

**AML / CFT**

Anti-money laundering and countering financing of terrorism

# AML/CFT Programme Guideline



FINANCIAL MARKETS AUTHORITY

TE MANA TATAI HOKOHOKO - NEW ZEALAND



RESERVE  
BANK

O F N E W Z E A L A N D

INTERNAL AFFAIRS



Te Tari Taiwhenua

## What is this guideline for?

1. This guideline is designed to help reporting entities develop their AML/CFT programme.
2. If you are a reporting entity as defined in section 5 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ([the AML/CFT Act](#))<sup>1</sup>, your obligations under Part 2 of the AML/CFT Act come into force on 30 June 2013. Section 56 of the AML/CFT Act requires you to establish, implement and maintain a compliance programme (AML/CFT programme).
3. This guideline is provided for information only and cannot be relied on as evidence of complying with the requirements of the AML/CFT Act. It does not constitute legal advice from any of the AML/CFT supervisors and cannot be relied on as such.
4. After reading this guideline, if you still do not understand any of your obligations you should seek legal advice, or contact your AML/CFT supervisor.

## What is an AML/CFT programme?

5. An AML/CFT programme sets out the internal policies, procedures and controls necessary to detect money laundering and financing of terrorism (ML/FT) and to manage and mitigate the risk of it occurring. For the purposes of this guideline:
  - *policies* set out expectations, standards and behaviours in a business;
  - *procedures* are more detailed and set out day-to-day operations; and
  - *controls* are tools that management use to ensure the business complies with policies and procedures.
6. Section 57 of the AML/CFT Act states that a reporting entity's AML/CFT programme must be based on its risk assessment. This means that before starting to develop your AML/CFT programme, your risk assessment must be completed in accordance with section 58 of the AML/CFT Act. A [Risk Assessment Guideline](#)<sup>2</sup> is available from the AML/CFT Supervisors.
7. An AML/CFT programme should take into account the risks your particular business can reasonably be expected to face from ML/FT. Although you have flexibility to develop your AML/CFT programme based on your particular situation and risk assessment, section 57 of the AML/CFT Act requires that the policies, procedures and controls set out in your AML/CFT programme must be adequate and effective. The minimum requirements are discussed in further detail in this guideline.

---

<sup>1</sup>[http://www.legislation.govt.nz/act/public/2009/0035/latest/whole.html?search=ts\\_act\\_anti+money+laundrying\\_rese&p=1#d1m2140720](http://www.legislation.govt.nz/act/public/2009/0035/latest/whole.html?search=ts_act_anti+money+laundrying_rese&p=1#d1m2140720)

<sup>2</sup>[http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT\\_RiskAssessmentGuidelineFINAL\\_14June2011.pdf/\\$file/AMLCFT\\_RiskAssessmentGuidelineFINAL\\_14June2011.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT_RiskAssessmentGuidelineFINAL_14June2011.pdf/$file/AMLCFT_RiskAssessmentGuidelineFINAL_14June2011.pdf)

8. You have a certain amount of discretion to decide how to implement policies, procedures and controls that are suitable for your business. These decisions should be documented in your AML/CFT programme. The effectiveness of the AML/CFT programme may be subject to scrutiny by your AML/CFT supervisor.
9. The policies, procedures and controls you implement must be adequate and effective. They must be sufficiently robust to reasonably address the risks outlined in your risk assessment. For example, if you rated a particular type of customer as “high risk” in your risk assessment, then your AML/CFT programme should reflect this risk rating with adequate and effective policies, procedures and controls. This could include a policy to conduct enhanced due diligence on such customers, the procedures for doing so and the controls necessary to ensure that happens.

## **Who is responsible for the AML/CFT programme?**

10. Section 56 of the AML/CFT Act requires you to designate an employee of your business as an AML/CFT 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 AML/CFT programme. If your business does not have employees, you must appoint a suitable person to act as an AML/CFT compliance officer or fulfil the role yourself.
11. 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 policy should set out which positions in your organisation are considered to be “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.
12. The AML/CFT 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 reporting entity you can have one employee who is both the AML/CFT compliance officer and a senior manager.

## **Minimum requirements for a AML/CFT programme**

### **Vetting**

13. Under section 57(a) of the AML/CFT Act, your AML/CFT programme must set out your policies, procedures and controls for vetting senior managers, your AML/CFT compliance officer and any other employees whose roles involve AML/CFT duties.
14. Like AML/CFT compliance officers, senior managers are in positions where they may be able to influence or override decisions, such as taking on new business that may pose a ML/FT risk. Employees can also be sources of ML/FT risk.
15. Vetting involves checking someone’s background to determine their suitability for the position, making sure they are who they say they are and the information they have provided is correct. In this context, its purpose is to help you avoid hiring a person who may use your business (or allow their associates to use your business) for ML/FT.

16. When you design your policies, procedures and controls for vetting of employees, including vetting by third parties, you must take into account the risks identified in your risk assessment. You should then relate these risks to the roles performed by the employees. For example, you may wish to design policies, procedures and controls that require:
  - checks to identify any criminal convictions prospective or current employees may have. (The process for obtaining a person's criminal record from the Ministry of Justice can be found on the Ministry of Justice's [website](#)<sup>3</sup>);
  - 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 positions; and
  - people who conduct background checks on prospective or current staff to have the appropriate skills and experience to do so.
17. If you already have comprehensive and effective policies in place for staff vetting you could include them in this section of your AML/CFT programme if they are suitable for AML/CFT purposes.

### **Training**

18. Under section 57(b) of the AML/CFT Act, your AML/CFT programme must set out your policies, procedures and controls for training on AML/CFT matters for senior managers, your AML/CFT compliance officer and any other employees with roles involving AML/CFT duties.
19. The main purpose for providing AML/CFT training is to ensure that relevant employees are aware of the risks of ML/FT faced by your business and how they should respond when confronted with such risks.
20. Your AML/CFT programme could document the following:
  - the scope and nature of the training. For example, you could include training on relevant AML/CFT legislation, your AML/CFT policies, procedures and controls, your ML/FT risks (as set out in your risk assessment), trends and techniques of ML/FT, and how to identify unusual behaviour;
  - 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, and delivery methods;
  - how you will track that relevant staff have completed the required training;

---

<sup>3</sup> <http://www.justice.govt.nz/services/get-a-copy-of-your-criminal-record/obtaining-a-copy-of-your-criminal-record>

- 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; and
- whether and how employees are assessed for knowledge, application and retention of the AML/CFT training.

### **Customer due diligence**

21. Sections 10 to 39 of the AML/CFT Act detail your customer due diligence (CDD) obligations. Your AML/CFT programme should therefore be designed to ensure that your CDD policies, procedures and controls, as required under section 57(c), meet those requirements and the risks identified in your risk assessment.
22. CDD is the process through which a reporting entity develops an understanding about its customers and the ML/FT risks they pose to the business. CDD is a cornerstone of an AML/CFT programme. CDD involves gathering and verifying information about a customer's identity, beneficial owners and representatives. Effective CDD is very important to help protect your business from ML/FT.
23. Those seeking to launder money or finance terrorism will generally try to avoid attracting attention, particularly from reporting entities and law enforcement agencies, by attempting to mask:
  - their identity; or
  - the illegal source of their funds (in part or whole), or intent to misuse legally obtained funds; or
  - the identity of the beneficiaries of those funds.
24. If your business has appropriate policies, procedures and controls to ensure that you know who your customer is (and understand their financial activities), it will make it more difficult for money launderers or financiers of terrorism to conduct illegal transactions through your business.

### Three types of CDD

25. There are three types of CDD under the AML/CFT Act depending on your customer, and the type of transactions they conduct. They are standard CDD, simplified CDD and enhanced CDD.
26. 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 this verification is according to the level of risk involved.
27. AML/CFT supervisors have released the [Identity Verification Code of Practice 2011](http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT_IdentityVerificationCodeofPractice2011.pdf/$file/AMLCFT_IdentityVerificationCodeofPractice2011.pdf)<sup>4</sup> for name and date of birth identity verification of customers (who are

<sup>4</sup>[http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT\\_IdentityVerificationCodeofPractice2011.pdf/\\$file/AMLCFT\\_IdentityVerificationCodeofPractice2011.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT_IdentityVerificationCodeofPractice2011.pdf/$file/AMLCFT_IdentityVerificationCodeofPractice2011.pdf)

natural persons) you have assessed as medium to low risk. The code of practice will help you develop this section of your AML/CFT programme.

28. Simplified CDD can be conducted on a specified set of organisations such as Government departments, local authorities, the New Zealand Police and certain listed companies<sup>5</sup>. 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.
29. Enhanced CDD must be conducted in a number of specific situations as set out in section 22 of the AML/CFT Act. In addition enhanced CDD must be conducted when you consider (based on your risk assessment) that the level of risk involved is such that enhanced CDD should apply. Enhanced CDD 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 the funds or wealth of the customer.
30. Under section 57(j) of the AML/CFT Act your AML/CFT programme must outline how your business will determine when enhanced CDD must be conducted and when simplified CDD may be permitted.
31. Your AML/CFT programme could 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 you had before 30 June 2013<sup>6</sup>;
  - what customer information/documents you require 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 or enhanced CDD;
  - how you will carry out enhanced due diligence for higher risk customers or transactions, including how you will obtain information related to the source of funds or wealth of the customer;
  - how you will establish whether a customer or beneficial owner of a customer is a Politically Exposed Person (PEP) as defined under section 5 of the AML/CFT Act. For example, you may use the services of a commercial PEP list provider;
  - how your senior management will approve establishing or continuing the business relationship with the PEP or other high risk customer;

---

<sup>5</sup> Section 18 of the AML/CFT Act and regulation 5 of the Anti-Money Laundering and Countering Financing of Terrorism (Requirements and Compliance) Regulations 2011

<sup>6</sup> Section 14(c) of the AML/CFT Act

- how you will ensure that your staff understand the definition of beneficial owner as set out in section 5 of the AML/CFT Act; and
  - how your CDD processes will identify your customers' beneficial owners.
32. The list above is not comprehensive. You must consider the AML/CFT Act and AML/CFT Regulations, and how they relate to your own business and risk assessment.

#### Ongoing CDD and account monitoring

33. Ongoing CDD requires you to regularly 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 that occur and detect patterns or unusual transactions. Your account monitoring requirements will be determined by the factors considered in your risk assessment. For some reporting entities a manual system will not be adequate. 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 monitor transactions.
34. The ongoing CDD and account monitoring you conduct must allow you to identify any inconsistencies between what you know about your customer and the transactions they undertake. To do this you must 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 AML/CFT risk assessment. You must also consider the type of CDD undertaken when the business relationship was established and your current assessment of the level of risk involved. This will allow you to identify grounds for suspicious transaction reporting.

#### CDD conducted on your behalf

35. The AML/CFT Act permits you, in certain circumstances<sup>7</sup>, to rely on CDD conducted on your behalf by another person who is:
- a member of your designated business group; or
  - your agent; or
  - a reporting entity that consents to do so; or
  - all of the following;
    - resident in a country with sufficient AML/CFT systems and measures in place; and
    - supervised or regulated for AML/CFT purposes; and
    - who consents to do so.
36. A person or reporting entity (that is not your agent or member of your designated business group) that you rely on must have a business relationship with the

---

<sup>7</sup> Sections 32 to 34 of the AML/CFT Act

customer concerned. They must have conducted CDD to at least the standard required by the AML/CFT Act and provided you with relevant identity and verification information.

37. Where CDD is conducted on your behalf by a member of your designated business group, or a person that is not your agent, the relevant verification information must be provided to you as soon as practicable but no later than five working days after the business relationship is established or the occasional transaction is conducted.
38. If your business relies on CDD conducted on your behalf by another person, section 57(k) of the AML/CFT Act requires your AML/CFT programme to set out:
  - policies, procedures and controls for circumstances under which you rely on CDD conducted on your behalf; and
  - procedures that will be followed by the person conducting CDD on your behalf.
39. Your policies, procedures and controls will have to be adequate and effective to detect and deter the AML/CFT risks that your risk assessment has identified. For example, in this section 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.
40. You are responsible for the adequacy of the CDD conducted on your behalf. This means that it is desirable for you to communicate the relevant policies, procedures, controls and CDD requirements clearly to the third party. It is also desirable for you to check periodically whether the third party is carrying out CDD to the required standard.

#### **Written findings**

41. Section 57(g) of the AML/CFT Act requires that your AML/CFT programme contains policies, procedures and controls to examine and keep written findings on any activity that is likely by its nature to be related to ML/FT. 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.
42. Your policies, procedures and controls must also set out, as required by section 57(h) of the AML/CFT Act, how you will monitor, examine, and keep written findings relating to business relationships and transactions with countries that do not have or have insufficient AML/CFT systems in place. Your AML/CFT 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 transaction reporting**

43. Suspicious transaction reporting requirements are detailed in sections 40 to 48 of the AML/CFT Act. Under section 57(d) of the AML/CFT Act your AML/CFT programme should set out adequate and effective policies, procedures and controls for reporting suspicious transactions to the New Zealand Police Financial Intelligence Unit. This may include:

- how staff will determine if there are grounds for forwarding suspicious transaction reports;
  - how to complete, authorise and forward suspicious transaction reports; and
  - which roles have responsibility for authorising and forwarding suspicious transaction reports to the New Zealand Police Financial Intelligence Unit.
44. The New Zealand Police Financial Intelligence Unit will issue guidelines on how to meet the obligation for submitting suspicious transaction reports.

### **Record keeping**

45. Under section 57(e) of the AML/CFT Act your AML/CFT programme must include adequate and effective policies, procedures and controls for the record keeping requirements described in sections 49 to 54 of the AML/CFT Act. Records must be kept for a minimum of five years after a transaction or wire transfer has been completed or a business relationship has ended. This includes records:
- necessary to enable transactions 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; and
  - relating to risk assessments, AML/CFT programmes, and audits.
46. Your record keeping policy and procedures could describe how you manage the retention of your records. For example, how and where your records will be stored and whether there is a formal retention and disposal schedule to readily identify records to be retained or destroyed.
47. If you keep these records under other legislation, you are not required to keep a separate set of records for the purposes of the AML/CFT Act. You may be required to keep certain records for longer periods under different legislation or at the request of your AML/CFT supervisor or the New Zealand Police Financial Intelligence Unit.
48. If you do not keep your records in written form in the English language, for example if records are kept in another language, then your AML/CFT programme will have to set out how the records can be easily accessed and readily converted into English.

### **Products and transactions that favour anonymity**

49. Section 57(i) of the AML/CFT Act requires your AML/CFT programme to set out how you will prevent the use, for ML/FT, of products and transactions that might favour anonymity.
50. Money launderers and financers of terrorism continually seek new ways to mask their identity or the identity of the recipients of their funds. This makes products and transactions that favour anonymity particularly attractive for ML/FT.

51. Enhanced CDD on its own may not be sufficient to prevent ML/FT through products and services that favour anonymity, for example products that permit online transactions. 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.
52. If you offer products or services that favour anonymity, your AML/CFT programme must have adequate and effective policies, procedures and controls to detect and deter the use of such products and services to launder money or finance terrorism. These may allow for monitoring the customer's transactions to detect anomalies in your knowledge of the client's business and the transactions that are being conducted through the account. For example, this may include checking the physical address provided by the client against the location/s from where the client logs on.

### **Managing and mitigating risk**

53. The ML/FT risks in your business are not static. Money launderers and financiers of terrorism will modify their ML/FT methods to avoid detection and overcome measures you put in place to manage and mitigate ML/FT risks. Under section 57(f) of the AML/CFT Act, your AML/CFT programme must include policies, procedures and controls that continue to manage and mitigate ML/FT risks identified in your risk assessment, any new products and services you may offer and new or emerging ML/FT methods. The following sources will provide additional information about current ML/FT methods:

- NZ Police FIU ([National Risk Assessment and Quarterly Typology Report](#))<sup>8</sup>;
- AML/CFT Supervisors ([Sector Risk Assessment](#)<sup>9</sup> and [guidelines](#)<sup>10</sup>);
- [Financial Action Task Force](#)<sup>11</sup>; and
- [The Asia/Pacific Group on Money Laundering \(APG\)](#)<sup>12</sup>.

### **Ensuring compliance with the AML/CFT programme**

54. As required by section 57(l) of the AML/CFT Act, your AML/CFT programme must have policies, procedures and controls that set out how your business will monitor and manage compliance with the AML/CFT programme. Effective oversight and monitoring of the AML/CFT programme must be in place to ensure continued compliance with it.

55. Policies, procedures and controls relevant to managing compliance with the AML/CFT programme should also set out how you will communicate and train staff on aspects of your AML/CFT programme relevant to their roles.

56. You must ensure that your branches and subsidiaries that are in a foreign country apply your AML/CFT programme to the extent permitted by the law of that

<sup>8</sup> <http://www.justice.govt.nz/policy/criminal-justice/aml-cft/risk-assessments>

<sup>9</sup> [http://www.dia.govt.nz/diawebsite.nsf/wpg\\_URL/Services-Anti-Money-Laundering-Sector-and-National-Risk-Assessments?OpenDocument](http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Sector-and-National-Risk-Assessments?OpenDocument)

<sup>10</sup> [http://www.dia.govt.nz/diawebsite.nsf/wpg\\_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines?OpenDocument](http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines?OpenDocument)

<sup>11</sup> [http://www.fatf-gafi.org/pages/0,2987,en\\_32250379\\_32235720\\_1\\_1\\_1\\_1\\_1.00.html](http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1.00.html)

<sup>12</sup> <http://www.apgml.org/>

country. If the law of the foreign country does not permit implementation of any part or your entire AML/CFT programme, you must inform your AML/CFT supervisor and take additional measures to effectively handle the ML/FT risk, as set out in section 61 of the AML/CFT Act.

## **Review and audit of the AML/CFT programme**

### Review of the AML/CFT programme

57. Under section 59(1) of the AML/CFT Act you must review your AML/CFT programme to ensure that it remains current, to identify any deficiencies and make any changes necessary to address them. For example:

- if you find that the AML/CFT training you have outlined in your AML/CFT programme is insufficient you must take steps to address this; or
- if your risk assessment changes, you must consider whether your AML/CFT programme should be amended to reflect the changed risk.

### Audit of the AML/CFT programme

58. Under section 59(2) of the AML/CFT Act, a reporting entity must ensure that its AML/CFT programme is audited every two years, or at any other time at the request of your AML/CFT supervisor.

### Who can audit my AML/CFT programme?

59. Section 59(3) of the AML/CFT Act states that the auditor must be appropriately qualified to conduct the audit. This does not necessarily mean that the person has to be a Chartered Accountant or qualified to undertake financial audits. An audit conducted for the purposes of the AML/CFT Act does not have to meet audit standards set by professional accounting bodies. However, the person must have relevant skills or experience to conduct the audit. For example, people with AML/CFT or relevant financial experience in your sector might be suitably qualified. You must be able to justify to your AML/CFT supervisor why the auditor is appropriately qualified.

### The audit should be conducted by an independent person

60. Section 59(5) of the AML/CFT Act further provides that the person who conducts this audit must be independent, and not involved in the development of a reporting entity's risk assessment, or the establishment, implementation or maintenance of its AML/CFT programme.

61. The person appointed to undertake the audit may be a member of your staff, provided he/she is adequately separated from the area of the business carrying out your risk assessment and AML/CFT programme.

62. Similarly, you may choose to appoint an external firm to undertake the audit, but the same separation must apply. Those within the firm undertaking the audit must be separate from those involved with the risk assessment and AML/CFT programme.

- 
63. The annual report that you are required to provide to your AML/CFT supervisor must take into account results and implications of the audit.