AML/CFT

Anti-money laundering and countering financing of terrorism

AML/CFT Programme Guideline

Updated October 2022

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

Reserve Bank of New Zealand
Te Pūtea Matua

Te Tari Taiwhenua
Internal Affairs

What is this guideline for?

1. This guideline is designed to help you develop and implement your anti-money laundering and countering financing of terrorism programme (programme) under the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 (the Act).

2. You understand your business better than anyone else. You are best placed to identify and determine the level of risks your business faces from money laundering (ML) and terrorism financing (TF), and to develop appropriate strategies to manage, reduce and control these risks.

3. Developing your programme is the next step after conducting your ML/TF risk assessment (risk assessment). It involves developing the procedures, policies, and controls to manage the inherent risks you identified and assessed that your business reasonably expects to face from ML/TF. Your programme **must** be based on your risk assessment.

4. You should keep in mind that an effective AML/CFT regime is risk-based. Your programme must manage and mitigate the ML/TF risks faced by your business. For instance, if you are a low-risk business you may only need a simple programme that is proportionate to your low risk.

5. Following this guideline is not mandatory. However, you must undertake a risk assessment and must establish a programme.

6. Your risk assessment and programme should reflect a risk-based approach that allows you some flexibility in the steps you take when meeting your AML/CFT obligations. A risk-based approach does not stop you from engaging in transactions/activities or establishing business relationships with higher-risk customers. Rather, it should help you to effectively manage and prioritise your response to ML/TF risks. The examples in this guideline are suggestions to help you meet your obligations under the Act. They are not exhaustive and are illustrative in nature.

7. This guideline is for information purposes only. It cannot be relied on as evidence of complying with the requirements of the Act. It does not constitute legal advice from any of the AML/CFT supervisors and cannot be relied upon as such. After reading this guideline, if you still do not understand any of your obligations you should contact your AML/CFT supervisor or seek independent professional advice.

8. You can access the AML/CFT guidance referenced in this guideline 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

9. The Act does not define the terms set out below. For the purposes of this guideline the following definitions apply.
   - **Material change –** ML/TF risk is not static and can change quickly. A material change is an event, activity, or situation that you identify that could change the level of ML/TF risk you may encounter.
   - **Risk-based approach** refers to the proportionate AML/CFT measures that you implement in response to identified risks. An effective risk-based approach (sometimes called RBA) allows you to exercise informed judgement when meeting your AML/CFT obligations. Under a risk-based approach, there is no such thing as "zero risk".
   - **Inherent risk** is the assessed ML/TF risk before any AML/CFT controls and measures are in place.
   - **Residual risk** is the assessed ML/TF risk after AML/CFT controls and measures have been put in place.

10. 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.

Structure of this guideline

Part 1: Introduction

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009

11. The purposes of the Act are to:
    - detect and deter ML and TF
    - 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)
    - contribute to public confidence in the financial system.

What you have to do

12. The first things you should do as part of your obligations under the Act are:
    - appoint an AML/CFT compliance officer (compliance officer)
    - conduct a risk assessment to identify and determine the ML/TF risks you may encounter in the course of your business
    - develop and implement a programme containing the procedures, policies, and controls used to manage and mitigate those risks.

Your programme is based on your risk assessment

13. You **must** base your programme on your risk assessment. The risk assessment is the foundation document of your entire AML/CFT programme. Your programme must clearly show the link between identified risk and the procedures, policies and controls relating to that risk.

14. Your programme should be proportionate to the risks identified in your business. Your AML/CFT supervisor expects that you will have a clear understanding of how you will manage the risks and vulnerabilities you face during the course of business. Large businesses with complex risks will require more detailed and comprehensive programmes than smaller businesses or sole practitioners with simple risks.

Using AML/CFT guidance

15. You **must** consider any applicable guidance material produced by your AML/CFT supervisor or the New Zealand Financial Intelligence Unit (FIU) and any other factors in regulations. We strongly recommend that you are familiar with the following documents before you develop your programme.
    - The National Risk Assessment (NRA) and FIU guidance material (accessible only to reporting entities registered with the FIU's goAML system)[1]
    - Sector risk assessments (SRAs) produced by the AML/CFT supervisors[2]

[1] http://bit.ly/2zpmWPJ
[2] http://bit.ly/2HPNEou

- Industry-specific guidance – for example, DIA has produced the *Lawyers and Conveyancers Guideline*[3]
- AML/CFT supervisor guidance – for example, the FMA has produced the *AML/CFT Guide for Small Financial Adviser Businesses*[4] and DIA has produced *Risk Assessment and Programme: Prompts and Notes for DIA Reporting Entities*[5]

Designated business group

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

Legal obligations relating to your programme

17. As a reporting entity[6] you have a number of obligations under the Act in relation to your programme (see Part 3 of this guideline for more information):
    - Your programme **must** address the risk of ML/TF you may face during your business.
    - Your programme **must** contain the AML/CFT procedures, policies and controls you will use in relation to relevant obligations under the Act. This includes managing the ML/TF risk presented by your customer, the products, and services you offer and the countries you deal with.
    - Your programme procedures, policies and controls must be both adequate and effective.
    - Your programme **must** be in writing and should include a description of how you will keep it up to date.
    - Your programme must be based on your risk assessment (refer to the Risk Assessment Guideline[7] for further information).
    - You **must** review your programme to ensure it is up to date, identify any deficiencies, and make any changes identified as necessary.[8]
    - Your 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, It may also be required at any other time at the request of your AML/CFT supervisor.
    - You **must** also prepare and submit an annual report to your AML/CFT supervisor. This **must** be in the prescribed form and **must** be provided at a time appointed by the supervisor. Refer to the User Guide: *Annual AML/CFT Report 2016* for further information.

[3] http://bit.ly/2GP2Bbi

[4] https://bit.ly/3T6RMVT

[5] https://bit.ly/3fOQHU2

[6] Except for high-value dealers, who only need to comply with parts of the Act from 1 August 2019. While high-value dealers are not required to maintain a written programme, they should consider industry-specific guidance for their sector (to be published at a later date).

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

[8] The use of version control of your document can help demonstrate that you are keeping your programme current.

18. You do not have to follow the processes contained in this guideline to develop and implement your programme. As long as you comply with your obligations under the Act and any other applicable laws or regulations, you can choose a programme that best suits your business. For example, large financial institutions may have their own systems and methodology for implementing a risk management programme. However, you should be prepared to explain and demonstrate to your AML/CFT supervisor the adequacy and effectiveness of your procedures, policies, and controls.

Background

19. **Financial Action Task Force (FATF) recommendations**[9] - All countries are exposed to illicit international money flows. The global nature of ML/TF is reflected in the work of the FATF based on input from international experts. The FATF 40 Recommendations and 11 Immediate Outcomes represent a global standard of AML/CFT. Compliance with and demonstrated effective use of these standards are an important part of New Zealand's international reputation and ability to combat ML/TF. New Zealand was evaluated on these standards and outcomes in 2020[10].

20. **Domestic and international money laundering threat** - The FIU estimates that NZ$1.35 billion in illicit funds is generated annually for laundering. This figure excludes transnational laundering of overseas proceeds of crime and laundering the proceeds of domestic tax evasion. The transactional value of ML and the harm caused by ML and associated offending is likely to be significantly more than this figure.

21. New Zealand faces an unknown scale of ML generated from overseas proceeds of crime. The International Monetary Fund estimates that approximately 2–5% of global GDP (approximately US$2 trillion) is the proceeds of crime.

Terrorism financing

22. Although TF risk is assessed as low in New Zealand, it is prudent to provide guidance on the vulnerabilities and risks associated with the global issue of TF. Please refer to your relevant SRA and the NRA for more information on the financing of terrorism.[11]

Stages of money laundering

23. It is worthwhile covering some of the basics of ML/TF before considering ML/TF risk. ML is generally considered to take place in three phases: placement, layering and integration. TF shares many of the characteristics of ML but may also involve legitimate funds and usually involves smaller amounts.

24. **Placement** occurs when criminals introduce proceeds of crime into the financial system. This can be done by breaking up large amounts of cash into smaller sums

[9] http://www.fatf-gafi.org/
[10] https://bit.ly/3M8VD2c
[11] http://bit.ly/2HPNEou

that are then deposited directly into an account, or by purchasing shares or by loading credit cards. In some offences, such as fraud or tax evasion, placement is likely to occur electronically and may be inherent in the offending.

25. **Layering** occurs once proceeds of crime are in the financial system. Layering involves a series of conversions or movements of funds in order to distance or disguise them from their criminal origin. The funds might be channelled through the purchase and sale of investment instruments or high-value goods or be wired through various accounts across the world. In some instances, the launderer might disguise the transfers as payments for goods or services, giving them an appearance of legitimacy.

26. **Integration** occurs once enough layers have been created to hide the criminal origin of funds. This stage is the ultimate objective of laundering: funds re-enter the legitimate economy, such as in real estate, high-value assets, or business ventures, allowing criminals to use the criminal proceeds of offending.

Predicate offences

27. Predicate offences are the crimes underlying ML/TF activity. It is important that you understand the various types of predicate offences. Please refer to your relevant SRA and the NRA for more information on predicate offending.

Part 2: What is an AML/CFT programme?

28. Your programme sets out the internal procedures, policies, and controls necessary to detect and deter ML/TF and to manage and mitigate the risk of it occurring. For the purposes of this guideline:
    - **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.

29. As part of developing and implementing your programme, you are expected to address your “inherent risks”. These are the ML/TF risks present before you apply controls and mitigations. As a result of your programme and the application of your controls and mitigations, you may wish to assess your “residual” risk (the risk after your controls and mitigations). Your AML/CFT supervisor will expect that your programme contains AML/CFT measures and controls resulting in residual risk. You will need to document and demonstrate how you arrived at your residual risk ratings.

30. For example, if you rated a particular type of customer as “high risk” in your risk assessment, your programme should address this risk rating with adequate and effective procedures, policies, and controls. This could include a policy to conduct enhanced customer due diligence (EDD) on such customers, the procedures for doing so, and the controls necessary to ensure that happens.

31. The Act requires you to designate an employee of your business as a compliance officer. The employee may be based overseas but **must** report to a senior manager of your business and be responsible for administering and maintaining your programme. Alternatively, the compliance officer may be a senior manager themselves. If your business does not have employees, you **must** appoint a suitable person to act as a compliance officer, you are unable to fill the role yourself.

32. 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 programme should set out which positions in your organisation are "senior managers". It could be a company director, trustee of a trust, partner in the business or other senior managers such as the chief executive or the chief financial officer.

33. The compliance officer can carry out other duties not related to AML/CFT compliance. It does not have to be a stand-alone position. Within your business you can have one employee who is both the compliance officer and a senior manager.

34. The size and complexity of your business plays an important role in how attractive or susceptible it may be to ML/TF. For example, a large business may be less likely to know its customers personally, so could offer more anonymity than a small business. Likewise, a business that conducts complex international transactions could offer greater opportunities to money launderers than a domestic only business. Your programme will need to reflect the complexities of your business and the resources allocated to manage ML/TF risk, especially if your business is a large and/or transnational organisation.

35. When developing your programme, along with domestic guidance, it may be useful to consider guidance material produced by the FATF, the Asia Pacific Group on Money Laundering (APG)[12] and other overseas AML/CFT agencies such as the Australian Transaction Reports and Analysis Centre (AUSTRAC).[13]

Part 3: Minimum requirements of a programme

36. When evaluating your programme (and risk assessment), supervisors and auditors will want to explore both **adequacy** and **effectiveness**. Adequacy is described as how compliant your programme is with the various obligations of the Act. Effectiveness is described as how well the practical application of the programme meets the obligations of the Act. This will be something you discuss with your supervisor and auditor.

[12] http://www.apgml.org/
[13] http://www.austrac.gov.au/

Vetting

37. Your programme **must** set out your procedures, policies, and controls for vetting senior managers, your compliance officer and any other employees who have AML/CFT duties.

Like compliance officers, senior managers are in positions where they may be able to influence or override decisions, such as taking on new businesses that may pose ML/TF risk. Employees can also be sources of ML/TF risk.

38. Vetting should be of a high standard and appropriate to the risks involved with the different types of roles. You may want to consider vetting staff at a higher level and/or on an ongoing basis depending on the risk profile of their role.

39. 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 may use your business (or allow their associates to use your business) for ML/TF.

40. When you design your procedures, policies, and controls for vetting employees, including vetting by third parties, you should consider the risks identified in your risk assessment and relate these risks to the roles performed by the employees. For example, you may wish to design procedures, policies and controls that require:
    - checks to identify any criminal convictions prospective or current employees may have
    - checks to identify politically exposed person (PEP) status or sanctions status (if relevant)
    - character references or any other background checks, including criteria for managing any negative or undesirable information
    - different levels of vetting for different staff, depending on the level of AML/CFT risk your business faces from people in those roles
    - checks to identify any employee's secondary business interests that may present ML/TF risk
    - people who conduct background checks on prospective or current staff should have the appropriate skills and experience to do so.

41. You should also consider completing appropriate vetting checks on existing employees, including those who transfer into a higher-risk role or those who have been in a high-risk role for an extended period. Depending on the risk involved and the role, you may also want to carry out credit or financial checks.

42. If you already have comprehensive and effective policies in place for staff vetting, you could include them in this section of your programme if they are suitable for AML/CFT purposes. Note that your vetting procedures, policies, and controls will be subject to audit as part of the wider three-yearly programme audit.

Training

43. Your programme **must** set out your procedures, policies, and controls for training on AML/CFT matters for senior managers, your compliance officer and any other employees with roles involving AML/CFT duties. The main purpose for providing AML/CFT training is to ensure that relevant employees are aware of the risks of ML/TF faced by your business, and how they should respond when they encounter those risks.

44. Your AML/CFT programme should document the following:
    - the scope and nature of the training including:
        - training on relevant AML/CFT legislation
        - your AML/CFT procedures, policies, and controls
        - your ML/TF risks (as set out in your risk assessment)
        - trends and techniques of ML/TF
    - how to identify unusual transactions/activities
    - which tasks or duties may only be carried out by staff who have had appropriate AML/CFT training
    - how you will apply the AML/CFT training including:
        - frequency
        - delivery methods
        - completion dates
        - completion rates
    - how training is tailored for different employees depending on the tasks carried out and the level of AML/CFT risk your business faces from people in their position
    - whether and how employees are assessed for knowledge, application, and retention of the AML/CFT training.

Customer due diligence (CDD)

45. CDD, along with suspicious activity reporting, represents a cornerstone of your AML/CFT regime. You should focus a significant amount of time and attention on this obligation and ensure adequate and effective resourcing. **Your AML/CFT supervisor will closely review your CDD procedures, policies, and controls**. Your programme should meet the CDD requirements of the Act, and the risks identified in your risk assessment.

46. CDD is the process through which you develop an understanding about your customers and the ML/TF risks they pose to your business. CDD involves gathering and verifying information about your customer's identity, beneficial owners, and representatives. Effective CDD, including identifying beneficial ownership, is very important to help protect your business from ML/TF. In the event of reporting on suspicious activity, beneficial ownership is a key piece of information.

47. 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.

48. If your business has adequate and effective procedures, policies, and controls to know who your customer is (and understand their financial activities), it will make it more difficult for money launderers or financers of terrorism to conduct illegal transactions through your business.

49. **Types of CDD** – The Act outlines three types of CDD: standard CDD, simplified CDD and enhanced CDD (EDD). The type of CDD you should conduct depends on the risks presented by your customer and the types of activities and transactions they undertake.

50. Standard CDD is likely to apply to most New Zealand customers. It involves the collection of identity information of the customer, any beneficial owner of the customer, or any person acting on behalf of the customer. It also includes the verification of that information. For beneficial owners or persons acting on behalf of the customer, this verification is according to the level of risk involved.

51. The *Amended Identity Verification Code of Practice*[14] (IVCOP) produced by the AML/CFT supervisors provides a "safe harbour" for the verification of a customer's (who is a natural person) name and date of birth (not address). The IVCOP applies to customers you have assessed as medium to low risk and will help you develop the CDD section of your AML/CFT programme.

52. Simplified CDD can only be conducted on a specified set of organisations including government departments, local authorities, and certain listed companies.[15] According to the level of risk involved, you **must** verify the identity of the person acting on behalf of these customers, and their authority to do so.

53. EDD **must** be conducted in several specific situations as set out in the Act. In addition, EDD **must** be conducted when you consider (based on your risk assessment) that the level of risk involved is such that EDD should apply. EDD requires the collection and verification of the same information as standard CDD as well as, according to the level of risk involved, the collection and verification of information relating to the source of wealth (SoW) and source of funds (SoF) of the customer. There are further EDD requirements relating to PEPs, wire transfers and new and developing technologies that may favour anonymity. Please refer to the *Enhanced Customer Due Diligence Guideline*[16] for more information on this topic.

[14] https://bit.ly/3EjLLRq

[15] Refer to section 18 of the Act for more information: http://bit.ly/2gS5b3V

[16] https://bit.ly/3CeAZt8

54. Your AML/CFT programme **must** outline how your business will determine when EDD is to be conducted and when simplified CDD may be permitted.

55. The CDD section of your AML/CFT programme should set out:
    - an overview of how your business will address the risks identified in your risk assessment and its approach to conducting CDD
    - how you will identify if there has been a material change in the nature or purpose of a business relationship with customers
    - what customer information/documents you require in order to conduct CDD
    - how you will verify this information
    - how you have incorporated CDD into your account opening process, including the process that will determine when to conduct simplified CDD or EDD
    - how you will carry out EDD for higher-risk customers or transactions, including how you will obtain and verify information related to the SoW/SoF of the customer
    - how you will establish whether a customer or beneficial owner of a customer is a PEP
    - how your senior management will approve establishing or continuing the business relationship with the PEP or other high-risk customer
    - how you will ensure that your staff understand the definition of beneficial owner
    - how your CDD processes will identify your customers' beneficial owners.

56. The list above is not comprehensive. You should consider all the CDD requirements of the Act (and its regulations) and how they relate to your own business and risk assessment.

57. **Ongoing CDD and account monitoring** – Ongoing CDD requires you to review information about the business relationship you have with your customers. Account monitoring involves reviewing account activity and transaction behaviour. You can do this using a manual or electronic system to review the transactions and activities that occur and detect patterns or unusual behaviour. Your account monitoring requirements will be shaped by the factors considered in your risk assessment. For some businesses, a manual system will be sufficient but not so for others. For example, if you process a large number of transactions, or have a large customer base, a manual system may not allow you to adequately or effectively monitor transactions or activity.

58. Your ongoing CDD and account monitoring should allow you to identify any inconsistencies between what you know about your customer and the transactions and activities they conduct. To do this you should consider what you know about the customer's use of your products and services as well as the risk rating for the customer type according to your risk assessment. You should also consider the type of CDD undertaken when the business relationship was established and your

current assessment of the level of risk involved. These factors will help you to identify grounds for suspicious activity reporting.

59. **Importance of nature and purpose** – The nature and purpose of your customer's transactions and activities will directly influence the level of ML/TF risk they present. This is an important consideration in your on-boarding process. Determining the nature and purpose of your business relationship with your customer will help you with account monitoring and ongoing CDD. It will also help you in identifying SoW/SoF and submitting SARs.

60. **CDD conducted on your behalf** – The Act permits you, in certain circumstances, to rely on CDD conducted on your behalf by another person who is:
    - a member of your designated business group
    - your agent
    - a reporting entity (including an approved entity[17]) that consents to do so
    - a person resident in a country with sufficient AML/CFT systems and measures in place who is supervised or regulated for AML/CFT purposes and consents to do so.

61. The Act requires your programme to have procedures, policies, and controls for circumstances under which you rely on CDD conducted by other parties. For example, in your programme you could set out how a person resident in another country will conduct CDD on a trust in that country before you enter into a business relationship with the trust.

62. A person or business (that is not your agent) that you rely on **must** have a business relationship with the customer concerned. They **must** have conducted CDD to at least the standard required by the Act and provide you with relevant identity information before you establish a business relationship, or an occasional transaction or activity is conducted. They **must** also provide relevant verification information to you on request and within five working days.

63. The Act requires that personal information supplied by any member of a designated business group to another member of that group **must** be subject to certain privacy protections under the Privacy Act 2020.

64. You are responsible for the adequacy of the CDD conducted on your behalf.[18] This means you should communicate your procedures, policies, and controls and CDD requirements clearly to the third party undertaking CDD for you. You should also check whether the third party is carrying out CDD to the required standard.

65. **CDD and prohibitions** – Among other matters, you **must not** establish or continue a business relationship with a customer if you are unable to conduct CDD

[17] Section 33 of the Act enables a business to rely on a reporting entity that is an "approved entity" or is within a class of "approved entities". Currently there are no prescribed approved entities or class of approved entities

[18] There is an exception when using an approved entity – see section 33(3A) of the Act (https://bit.ly/2nQNm8F).

in accordance with the Act. Your programme should cover these prohibitions. You **must** consider submitting an SAR if you are unable to conduct CDD. Other prohibitions apply to customer anonymity and shell banks.

Written findings

66. Your programme **must** contain procedures, policies, and controls to examine and keep written findings on any activity that is likely to be related to ML/TF. You must also examine and keep written findings on any complex or unusually large transactions and unusual patterns of transactions with no obvious economic or lawful purpose.

67. Your procedures, policies and controls must also set out how you will monitor, examine, and keep written findings relating to business relationships and transactions/activities with countries that do not have or have insufficient AML/CFT systems in place. Your programme must include additional measures that restrict any dealings with these countries. For example, you may require senior management approval for transactions to or from these countries.

Suspicious activity reports (SARs)

68. Submitting SARs is an important aspect of your AML/CFT programme. You should focus a significant amount of time and attention on this topic and ensure adequate and effective resourcing. **Your AML/CFT supervisor will closely review your SAR procedures, policies, and controls.**

69. Your programme should meet the SAR requirements of the Act and the risks identified in your risk assessment.

70. You will need to consider the following:
    - You **must** report suspicious activity to the FIU as soon as practicable, but no later than three working days after forming your suspicion.
    - Forming suspicion **must** be based on information that would **objectively** justify that suspicion.[19]
    - You **must** submit SARs when you become aware of this information or by reasonable diligence would have become aware of it.
    - Urgent SARs can be made orally but you **must**, as soon as practicable, and within three working days, forward the SAR to the FIU.
    - You **must** submit SARs via the FIU's online goAML system.[20]

71. Your programme **must** set out adequate and effective procedures, policies, and controls for reporting suspicious activities to the FIU. This may include:
    - how your staff will determine if there are grounds for forwarding SARs
    - how you will complete, authorise, and forward SARs to the FIU
    - which roles within your business have responsibility for authorising and forwarding SARs to the FIU

[19] *DIA v Ping An Finance (Group) New Zealand Limited Company Limited* [2017] NZHC 2363

[20] https://bit.ly/2ygOri3

- how you will meet the three-working-day timeframe for submitting SARs
- how you will ensure there is no "tipping off" in regards to SARs[21]
- how legal privilege, if relevant to you, will operate with SARs.

72. The FIU will issue updated guidelines on SARs later in 2018. Existing FIU guidance on suspicious transaction reports still provides relevant information on this topic.[22]

Prescribed transaction reports (PTRs)

73. Your programme **must** set out adequate and effective procedures, policies and controls for submitting PTRs to the FIU. PTRs cover international wire transfers and domestic physical cash transactions.

74. You **must** submit PTRs for large physical cash transactions of NZ$10,000 and over and international wire transfers of NZ$1,000 and over. PTRs for international wire transfers **must** be submitted by ordering or beneficiary institutions. PTRs **must** be submitted to the FIU (individually or in batches) within 10 working days of the transaction. Your programme documentation will need to explain how you meet these obligations.

75. The FIU has produced a range of guidance material for PTRs on their website.[23]

Record keeping

76. Your programme **must** include adequate and effective procedures, policies, and controls for the record-keeping requirements. You **must** keep your records for a minimum of five years after a transaction, activity or wire transfer has been completed or a business relationship has ended (whichever is later). This includes records:
    - necessary to enable transactions/activities to be readily reconstructed
    - necessary to enable the nature of the evidence for identification and verification to be obtained
    - relevant to the establishment, or nature and purpose, of a business relationship
    - relating to risk assessments, AML/CFT programmes, and audits.

77. Your record-keeping policy and procedures could describe how you manage the retention of your records – for example, how and where you will store your records and whether you have a formal retention and disposal schedule to identify records to be retained or destroyed.

78. If you keep these records under other legislation, you are not required to keep a separate set of records for the purposes of the Act. You may be required to keep

[21] You must not disclose SAR-related information with anyone who is not required to have access to the SAR. You must not inform your customer that you are submitting an SAR about them.

[22] *Suspicious Transaction Guideline 2013*: http://bit.ly/2zxU4Jj

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

certain records for longer periods under different legislation or at the request of your AML/CFT supervisor or the FIU.

79. If you do not keep your records in written form in English, then your programme **must** set out how the records can be easily accessed and readily converted into English.

Products and transactions that favour anonymity

80. The Act requires your programme to set out how you will prevent the use, for ML/TF, of products, services, transactions, and activities that might favour anonymity. Money launderers and financers of terrorism seek new ways to mask their identity or the identity of the recipients of their funds. This makes products, services, transactions, and activities that favour anonymity or enable obscured beneficial ownership particularly attractive for ML/TF.

81. EDD on its own may not be sufficient to prevent ML/TF through products and services that favour anonymity – for example, products that permit online transactions that conceal or disguise beneficial ownership. This is because, without effective account monitoring, it can be difficult to ensure that the account holder does not permit another person to operate the account.

82. If you offer products or services that favour anonymity, your programme **must** have adequate and effective procedures, policies, and controls to detect and deter their use to launder money or finance terrorism. For instance, according to the level of risk involved, you should monitor transactions and activities to detect patterns of behaviour that are inconsistent with your knowledge of your customer, and the nature and purpose of the business relationship.

Managing and mitigating risk

83. The ML/TF risks in your business are not static. Money launderers and financers of terrorism will modify their ML/TF methods to avoid measures you put in place to manage and mitigate ML/TF risks. Your programme **must** include procedures, policies and controls that continue to manage and mitigate ML/TF risks identified in your risk assessment. This also applies to risks associated with any new products and services you may offer and new or emerging ML/TF methods. The following sources provide additional information about current ML/TF methods:
    - The NRA and FIU guidance material[24]
    - SRAs and guidance on the website of your relevant AML/CFT supervisor
    - AML/CFT supervisor newsletters and publications sent to your compliance officer
    - FATF website[25]
    - APG website[26]
    - Trusted media sources

[24] http://bit.ly/2zpmWPJ
[25] http://www.fatf-gafi.org/
[26] http://www.apgml.org/

- Comparable jurisdiction AML/CFT agency websites (e.g., AUSTRAC[27])

84. Without adequate and effective management and mitigation, your AML/CFT measures will fail to adapt to the dynamic ML/TF risks and vulnerabilities and will not detect and deter ML/TF activity as they should.

Ensuring compliance with the AML/CFT programme

85. Your programme must have procedures, policies and controls that set out how your business will monitor and manage compliance with the programme. Effective oversight and monitoring must be in place to ensure continued AML/CFT compliance. For instance, you should have procedures, policies and controls covering:
    - the role of internal and external audits and reviews
    - the role of management information tools
    - how you access and incorporate guidance material in your risk assessment and programme
    - how your compliance officer maintains their AML/CFT awareness (e.g., attending training events and keeping a watching brief on the media)
    - how you will incorporate the findings of supervisory interactions and audits into your AML/CFT regime.

86. You should actively monitor your AML/CFT compliance functions (preferably with senior management involvement). If you identify instances of non-compliance, you should take immediate steps to rectify the situation.

87. You **must** ensure that your branches and subsidiaries that are in a foreign country apply your programme to the extent permitted by the law of that country. If the law of the foreign country does not permit implementation of any part of your entire programme, you **must** inform your AML/CFT supervisor and take additional measures to manage the ML/TF risk.

Part 4: Applying a programme

88. Your programme should detail how you prioritise your risks and provide a framework of how you will manage and mitigate those risks. Your programme should allow for different situations that currently arise in your business or are likely to arise in the near future. For instance, your programme should consider the impact of new products, services, or customer types, as well as forecast and emerging technology.

89. ML/TF risks will often operate together and represent higher risks in combination. For example, you may offer high-risk products to customers in high-risk countries resulting in a very high, compounded ML/TF risk rating. Your programme should reflect how you mitigate this type of compounding risk.

[27] http://www.austrac.gov.au/

90. Your programme **must** enable you to meet your relevant obligations under the Act and its regulations. For instance, your programme should provide sufficient detail for your staff on how and when you determine the SoW/SoF for your customers as part of EDD.

New and developing technologies and products

91. New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. Your programme should consider whether your business is, or may be, exposed to customers involved in new and developing technologies and products. Your programme should then detail the procedures, policies, and controls that you will implement for this type of customer and technology.

Material changes and your programme

92. Your programme should be able to adapt when there is a material change in the nature and purpose of your business. A material change could present an increase, or decrease, in ML/TF risk or reduce the effectiveness of AML/CFT measures.

93. Material change could include circumstances where you introduce new products or services, or have customers based in new jurisdictions. Material change can include when you start using new methods of delivering your services or you have new corporate or organisational structures. It could be if you decide to outsource CDD functions or change your processes for dealing with PEPs. In these circumstances, you may need to refresh your programme, and perhaps your risk assessment.

Definition of risk

94. Risk can be defined in many ways, and there is no one-size-fits-all risk assessment model. Whatever definition of risk and risk rating model you used in your risk assessment should align with your programme.

Part 5: Review and audit of programme

Reviewing a programme

95. The Act requires that you **must** review your programme to:
    - ensure it is current at all times
    - identify any deficiencies in its effectiveness
    - make any changes that are identified as being necessary in this process.

96. You may want to schedule this annually as part of your annual report process and/or as a result of a trigger event. A trigger event could be the emergence of new technology; a new customer base; new services or products; new ML/TF risks as determined by the FATF, AML/CFT supervisors or the FIU; or updated regulations. Version control of documents is useful to demonstrate this.

Auditing a programme

97. You **must** audit your programme (as well as your risk assessment) every three years, unless you are notified by your AML/CFT supervisor that a four-year timeframe applies. It also may be requested 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.

98. **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 the assessment. You should be able to justify to your AML/CFT supervisor how your auditor is appropriately qualified.

99. **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 programme. The person/s appointed to undertake the audit may be a member of your staff (for instance, an internal audit team), provided they are adequately separated from the AML/CFT area of your business. You should be able to justify to your AML/CFT supervisor how your auditor is independent.

100. You may choose to appoint an external firm to undertake both the audit and review provided you are satisfied there are appropriate separation and conflict of interest arrangements. The annual report that you are required to provide to your AML/CFT supervisor **must** consider results and implications of the audit. Refer to the AML/CFT supervisor guidance *Guideline for Audits of Risk Assessments and AML/CFT Programmes*[28] for more information.

[28] http://bit.ly/2u6zb5

Part 6: List of abbreviations

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

Version history

May 2018	Initial version
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