# AML/CFT

**Anti-money laundering and countering financing of terrorism**

# Risk Assessment Guideline

**May 2018**

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 conduct your money laundering and terrorism financing risk assessment (risk assessment) 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 and control these risks.

3. A risk assessment is the first step you must take before developing your AML/CFT programme (programme). It involves identifying and assessing the inherent risks your business reasonably expects to face from ML/TF. Once you complete your risk assessment, you can then put in place a programme that minimises or mitigates these risks. 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.
    - **Gatekeepers** – The legal, accountancy, real estate, and trust and company service provider sectors are known as designated non-financial businesses and professions, or more commonly as “gatekeepers”. Gatekeepers refers to the role they play in providing services and products that can be used to facilitate the entry of illicit funds into the legitimate financial system.

10. On 1 July 2018, suspicious transaction reports (STRs) will be 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 money laundering (ML) and terrorism financing (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.

## Risk assessment

13. A core element of your AML/CFT regime is an adequate and effective risk assessment. The risk assessment is the foundation of a proportionate risk-based AML/CFT framework. Your AML/CFT supervisor expects that you will have a clear understanding of the ML/TF risks and vulnerabilities you face during the course of business.

14. You **must** base your programme on your risk assessment. The risk assessment is the foundation document for your entire AML/CFT regime. This should be clearly explained in your risk assessment and programme documentation.

## 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 information provided in relation to the regulations. We strongly recommend that you are familiar with the following documents before you undertake your risk assessment.
    - The National Risk Assessment (NRA) and FIU guidance material (accessible to reporting entities registered with the FIU's goAML system)[1]
    - Sector risk assessments (SRAs) produced by the AML/CFT supervisors[2]
    - Industry-specific guidance – for example, DIA has produced the *Lawyers and Conveyancers Guideline*[3]

[1] http://bit.ly/2zpmWPJ
[2] http://bit.ly/2HPNEou
[3] http://bit.ly/2GP2Bbi

- 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]

## Legal obligations relating to risk assessments

16. As a reporting entity[6] you have a number of obligations under the Act in relation to your risk assessment:
    - Your risk assessment **must** identify the risk of ML/TF you may reasonably expect to face during your business.
    - Your risk assessment **must** enable you to determine the level of risk involved in relation to relevant obligations under the Act. This includes the ML/TF risk presented by your customer, the products and services you offer and the countries you deal with.
    - Your risk assessment **must** be in writing and include a description of how it will be kept up to date.
    - Your risk assessment **must** have regard to guidance produced by the AML/CFT supervisors and the FIU.
    - You **must** use your risk assessment to develop your programme as set out in the Act. Refer to the *AML/CFT Programme Guideline*[7] for further information.
    - You **must** review your risk assessment to ensure it is up to date, identifies any deficiencies, and make any changes identified as necessary.[8]
    - Your risk assessment **must** be independently audited by an appropriately qualified person every two years or at any other time at the request of your AML/CFT supervisor.

17. 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.

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

---

[4] http://bit.ly/2nb1TyA

[5] http://bit.ly/2EBUMXy

[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 conduct a risk assessment, they should consider industry-specific guidance for their sector (to be published at a later date).

[7] http://bit.ly/2poP4i2

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

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

## Background

20. **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 will be evaluated on these standards and outcomes in 2020.

21. **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.

22. 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

23. 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.[10]

## Stages of money laundering

24. 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.

25. **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 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.

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

26. **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.

27. **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

28. 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: Identifying risk

29. As part of assessing risk, you **must** address your “inherent risks”. These are the ML/TF risks present before you apply controls and mitigations. You may wish to assess your “residual” risk (the risk after your controls and mitigations) as part of your risk assessment. However, your AML/CFT supervisor will expect that your risk assessment deals with inherent risk. If your risk assessment covers residual risk, you will need to document and demonstrate how you arrived at your residual risk ratings.

30. When you identify how your business may be vulnerable to ML/TF risks, you **must** consider all of the following:
    - the nature, size and complexity of your business
    - the products and services you offer
    - the way you deliver your products and services
    - the types of customers you deal with
    - the countries you deal with
    - the institutions you deal with.

### The nature, size and complexity of your business

31. The size and complexity of your business plays an important role in how attractive or susceptible it is for ML/TF. For example, because a large business is less likely to know its customers personally, it could offer a greater degree of anonymity than a small business. Likewise, a business that conducts complex transactions across international jurisdictions could offer greater opportunities to money launderers than a purely domestic business.

32. Use of corporate data will help you work out what parts of your business are vulnerable to ML/TF activity. For instance, you may have identified a higher-risk product, but without knowing how many of those products you have provided to

customers, and where they are domiciled, this will result in a flawed assessment of risk. Using your annual report data will help in this matter.

### The products and services your business offers

33. Some products and services are vulnerable to ML/TF by their nature. When considering whether the products and services your business offers could be exploited for ML/TF purposes, we recommend you consider issues such as:
    - Does the product/service allow for anonymity?
    - Does the product/service disguise or conceal the beneficial owner of your customer?
    - Does the product/service disguise or conceal the source of wealth or funds of your customer?
    - Does the product/service allow payments to third parties?
    - Does the product/service commonly involve receipt or payment in cash?
    - Has the product/service been identified in the NRA, FIU guidance material or SRAs as presenting a higher ML/TF risk?
    - Does the product/service allow for the movement of funds across borders?

34. Many other factors can contribute to the ML/TF risk of your products and services. It will be your responsibility to identify those factors as part of your risk assessment. Domestic AML/CFT guidance material will help you in this exercise. The FATF, the Asia Pacific Group on Money Laundering (APG)[11], and other overseas AML/CFT agencies (such as the Australian Transaction Reports and Analysis Centre (AUSTRAC)[12]) also publish documents in relation to the methods and trends used for ML/TF (these are also called typologies).

### The way your business delivers its products and services

35. The way your business on-boards your customers and delivers your products and services affects its vulnerability to ML/TF. For example:
    - Does your business have non-face-to-face customers (via post, telephone, internet or via intermediaries)?
    - Do you provide your products/services via the internet?
    - Does your business have indirect relationships with customers (via intermediaries, pooled accounts, etc)?
    - Do you provide your products/services via agents or intermediaries?
    - Do you provide your products/services to overseas jurisdictions?

### The types of customers your business deals with

36. Some categories of customers pose a higher risk of ML/TF than others, especially when combined with higher-risk products/services and jurisdictions.

37. The Act sets out circumstances where you **must** conduct enhanced customer due diligence (EDD) and where simplified customer due diligence (CDD) applies.

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

These sets of circumstances are a useful reference point for the types of situations that may present a higher or lower risk of ML/TF. Refer to the *Enhanced Customer Due Diligence Guideline*[13] for further information.

38. Questions you will need to ask yourself about your customers, new and existing, include:
    - Are they a trust or other legal person?
    - Have you identified beneficial ownership?
    - Are they specified in the Act as requiring EDD?
    - Are they involved in occasional or one-off activities/transactions above a certain threshold?
    - Do they use complex business structures that offer no apparent financial benefits?
    - Are they a politically exposed person (PEP)?[14]
    - Are they a cash-intensive business?
    - Are they involved in businesses associated with high levels of corruption?
    - Do they have an unexplained or hard to verify source of wealth and/or source of funds?
    - Do they conduct business through, or are they introduced by, gatekeepers such as accountants, lawyers, or other professionals? (Refer to your relevant SRA for more information on gatekeepers.)
    - Are they a non-profit organisation?
    - Have they been identified in the NRA, FIU guidance material or SRAs as presenting a higher ML/TF risk?

39. This list is not exhaustive, and many other factors can contribute to customer ML/TF risk. As with your products and services it will be your responsibility to identify those factors as part of your risk assessment. Domestic and international guidance material will help you in this exercise.

### The countries your business deals with

40. It is important to understand that the risks associated with a country are wider than having insufficient AML/CFT measures in place. It is also important to recognise the international operation of ML/TF and that New Zealand's reputation as a high-integrity, low-corruption jurisdiction makes it vulnerable to abuse. Country risk can result from:
    - ineffective AML/CFT measures
    - ineffective rule of law and economic stability
    - high levels of organised crime
    - prevalence of bribery and corruption
    - association with TF

[13] http://bit.ly/2puaRpm

[14] A PEP is a person who in the last 12 months has held a prominent overseas position. The term PEP includes their relatives and close associates, who are sometimes called RCAs. It also includes people who have beneficial ownership of legal entities or arrangements existing to benefit PEPs. Refer to the *Enhanced Customer Due Diligence Guideline* for more information on PEPs.

- conflict zones and their bordering countries
- production and/or transnational shipment of illicit drugs.

41. To help you determine country risk, the AML/CFT supervisors produced the *Countries Assessment Guideline*.[15] Other information sources that can help you in assessing country risk include:
    - FATF list of high-risk and non-cooperative jurisdictions[16]
    - FATF mutual evaluation reports
    - European Union AML and tax blacklists
    - Basel AML Index[17]
    - United Nations Office on Drugs and Crime (UNODC)[18] reports
    - Transparency International Corruption Perceptions Index[19]
    - trusted and independent media sources.

42. While not directly associated with AML/CFT, you may want to consider checking if countries are subject to United Nations sanctions, embargoes or similar measures.

### The institutions your business deals with

43. Some institutions present more ML/TF risk than others. This may be due to the nature of their industry or their association, or the types of business relationships that they have. For instance, financial institutions that are unregulated or shell companies and banks are high-risk institutions and are more likely to be used for ML/TF purposes or operated by criminals to disguise beneficial ownership.

44. Higher-risk entities such as banks, money remitters and gatekeepers are vulnerable to exploitation for ML/TF purposes and can represent risk to your business. We recommend that you refer to the NRA and your relevant SRA for further information.

### Other factors to consider when identifying aspects of your business that may be susceptible to ML/TF

45. The Act also sets out special steps you **must** take in relation to PEPs, wire transfers, correspondent banking and new technologies. This information should help you to identify high-risk areas of your business.

46. The NRA and SRAs are useful sources of information when identifying how your business could be used for ML/TF. You should also consider emerging trends that are signalled by the FIU in their guidance when identifying risks in your business. Information on current ML/TF methods is available on the FATF website. This website also has links to other internet pages that you could refer to when assessing the risk your business could be reasonably expected to face.

---

[15] http://bit.ly/2hOTHPk
[16] https://bit.ly/1RA355J
[17] https://index.baselgovernance.org/
[18] http://www.unodc.org/
[19] https://bit.ly/2BJaDBF

## Part 3: Assessing risk

47. Risk can be defined in many ways, and there is no one-size-fits-all assessment model for this process. Once you have identified the ML/TF risk that you face during business, you **must** determine the level of that risk. When assessing risk, you should consider:
    - each element of risk you have identified
    - your business experience in relation to that risk
    - information and guidance published by the AML/CFT supervisors and the FIU
    - information and guidance published by international organisations such as the FATF, APG and UNODC, and AML agencies from equivalent jurisdictions such as AUSTRAC.

48. You should allow for the different situations that currently arise in your business or are likely to arise in the near future. For instance, your risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF risks will often operate together and represent higher risks in combination.

49. Potential ways to assess risk include but are not limited to:
    - how likely an event is
    - how likely an event is and the consequence of that event
    - vulnerability, threat and impact
    - the effect of uncertainty on an event

50. Some examples are provided later in this section, but whichever method you use you will need to explain and demonstrate its adequacy and effectiveness to your AML/CFT supervisor **and** ensure it is appropriate and proportionate to your needs.

51. Your assessment of risk should be informed, logical and clearly recorded. For instance, if you have identified gatekeepers as presenting higher inherent risk in relation to the delivery of your product, your risk assessment should indicate how you arrived at this rating (domestic guidance, case studies, direct experience).

### Risk assessment (lower complexity)

52. In line with the previous AML/CFT supervisor guidance, you may want to assess risk by only considering the likelihood of ML/TF activity. This assessment should involve considering each risk factor you have identified, combined with your business experience and information published by regulators and international organisations such as the FATF. Your likelihood rating could correspond to:

| Very unlikely | Possible | Likely | Very likely |
|---|---|---|---|
| There is very little chance of ML/FT occurring in this area of your business. | There is a small chance of ML/FT occurring in this area of your business | There is a moderate chance of ML/FT occurring in this area of your business. | There is a high chance of ML/FT occurring in this area of your business |

53. For example, you may have identified that one of your products is vulnerable to ML/TF due to the potential for cross-border movement of funds. Your risk assessment highlights the product is easily accessible, that many customers are using it, and it is used in higher-risk jurisdictions. Combined with domestic and international guidance, you assess that the inherent risk rating of this product as *likely.*

54. Your programme should then address this *likely* risk with appropriate control measures. You will need to do this with each of your identified risks.

### Risk assessment (medium complexity)

55. Another way to determine the level of risk is to work out how **likely** the risk is going to happen and cross-reference that with the **consequence** of that risk (see the example of a risk matrix below).

56. Using likelihood ratings and consequence ratings can provide you with a more comprehensive understanding of your risk and a robust framework to help you arrive at a final risk rating. These ratings, in combination with structured professional opinion and experience, will assist you in applying the appropriate risk management measures as detailed in your programme.

57. For example, you may have identified that one of your products is vulnerable to ML/TF and you assess that the likelihood of this product being used in ML/TF activity is *highly probable.* You judge the impact of the identified risk happening in terms of financial loss and assess the consequence as *moderate*.

58. Cross-referencing *highly probable* with *moderate* in the risk matrix below results in a final inherent risk rating of *medium-high*. Your programme should then address this *medium-high* risk with appropriate control measures. You will need to undertake this exercise with each of your identified risks. The risk matrix below is provided as an illustrative example only.

| | | | | | | |
|---|---|---|---|---|---|---|
| Likelihood scale | 5 Almost certain | 11 | 16 | 20 | 23 | 25 |
| | 4 Highly probable | 7 | 12 | 17 | 21 | 24 |
| | 3 Possible | 4 | 8 | 13 | 18 | 22 |
| | 2 Unlikely | 2 | 5 | 9 | 14 | 19 |
| | 1 Improbable | 1 | 3 | 6 | 10 | 15 |
| | | 1 Minimal | 2 Minor | 3 Moderate | 4 Significant | 5 Severe |
| | Consequence scale | | | | | |
| Risk rating | Low | Medium | | Medium-high | | High |

### Risk assessment (higher complexity)

59. More complicated and comprehensive assessments of risk may suit larger businesses with multiple products or services.

60. You could assess risk likelihood in terms of threat and vulnerability. For example, you may consider domestic tax evasion criminals as the threat, and your accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method you use, this could result in an inherent risk rating of *highly probable*. You may then want to assess the impact of this event on your business and the wider environment.

61. Determining the impact of ML/TF activity can be challenging but can also help you focus your AML/CFT resources in a more effective and targeted manner. When determining impact, you may want to consider a number of factors, including:
    - nature and size of your business (domestic and international)
    - economic impact and financial repercussions
    - potential financial and reputational consequences
    - terrorism-related impacts
    - wider criminal activity and social harm
    - political impact
    - negative media.

62. You may want to give more weight to certain factors to provide a more nuanced understanding of your ML/TF risk.

63. In addition, you may want to consider how your risks can compound across the various risk factors. For example, you may identify that one of your products is high-risk **and** is being used in a high-risk jurisdiction that is directly involved in the production or transnational-shipment of illicit drugs. As such, you assess the compounded risk of this scenario as presenting an inherent risk rating of *severe*. You would be expected to prioritise and allocate your resources accordingly.

## Part 4: Applying a risk assessment

64. Your risk assessment should help you rank and prioritise your risks and provide a framework of how you will manage those risks.

65. Your risk assessment **must** enable you to prepare a comprehensive programme. It should enable you to meet your relevant obligations under the Act and regulations, including your obligations to conduct CDD, monitor accounts and activities and report suspicious activity.

66. Your risk assessment should help in determining suspicion and consequently assist in the decision to submit an SAR to the FIU. You **must** submit an SAR to the FIU if you think activities or transactions are suspicious. For instance, you may consider unexpected international activity of a domestic-based customer unusual, especially if it involves a high-risk jurisdiction, and submit an SAR.

67. You **must** conduct ongoing CDD. Your risk assessment will help you target and prioritise the resources needed for ongoing CDD. For instance, you may want to undertake ongoing CDD on your high-risk customers on a more regular basis than on your lower-risk customers.

68. You **must** undertake account monitoring. Your risk assessment will help you design the triggers, red flags and scenarios that can form part of your account monitoring. For instance, you may want the activity of a high-risk customer in a high-risk jurisdiction (as identified in your risk assessment) to be subject to more frequent and in-depth scrutiny.

### New and developing technologies and products

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

### Material changes and risk assessment

70. Your risk assessment should adapt when there is a material change in the nature and purpose of your business or your relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.

71. Material change could include circumstances where you introduce new products or services or have customers (or their beneficial owner) 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 result from you deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, you may need to refresh your risk assessment.

## Part 5: Review and audit of risk assessment

### Reviewing a risk assessment

72. You **must** review your risk assessment to:
    - ensure it remains current at all times
    - identify any deficiencies in its effectiveness
    - make any changes that are identified as being necessary in this process.

73. 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 risk assessment

74. You **must** audit your programme (as well as your risk assessment) every two years, or 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.

75. **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.

76. **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.

77. 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*[20] for more information.

## Part 6: 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 |
| 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 |
| RBA | Risk-based approach |
| RBNZ | Reserve Bank of New Zealand |

[20] http://bit.ly/2u6zb5l

| | |
|---|---|
| RCA | Relative and close associate |
| Risk assessment | AML/CFT risk assessment |
| SAR | Suspicious activity report |
| SRA | Sector risk assessment |
| STR | Suspicious transaction report |
| TF | Terrorism financing |
| UNODC | United Nations Office on Drugs and Crime |