CDD (conducted by the provider for you) may itself trigger enhanced CDD (refer paragraph [57] above). Conversely, the extent of the CDD that your provider must conduct for you could be reduced for a lower risk customer.
- As part of your ongoing CDD and account monitoring obligations, you must review and may need to update the CDD information you hold for a customer, including that undertaken by the third-party provider (refer paragraph [77] to [82] above).
- Your record keeping obligations require you to retain records of the data, documents or information used for the purpose of identity verification, including when you use a third-party provider. These records must be in a form that is readily accessible (refer paragraphs [110] to [114] above). This obligation

[119] The banking standard 11 (BS11) sets out specific requirements for large banks (defined as New Zealand registered banks whose net liabilities exceed NZD$10 billion) looking to outsource. If your reporting entity is captured by BS11, it is important that you consider these requirements as part of your AML/CFT programme.

continues even if you cease the outsourcing relationship with a particular provider.

Using third-party software solutions

145. Some reporting entities employ third-party software solutions to assist to comply with the requirements of the Act. This may include AML/CFT compliance management software, including as an intermediary for electronic identity verification (from underlying electronic sources), account monitoring, prescribed transaction and suspicious activity reporting, and/or record keeping.

146. Using third party software to assist you to comply with the requirements of the Act differs from relying on an agent. This is because you are the user of the software, conducting CDD or meeting AML/CFT obligations through it, and have control over its functionality. Notwithstanding, you should ensure that your use of any third-party software solution, and its function(s) as part of your AML/CFT programme, is fully detailed in your AML/CFT programme.

Check list:

U. You must ensure that your use of a third party to assist in delivering your AML/CFT programme (whether reliance within a DBG, on another reporting entity or an agent, or your use of a third-party software solution), is fully documented in your AML/CFT programme. This includes steps taken to mitigate any risks associated with your use of the third party (as identified in your risk assessment).

V. You must comprehensively set out all procedures, policies and controls for the CDD or other function(s) carried out by the third party, including how you use any third-party software solution. If the third-party software is used as an electronic identity verification intermediary (from an underlying electronic source(s)), ensure you know and have detailed the reliable and independent sources used.

Part 7: Implementing your AML/CFT programme

147. Once you have established your AML/CFT programme (as set out in Parts 1 to 6 above), you must implement it.[120]

148. Effective implementation of your AML/CFT programme and monitoring and managing compliance with its procedures, policies and controls will enable you to effectively manage and mitigate your ML/TF risks.

149. A strong governance structure is the foundation of the effective implementation of your AML/CFT programme. Your compliance officer, and your wider AML/CFT compliance team, is pivotal to this. This must be supported by appropriate vetting and training of staff (and any agents) involved in delivering your AML/CFT compliance.

150. As with other requirements of the Act, the extent of the steps that you must take across these requirements are dependent on, and should be directed at, your ML/TF risks.

Compliance officer

151. You must designate an employee as a compliance officer. Your compliance officer is responsible for administering and maintaining your AML/CFT programme[121].

152. Your compliance officer must also report to a "senior manager".[122] Within your business you can have one employee who is both the compliance officer and a senior manager. A senior manager is a company director or anyone in your business in a position to influence the management or administration of the business. Your AML/CFT programme should set out which positions in your organisation are "senior managers". Also note:

    - If your reporting entity is a partnership, you may designate one of the partners as the compliance officer, irrespective of whether the partnership has employees. The partner must report to another designated partner in relation to AML/CFT matters.
    - Only if your reporting entity does not have employees are you able to appoint an external person as compliance officer[123].

153. Depending on the size of your reporting entity, the compliance officer can carry out other duties not related to AML/CFT compliance. It does not have to be a stand-alone position. However, for larger reporting entities, a dedicated compliance officer and in some circumstances, a wider compliance team, will be required.

[120] Section 56(1)
[121] Section 56(2)
[122] Within the meaning in s5(1). Section 56(4)
[123] Section 56(3)

Check list:

W. You should clearly outline the responsibilities of the compliance officer (including delegated functions to other persons or teams with AML/CFT compliance responsibilities) and their reporting line in your AML/CFT programme.

Supervisors' view:

You should ensure that you notify your AML/CFT supervisor of any changes to your compliance officer and provide their updated contact details. This will ensure you remain connected to your supervisor and are able to receive any correspondence, updated guidelines or other advice to reporting entities.

Monitoring and managing compliance with your AML/CFT programme

154. You **must** have adequate and effective procedures, policies and controls for monitoring and managing compliance with all other requirements of an AML/CFT programme.[124] Effective oversight and monitoring of your procedures, policies and controls provides assurance you are complying with your AML/CFT requirements (as described in Parts 2 to 6 above).

155. As with other requirements of the Act, the extent of your assurance processes for monitoring and managing your compliance will be dependent on the size of your business, the complexity of it and the nature of your ML/TF risks. A particularly important consideration is the extent to which you utilise technology to assist you to comply with the Act, particularly if you have automated systems for account monitoring.

156. Your compliance officer (and wider compliance team) has an important role and responsibilities. However, it is equally important that you have a strong AML/CFT culture from the top.

Supervisors' view:

To demonstrate a strong AML/CFT culture from the top, directors and senior managers could:

- Engage on and demonstrate a strong commitment to AML/CFT and actively promote its importance throughout the business, including ensuring there is sufficient resourcing (people, technology and financial support) to meet AML/CFT obligations.

[124] Section 57(1)(l). In practice, s57(1)(l) requires monitoring and managing compliance over s57(1)(a-k).

- Ensure they are provided with robust, regular and transparent reporting on AML/CFT matters, including relating to any compliance issues, trends, emerging risks and the effectiveness of the AML/CFT programme.
- Oversee AML/CFT procedures, policies and controls ensuring that they align with the business's overall strategy and risk appetite.

157. Your procedures, policies and controls for monitoring and managing compliance with your AML/CFT programme are not limited to CDD. You should have processes in place to ensure that all employees and systems adhere to all aspects of your AML/CFT requirements. This includes the Act's prohibitions (in the event CDD cannot be completed), account monitoring and record keeping.

Check list:

X. You should conduct regular assurance activity (sampling/testing) of all parts of your AML/CFT programme. This should be risk-based and include, but not be limited to:

- For CDD, you should test if your procedures, policies and controls are being complied with. This should include a range of customer types but greater focus on higher risk customers.
- For account monitoring, you should regularly test any transaction monitoring processes or software to ensure alerts/red flags are being generated in accordance with requirements, and being actioned correctly in the required timeframe.
- For required reporting to the FIU, you should regularly test to confirm that circumstances that require PTRs and SARs to be submitted are identified and that resulting actions and reports meet all regulatory and FIU requirements.

Y. You must ensure any identified deficiencies in AML/CFT procedures, policies and controls are remedied, with reporting to senior management as appropriate and/or changes made to your AML/CFT procedures, policies and controls.

Supervisors' view:

You will not know whether your AML/CFT procedures, policies and controls are functioning properly without testing them. However, the extent of the assurance activity you undertake should depend on the size, complexity and risks associated with your business.

Training

158. A comprehensive AML/CFT training programme ensures your ML/TF risks and AML/CFT requirements are understood across your business. This enables effective

implementation of your AML/CFT programme. It also assists to build a culture of AML/CFT compliance.

159. You must have procedures, policies and controls for training your compliance officer, your senior managers, and any employee or agent engaged in AML/CFT duties. Not every employee needs to be an AML/CFT expert. However, for those that require training, this must be appropriate to their role in delivering your AML/CFT duties.[125]

Supervisors' view:

You may wish to design procedures, policies and controls in your AML/CFT programme that detail:

- the scope and nature of your training, including:
  - on your ML/TF risks (as identified in your risk assessment)
  - your AML/CFT procedures, policies, and controls, including how to identify unusual transactions and activities.
  - trends and techniques of ML/TF.
- which tasks or duties may only be carried out by employees or agents who have had appropriate AML/CFT training.
- how AML/CFT training will be delivered, how often and in what format. For example, in person, online courses, on-the-job training, webinars, refresher training. Is it annually for some key areas (like red flag activity for your business) and less frequently for others?
- the different levels and types of training for different employees or agents, who requires training and what they require training on. Some employees or agents may only require a basic introduction to AML/CFT and others comprehensive training on all parts of your ML/TF risks and AML/CFT procedures, policies, and controls, depending on their role in delivering your AML/CFT duties and the associated ML/TF risks.[126]
- whether and how the effectiveness of the training is assessed to ensure that employees or agents understand and retain the material and can apply it in their roles.
- who will conduct your AML/CFT training. This could be your compliance officer, an in-house expert(s) or a suitably qualified person outside of the organisation.
- how and what records of AML/CFT training will be kept, including completion dates and completion rates.

Like other AML/CFT requirements, the extent of your procedures, policies and controls for training should depend on the size, complexity and risks associated with your business. For a low-risk business with a small number of employees, training

[125] Section 57(1)(b). Also Reg.15G of the AML/CFT (Requirements and Compliance) Regulations 2011

[126] In relation to a third-party AML/CFT specialist provider that is your agent, your focus should be conducting due diligence (rather than training the provider) to ensure their services meet your requirements under the Act.

requirements can be met internally (for example by the compliance officer periodically at a regular team meeting) without the need for bespoke training materials or courses. The compliance officer will need to be suitably trained.

Vetting

160. Your compliance officer, senior managers, employees or agents engaged in AML/CFT duties may pose ML/TF risk. This is particularly so if persons are in positions with control, influence or the ability to bypass or override AML/CFT requirements.

161. You must have procedures, policies and controls for vetting your compliance officer, your senior managers, and any employee or agent engaged in AML/CFT duties.[127] Vetting should be of a high standard and appropriate to the risks involved with the different types of roles.

162. Vetting involves checking someone's background to determine their suitability for the role, making sure they are who they say they are and the information they have provided is correct. Proper vetting helps you avoid hiring a person who later becomes a "rogue" employee that uses your business (or allows an associate(s) to use your business) for ML/TF.

Supervisors' view:

You may wish to design procedures, policies and controls in your AML/CFT programme that detail:

- the scope and nature of your vetting, including:
  - criminal history checks to identify prospective or current employees with a criminal record.
  - employment or character references or other background checks (for example credit checks), including criteria for managing any negative or undesirable responses.
  - checks to identify any employee or agent's secondary or other business interests that may present ML/TF risk.
  - whether vetting requires any other requirements, for example PEP or sanctions screening.
- which tasks or duties may only be carried out by employees or agents who have had certain levels of vetting.
- the different levels and types of vetting for different employees or agents, depending on their role in delivering your AML/CFT duties and the associated ML/TF risks.[128]

[127] Section 57(1)(a). Also Reg.15G of the AML/CFT (Requirements and Compliance) Regulations 2011

[128] In relation to a third-party AML/CFT specialist provider that is your agent, your focus should be conducting due diligence (rather than vetting the provider) to ensure their services meet your requirements under the Act.

- how often vetting is repeated for existing employees or agents and with what frequency for different roles, or when employees change to a different role or an event is triggered (for example adverse information received).
- who will conduct your vetting. This could be conducted in house or by a specialist third party vetting service.

163. You may already have existing policies in place for vetting employees and agents. Alternatively, some employees and agents may already have to meet character requirements as part of professional accreditation or licensing. If so, you are able to leverage these existing requirements as part of your vetting for AML/CFT purposes. You should ensure your AML/CFT programme clearly explains and sets out any additional vetting procedures required in relation to your AML/CFT responsibilities.

Check list:

Z. You should maintain a register of all AML/CFT training and vetting completed for employees and/or agents, including controls and reminders when renewals are due. This will assist you to track and ensure all training and vetting requirements are adhered to.

Part 8: Maintaining your AML/CFT programme

Reviewing your AML/CFT programme

164. Alongside the requirement that you monitor and manage compliance with your AML/CFT programme (as set out above), you are required to:

- ensure your AML/CFT programme is up to date;
- identify any deficiencies in its effectiveness; and
- make any changes that are identified as being necessary in this process.[129]

165. You may want to, and in most circumstances should, review your AML/CFT programme at least annually. This could be scheduled to align with your requirement to submit an annual report to your supervisor (refer paragraph [109] above).

166. However, it is important to understand that you may be required to review and update your AML/CFT programme in other circumstances. This includes:

- **Evolving ML/TF risks** - The ML/TF risks in your business are not static. Money launderers and terrorism financers are continually modifying their techniques. This includes finding new ways to avoid AML/CFT controls that reporting entities have in place.

  Staying informed and understanding the evolving ML/TF risk landscape is a key part of ensuring your AML/CFT programme is effective. Particularly, you should review and respond to any guidance material provided by the FIU (or your supervisor) regarding your sector's ML/TF risks. You should then update your risk assessment and AML/CFT programme as required.
- **Material change** - In the same way there can be a material change in a business relationship with a customer, there can also be a material change in your business.

  Examples include new corporate or organisational structures, new products or services, the ways that you deliver them, or new types of customer or countries dealt with. A material change in your business should prompt a review of your risk assessment and AML/CFT programme, with changes made as necessary to ensure it remains effective.
- **New or developing technologies** – There are particular ML/TF risks associated with new or developing technologies, or products, that might favour anonymity. If you provide products or services involving new or developing technologies that might favour anonymity, or have delivery mechanisms that involve them, you need to review (and update as required) your AML/CFT programme regularly. There is also a specific requirement to update your risk assessment (and programme if required) prior to using the new or developing technology.[130]

[129] Section 59(1)

[130] Section 57(1)(i). Also Reg. 13E of the AML/CFT (Requirements and Compliance) Regulations 2011

- **Monitoring and managing your compliance** – As set out at paragraphs [154] to [157], you are required to monitor and manage compliance with your AML/CFT programme. The procedures, policies and controls for this may identify AML/CFT deficiencies that require changes or updates to your AML/CFT programme.
- **Independent audit** – Similarly your independent audit (refer below) may identify AML/CFT compliance concerns and/or recommendations to improve your compliance. Again, this may require changes or updates to be made to your AML/CFT programme.

Independent audit

167. You **must** ensure an independent audit of your AML/CFT programme (as well as your risk assessment) is conducted every three years, unless you are notified by your AML/CFT supervisor that a four-year timeframe applies. An independent audit may be required at any other time at the request of your AML/CFT supervisor. You **must** provide a copy of your audit to your AML/CFT supervisor on request[131]:
    - **The auditor must be appropriately qualified** – The Act states that your auditor must be appropriately qualified to conduct the audit. This does not necessarily mean that the person must be a chartered accountant or qualified to undertake financial audits. It does mean that the person has to have relevant skills or experience to conduct an AML/CFT audit. You should be able to explain to your AML/CFT supervisor how you determined that your auditor is appropriately qualified[132].
    - **The audit must be conducted by an independent person** – The Act states that your auditor **must** be independent, and not involved in the development of your risk assessment or the establishment, implementation, or maintenance of your AML/CFT programme. The person/s appointed to undertake the audit may be an employee(s) (for instance, an internal audit team), provided they are adequately independent from the AML/CFT area of your business. You should be able to explain to your AML/CFT supervisor how you determined that your auditor is independent[133].

168. You may choose to appoint an external firm to perform the audit provided you are satisfied the auditor is independent, appropriately qualified and no conflict of interest exists with the auditor.

169. Refer to the *Guideline for Audits of Risk Assessments and AML/CFT Programmes* for further information.

[131] Section 59(2), 59B(5), Reg. 13 of the AML/CFT (Requirements and Compliance) Regulations 2011
[132] Section 59B(1) and (2)
[133] Section 59B(1) and (3)

List of abbreviations

The Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
AML/CFT	Anti-money laundering and countering financing of terrorism
AML/CFT Programme	AML/CFT compliance programme
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDD	Customer due diligence
DIA	Department of Internal Affairs
ECDD	Enhanced customer due diligence
FATF	Financial Action Task Force
FIU	New Zealand Police Financial Intelligence Unit
FMA	Financial Markets Authority
ML	Money laundering
NRA	National Risk Assessment
PEP	Politically exposed person
PTR	Prescribed transaction report
RBA	Risk-based approach
RBNZ	Reserve Bank of New Zealand
Risk assessment	ML/TF risk assessment
SAR	Suspicious activity report
SoF	Source of funds
SoW	Source of wealth
SRA	Sector risk assessment
STR	Suspicious transaction report
PF	Proliferation financing
TF	Terrorism financing

Version history

December 2011	Initial version
May 2018	Updated version following introduction of DNFBP sectors to the Act.
October 2022	Updated Privacy Act 1993 references to Privacy Act 2020 Updated audit timeframe references from two years to three-four years or on request by an entity's supervisor.
October 2024	Comprehensive review following the Ministry of Justice 2022 statutory review of the Act and new regulations that took effect on 31 July 2023 and 1 June 2024. Includes reordered and expanded content across eight sections to provide an overview of the requirements of the Act (that must be included in an AML/CFT programme), outsourcing options for CDD, implementing and maintaining your AML/CFT programme. Also included are check lists and the supervisors' view of interpretation of various requirements.

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 AML/CFT programme requirements under the Act. This guideline does not constitute legal advice.