Te Tari Taiwhenua
Internal Affairs

New Zealand Government

AML/CFT Risk Assessment and Programme:

Prompts and Notes for DIA reporting entities

December 2017

Contents

Executive summary

As a reporting entity, you must comply with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act or the Act) by assessing the risks of money laundering and terrorist financing (ML/TF) to your business, and by implementing a programme to manage those risks. Risks of ML/TF vary from business to business, as will the best ways to mitigate those risks. You understand your business better than anyone else, so you are best placed to identify the vulnerabilities and risks faced from ML/TF and how to develop appropriate strategies to manage and control those risks.

We recognise that assessing the risks faced by your business from ML/TF activities and establishing and implementing a programme will take time and effort, so we have developed this guideline to help you undertake your AML/CFT risk assessment (risk assessment) and design your AML/CFT compliance programme (programme).

How to read this guideline

This guideline provides you with a series of questions, supervisory expectation, reference material and suggested best practice[1] that will help guide your risk assessment and programme. It provides a starting point, which can be supplemented with the more detailed information provided by your supervisors. Before you read this guideline, make sure you are familiar with the Act[2], DIA supervisor guidelines[3] and Sector Risk Assessments and the National Risk Assessment[4].

Each section deals with a particular aspect of the risk assessment and programme and asks several questions that will help guide your understanding of your ML/TF risks and obligations.

Where AML/CFT guidance material is referenced (in bold type) it can be accessed at the following websites:

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

How to apply this guideline

This guideline can be used by all DIA-supervised reporting entities, both small and large. **Given the differences in size and complexity of reporting entities, some of the prompts and notes may not apply to your business or organisation.**

This guideline is not mandatory. You may choose to use alternative methodologies to conduct your risk assessment and develop your programme.

You should keep in mind that an effective AML/CFT regime is risk-based and your risk assessment and programme need to fit the risk your business faces. For instance, small and low-risk reporting entities should have a risk assessment and programme that is simple and proportionate to the risk they encounter.

This guideline is not a template for your risk assessment or programme. You should adapt the prompts and notes contained in this guideline to fit your individual business circumstances.

Disclaimer

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 and cannot be relied on as such. After reading this guideline, if you do not fully understand your obligations you should seek legal advice or contact your AML/CFT supervisor.

[1] Where suggested best practice is provided, which includes some supervisory expectations, this does not constitute legal advice, nor is it exhaustive in nature. It is there to help you meet your AML/CFT obligations more effectively and to help you understand and mitigate the ML/TF risk you will face in the ordinary course of business.

[2] http://bit.ly/2aFZRjN

[3] http://bit.ly/2gQ3Iev

[4] http://bit.ly/2ik1tAu

Conducting your risk assessment

Your first step to complying with the Act is to conduct a risk assessment on the potential ML/TF risks faced by your business. The specific requirements for a risk assessment are set out in section 58 of the Act. The prompts and notes provided below are there to assist you with understanding how to conduct your business' risk assessment.

1. Methodology

Prompts	Notes
Does your risk assessment have regard to applicable guidance material?	Your risk assessment must have regard to the **National Risk Assessment (NRA),** relevant **Sector Risk Assessment (SRA)** and applicable supervisor guidance. You should also use helpful reference material such as the **Financial Intelligence Unit (FIU) Quarterly Typology Reports**. Demonstrating and recording this in writing in the risk assessment will help supervisors and auditors understand how you have used guidance material.
Is your risk assessment in writing? Does it need to be complicated?	Your risk assessment must be in writing and adhere to the record keeping requirements of the Act. Low-risk businesses that do not offer complex products or services and have limited or no international exposure may not need an overly complex or sophisticated risk assessment.
Does your risk assessment use a valid and reliable methodology? Have you defined risk? Can you explain this to your staff, senior managers, board members, supervisors and auditors?	There is no one-size-fits-all ML/TF methodology for you to use. Your supervisor will expect you to have a clear methodology that can be explained by your AML/CFT compliance officer (compliance officer). The assessment of ML/TF risks faced by your business can be done using numerous methods. For instance, risk can be defined as the likelihood of an event and the consequence of that event. Risk can also be seen as a function of threat, vulnerability and impact[5]. Whichever method you choose, it should be appropriate and proportionate to your needs. You can find further information about risk in the relevant **SRA** and the **AML/CFT Risk Assessment Guideline**.
Does your risk assessment inform your programme? Is this recorded in your risk assessment?	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 articulated clearly in your risk assessment and programme documentation.
Does your risk assessment describe how it will be kept current?	Your risk assessment must be reviewed regularly and subject to audit every two years or as prescribed by regulations, or at any other time at the request of your supervisor. Use of version control at the front of your document can help demonstrate that you are keeping your risk assessment current.
Does your risk assessment **identify** the ML/TF risks faced in the ordinary course of business?	You will be expected to demonstrate how you identified your ML/TF risks. There is no one-size-fits-all ML/TF methodology for you to use. You can find further information about this in the **AML/CFT Risk Assessment Guideline**.
Does your risk assessment **determine the level** of ML/TF risk faced in the normal course of business?	You will be expected to demonstrate how you determined the level of your ML/TF risks. There is no one-size-fits-all ML/TF methodology for you to use. You can find further information about this in the **AML/CFT Risk Assessment Guideline**.

[5] As per Financial Action Task Force (FATF) guidance

Prompts	Notes
Have you considered "weighting" the potential ML/TF risk variables in your risk assessment?	You may decide that some variables are more important, or carry more weight, than others when undertaking your risk assessment. When weighting inherent risk and mitigating factors, you should make an informed judgement about the relevance of the different factors in relation to the assessment of ML/TF risk. You may decide not to weight factors to keep your risk assessment simple, or you may wish to undertake a more nuanced assessment of risk.
Have you considered "inherent" risk? These are the ML/TF risks present **before** the application of your controls and mitigation measures.	As part of conducting an assessment of risk, you are expected to address your "inherent risks". These are the ML/TF risks present before you apply controls and mitigations. You can find further information about this in the relevant **SRA** and the **AML/CFT Risk Assessment Guideline**.
Have you considered "residual" risk? These are the ML/TF risks present **after** the application of your controls and mitigation measures.	You may wish to assess your "residual" risk (the risk after your controls and mitigations) as part of your risk assessment. However, supervisors will expect that your risk assessment deals with inherent risk. If your risk assessment covers residual risk, you will need to document how you arrived at your residual risk ratings. You can find further information about this in the relevant **SRA** and the **AML/CFT Risk Assessment Guideline**.
Have you considered how ML/TF risks work together?	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.
Does your risk assessment have regard to any other factors provided for in regulation?	You will need to check that any regulations relevant to your business have been accounted for in your risk assessment.
Does your risk assessment have any exceptions or manual override functions, and what is the approval process?	There may be cases when you decide to override your risk assessment. Your risk assessment should describe how this operates, how it is approved (if applicable) and how it is recorded. For instance, you may decide that a high-risk rating in *any* of the risk variables means that the customer will be subject to extra customer due diligence (CDD) measures. The reasons for any overrides should be recorded as part of your AML/CFT record keeping.
Does your risk assessment explicitly deal with occasional transactions and occasional activities?	We recommend that your risk assessment also addresses the ML/TF risk presented by occasional transactions and activities.
Does your risk assessment address all the risk variables as laid out in the Act?	You may find it useful to structure your risk assessment to align with section 58(2)(a–f) of the Act. The following sections cover section 58(2)(a-f).

2. Nature, size and complexity

The nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors.

Prompts	Notes
Could the size of your business mask suspicious activity?	The larger your business is, the more scope there is for suspicious activities and transactions to be masked during your ordinary course of business. Using corporate structure diagrams may help you identify areas of your business that could benefit from increased levels of attention.
Could the value, volume and velocity of the transactions associated with your business mask suspicious activity?	Capacity for high-value, high-volume and high-velocity transactions is a potential risk. Individually, each variable presents possible avenues of ML/TF, and this risk is compounded in combination. The "three Vs" – value, volume and velocity – are key components in identifying ML/TF activity.
Does the **complexity** of your business make AML/CFT measures difficult to implement?	Greater complexity decreases the transparency of business transactions and activities, increases ML/TF vulnerability and may reduce the effectiveness of AML/CFT measures.
Does the **size** of your business make AML/CFT measures difficult to implement?	Large organisations may have difficulty tailoring their AML/CFT measures to meet AML/CFT requirements. Increased size may also result in reduced adequacy and effectiveness of AML/CFT measures.
Are the nature of your business transactions and activities recognised as being associated with ML/TF vulnerability?	The **NRA,** relevant **SRA, FIU Quarterly Typology Reports** and **supervisory guidance** and **newsletters** are available to assist you with this. In addition to these, you may wish to refer to FATF, Asia Pacific Group (APG), Egmont Group or other trusted AML/CFT sources. You can also refer to AML/CFT guidance from comparable jurisdictions, such as the Australian Transaction Reports and Analysis Centre (AUSTRAC) in Australia.
Does your business data or annual report data provide context to the assessment of ML/TF risk? Note: At the time of publication of these prompts and notes, Phase 2 reporting entities will not have any annual report data. However, they have their own existing business and corporate data to rely upon.	An assessment of risk requires context. Without context your assessment may be ineffective. Business data is an important aspect of this context. For instance, if you identify a product or service as being vulnerable to ML/TF, business data can indicate how many of your customers have use of this product or service, how many of them are high-risk and what jurisdictions they are in.

3. Products and services offered

Prompts	Notes
Are your products/services identified as presenting heightened risk by the AML/CFT supervisors?	You should refer to the **NRA,** the relevant **SRA,** and **FIU Quarterly Typology Reports** as well as **supervisory guidance** and **newsletters**.
Are your products/services identified as heightened risk by AML/CFT international guidance?	You should refer to FATF, APG, Egmont Group or other trusted AML/CFT sources. You can also refer to AML/CFT guidance from comparable jurisdictions, such as AUSTRAC in Australia.
Do your products/services support physical cash deposits and/or withdrawals? Note: Predicate offences are the crimes underlying ML/TF activity.	Cash is still a favoured method of ML/TF for certain predicate offending. The ease of movement without audit trail makes it highly vulnerable to ML/TF activity. You should consider ML/TF risk if your products or services can be used to deposit or obtain cash (e.g. at ATMs, at point of sale, or through a cash advance transaction).
Can your products/services be redeemed or traded for cash? Are they highly liquid? Do they support early redemption, conversion to cash or equivalent value?	Liquidity is a highly sought-after element for ML/TF activity. This can be cash or high-value goods (precious metals and gems) or certain financial instruments. You should be aware of the red flags associated with the ML/TF typologies contained in the **NRA,** relevant **SRA** and **supervisory guidance.**
Do your products/services provide international funds transfer capability?	If your products/services enable funds to be transferred to a jurisdiction outside of New Zealand (e.g. using wire transfers or high-value commodities) this may be considered an ML/TF risk.
Does your type of business facilitate prescribed transactions under the Act?	Prescribed transaction reports (PTRs) cover both international fund transfers and large cash transactions. If your business facilitates international fund transfers to a jurisdiction with weak AML/CFT controls, this may be considered an ML/TF risk. If your business deals with physical cash in large amounts, this may also be considered an ML/TF risk. We recommend you refer to **PTR reporting guidance** from the FIU on this topic.
Do your products/services support payments to/from third parties or non-customers?	This can disguise the beneficial ownership or effective control of funds. The presence of multiple intermediaries and agents can hide and disguise beneficial ownership.
Do your products/services support transactions that can be conducted remotely (e.g. via the internet) or without interaction with a reporting entity?	Less face-to-face interaction with a customer increases vulnerability to ML/TF activity. Online activity can facilitate high-speed, high-frequency and high-value activity on a global scale, often with little or no interaction between you and your customer. Gathering good information on the nature and purpose of the business relationship and expected patterns of transaction/activity will help you identify any unusual or suspicious activity.
Do your products/services allow high-value, high-volume and high-velocity transactions?	The value, volume and velocity of transactions and activities are key indicators and warnings of ML/TF activity. You should consider these elements individually and in combination.
Do your products/services operate using commission-based remuneration?	A conflict of interest between effective AML/CFT measures and commercial gain may lead to AML/CFT measures being ignored or reduced in order to gain/maintain business.

Prompts	Notes
Do your products/services support the pooling of funds and investments (e.g. a trust account or client account)?	This can disguise the beneficial ownership of funds. It can enable criminals to place money within the financial system with fewer questions being asked because of the perceived respectability and legitimacy of the source of funds. It can also act as the link between different ML/TF techniques, such as purchasing real estate.
Are your products/services targeted to offshore customers (e.g. foreign trusts)?	Having customers offshore may expose your business to ML/TF risks that are beyond your control, especially in connection with countries with weak AML/CFT regimes, high levels of corruption and bribery and organised crime.

4. Methods of delivery

This not only applies to the delivery but also the means by which a customer may apply for products and services.

Prompts	Notes
Does the method of delivery used in your business provide for anonymity?	Anonymity is highly sought after by criminal elements to facilitate ML/TF. A major part of your AML/CFT measures will be focused on removing anonymity and increasing transparency.
Does the method of delivery depend on intermediaries?	This may result in the customer's identity, beneficial owner or effective controller not being transparent to the reporting entity.
Does the method of delivery remove or minimise face-to-face contact with the customer?	Less face-to-face interaction with a customer increases vulnerability to ML/TF activity.
Does your business use a method of delivery targeted to offshore customers?	Having customers offshore may expose your business to ML/TF risks that are beyond your control, especially in connection with countries with weak AML/CFT regimes and high levels of corruption, bribery and organised crime.
Can a third party use this method of delivery?	This may result in your customer's identity, beneficial owner or effective controller not being transparent, which increases ML/TF risk.

5. Customer types

When considering customer risk, also consider the risk posed by the beneficial owner or effective controller of your customer where relevant.

Prompts	Notes
Are your customers and their ownership structure generally transparent?	Overly complex and non-transparent structures may hide and disguise beneficial ownership/effective control and mask ML/TF activity. Customers may establish legal entities in a chain of multi-jurisdictional structures to hide the true ownership and control of assets held overseas. Corporate structural diagrams may help you identify beneficial ownership and effective control and assist your AML/CFT supervisor to understand the particular ownership structure.
Do you have customers in high-risk occupations?	Some occupations can have greater vulnerability to ML/TF. For example, cash-intensive businesses, gatekeeper occupations, jewellers, high-value goods dealers, real estate agents, travel agents, import/export companies, remitters and money service businesses, and the construction industry.
Do your customers operate on a global scale?	Customers operating on a global scale will be exposed to international ML/TF risks and encounter regulation and law enforcement in different jurisdictions. This may result in undue complexity and confusion that could be used for ML/TF purposes. Global operation may hide and disguise ML/TF activity with seemingly legitimate business. For example, trade-based ML relies on the global flow of trade and complicated payment methods, producing an environment vulnerable to criminal abuse. In this environment buyers and sellers may collude to misrepresent the price, type, quality or quantity of goods to transfer funds or value between countries.
Do your customers reside in a high-risk jurisdiction?	See section 6 “Country risk” below.
Does domestic or international guidance identify the types of customers in your business as presenting a higher risk (e.g. trusts, shell companies, charities, non-profit organisations or companies with nominee shareholders or shares in bearer form)?	The AML/CFT supervisors and the FIU have produced guidance to help you meet your AML/CFT obligations. Part of this guidance provides information on ML/TF vulnerabilities and risks and should inform your risk assessment (and programme). You should refer to the **NRA,** relevant **SRA** and other **supervisory guidance** in relation to high-risk customers, as well as the **AML/CFT Beneficial Ownership Guideline** and **CDD fact sheets**.
Does your business have customers that provide financial or other professional services that are unregistered, or are poorly regulated?	Multiple financial and professional service providers involved in transactions and activities can mean greater vulnerability to ML/TF. Without proper regulation and supervision these customer types can be open to abuse.
Does your business have high net worth customers? Are they connected to high-risk industries?	High net worth customers (including heads of international organisations) can present a range of risks from illegal capital flight to high-level corruption. This risk is compounded by high-risk industries such as arms manufacturing, construction, import/export and mineral extraction.
What is the nature and purpose of the business relationships between you and your customers?	The nature and purpose of transactions and activities of your customers will directly influence the level of ML/TF risk and is an important consideration in the on-boarding process. Determining the nature and purpose of your business relationship with your customer will greatly help you with transaction monitoring (TM), ongoing CDD and submitting suspicious activity reports (SARs).

Prompts	Notes
Does your business have customers that are politically exposed persons (PEPs)?	PEPs and their relatives and close associates (RCAs) can mean greater vulnerability to ML/TF. Things to consider in relation to PEPs include association with organised crime, tax evasion, fraud, bribery and corruption, people trafficking, illegal fishing and drug offending. By the nature of the positions they hold and the opportunities they have to access large amounts of money (through corruption, bribery, kickbacks, extortion, and embezzlement), PEPs can be considered high-risk through all stages of the ML/TF process. PEPs can use their positions to influence individuals and institutions and facilitate the movement of funds. Their privileged position (access to state funds and decision-making) heightens ML/TF risk. PEPs may seek to obscure their financial position using RCAs to access the financial system. You should refer to the **EDD Guideline** for further information.
Have you considered the country risk associated with PEPs?	The risk presented by PEPs may be strongly influenced by the wider financial and geopolitical risks in their country of origin or residence.
Do your customers present other potential ML/TF risk?	When determining the ML/TF risk presented by your customers, you may wish to consider a variety of other factors, depending on your procedures, policies and controls. This will be your business decision and will be based on your appetite for ML/TF risk. Things you may wish to consider about your customers include: • Have they been the subject of previous SARs? • Are they connected to organised crime? • Have they been convicted of certain types of crime? • Have they been subject to previous civil sanctions? • Have they been subject to previous regulatory measures? • Are they the subject of adverse media? Adverse media can be explained and may not necessarily result in a higher assessment of ML/TF risk.

6. Country risk

Prompts	Notes
Does your business have dealings with countries that have weak or ineffective AML/CFT measures?	You should consider variables such as lesser AML/CFT provisions, weak regulation of business/company registration and weak law enforcement and border control capabilities. You should check if the FATF has assessed if the jurisdiction has AML/CFT deficiencies. You should refer to guidance from APG (and other FATF-style regional bodies) and the Basel AML Index. You should also have general awareness around ML/TF (media, academic study, conferences, professional body membership). We recommend you refer to the existing **Country Assessment Guideline**.
Does your business have dealings with countries that have general ML/TF risk?	Elements you may want to consider are whether the country has a cash-intensive economy, whether it is a source or a transit country for illicit commodities/services, and whether it has an unstable or weak government.
Does your business have dealings with countries that have a high degree of organised crime or drug-related crime? Does the country have a high degree of people trafficking or smuggling?	You should consider which jurisdiction your customer is from, or is resident in, when assessing ML/TF risk. The presence of a high level of organised crime is an important consideration and a primary driver of predicate offending in determining country risk. You should refer to trusted reference sources such as the United Nations Office on Drugs and Crime (UNODC) for further information on organised crime.
Does your business have dealings with countries that have a high degree of corruption and bribery?	The presence of a high level of bribery and corruption is an important consideration and a primary driver in determining country risk. Bribery and corruption fundamentally weaken any AML/CFT regime. You should refer to Transparency International for information on perceived corruption or FATF reports.
Does your business have dealings with countries that have been identified as high risk for ML/TF predicate offending?	Predicate offences are the crimes underlying ML/TF activity. They could involve fraud, tax evasion, drug-related offending, bribery, corruption, extortion, kidnapping, people trafficking, illegal fishing and high-value theft. You should refer to trusted reference sources such as the UNODC for further information on predicate crime.
Does your business have dealings with countries that are in a conflict zone or have significant terrorism activity?	Conflict zones present an extremely high risk of TF and ML. Tracing the flow of funds into and through these regions is extremely difficult. Non-profit organisations operating in these zones may be vulnerable to abuse or used as cover. Refer to the **NRA** and the relevant **SRA** for more information.
Does your business have dealings with countries that border a conflict zone? Are they a conduit country?	The movement of funds/commodities into conflict zones across borders is an identified ML/TF issue. Conduit countries may be international financial centres with well-regarded regulatory frameworks, but are near high-risk regions. This proximity can provide the capacity and links to serve as conduit countries for laundering criminal funds. Countries that are ostensibly lower-risk may be used in this way to reduce suspicion and risk of detection for funds that are then moved to other, higher-risk countries. Refer to the **NRA** and the relevant **SRA** for more information.
Does your business have dealings with countries that border a country with weak AML/CFT measures?	Cross-border movement of funds/commodities may be an issue where one jurisdiction has strong controls while their neighbour has poor controls. (Also see “conduit countries” in the row above.)

7. Institutions

Prompts	Notes
Does your business have a correspondent banking relationship?	Correspondent banking relationships are recognised internationally as potentially presenting a higher risk of ML/TF.
Does your business have dealings with institutions that have been subject to legal problems or negative media?	You should refer to previous legal actions and/or negative media using trusted sources. Legal action taken against an institution (or type of institution) may indicate weak AML/CFT measures, deliberate breaches or even criminality. Adverse media may be explained and may not necessarily result in a higher assessment of ML/TF risk.
Does your business have dealings with institutions that have been subject to regulatory action or negative AML/CFT comment from recognised and trusted sources, domestic and international?	If an institution, or type of institution, has been subject to negative regulatory action, this may indicate weak AML/CFT measures. In serious cases this could amount to wilful breaches or even criminal activity. You should refer to domestic AML/CFT supervisory guidance and FATF, APG, FIU, UNODC and trusted media sources for information on this topic.
Does your business have dealings with institutions that have suitable AML/CFT controls and supervision for AML/CFT compliance?	If an institution, or type of institution, has inadequate or ineffective AML/CFT controls, or is not subject to adequate and effective AML/CFT supervision, this may indicate weak AML/CFT measures. You should refer to domestic AML/CFT supervisory guidance and FATF, APG, FIU, UNODC and trusted media sources for information on this topic.

Preparing your AML/CFT programme

Once you have conducted your risk assessment, you are now ready to prepare your AML/CFT programme (programme). What your programme should contain is set out in section 57 of the Act. The prompts and notes provided below are to assist you with understanding how to prepare and maintain your business' programme.

1. General

Prompts	Notes
Does your programme have regard to applicable guidance material?	Your programme must have regard to the **NRA,** the relevant **SRA** and applicable **FIU** and **supervisory guidance**. Demonstrating and recording this in writing in the programme will assist supervisory and auditor functions.
Is your programme in writing?	Your programme must be in writing and adhere to the record keeping requirements of the Act.
Do you have a designated AML/CFT compliance officer?	You must have an AML/CFT compliance officer (compliance officer). The compliance officer is responsible for administering and maintaining your programme. It is also a good idea, where possible, to have a secondary officer to fill the role when the compliance officer is absent. This can be important considering some of the time constraints on certain parts of the Act (e.g. the three-day reporting rule for SARs and the potentially sensitive nature of ML/TF activity).
Have you provided a description of your business or organisation?	It may be useful to provide context to your programme by describing the nature and extent of your business or organisation. This will help supervisors and auditors as well as new staff. An organisational diagram may be useful.
Does the compliance officer report to a senior manager?	The compliance officer must report to a senior manager as part of their role under the Act. It is a good idea to record this reporting in meeting minutes, board presentations/reports and formal papers/memos.
Do you need to provide information on your governance structure?	Where relevant, you should describe the governance structure of your organisation as it applies to AML/CFT. This could involve the role of the Board, risk officers, AML/CFT committees and direct report lines.
Are you part of a designated business group?	If you are part of a designated business group (DBG), your programme should describe its structure and the division of shared and separate AML/CFT obligations where relevant.
Can you explain your programme to your staff, senior managers, board members, supervisors and auditors?	There is no one-size-fits-all programme format or methodology. Clear procedures, policies and controls (PPCs) that can be explained by your compliance officer will be expected by supervisors. Refer to the **AML/CFT Programme Guideline** for more information.
Is your programme based on your risk assessment? Is this recorded in your programme?	You must base your programme on your risk assessment. The risk assessment is the foundation document for your entire AML/CFT regime. ML/TF risks identified in your risk assessment must be addressed in your programme. If there are changes in your risk assessment they must be reflected in your programme. These changes may result from newly identified ML/TF trends, your AML/CFT audit or from supervisory inspections and reviews.
Does your programme describe how you will keep it current?	Your programme must be reviewed regularly and subject to audit every two years, or at a different time prescribed by regulations, or at any other time at the request of the relevant AML/CFT supervisor. Use of version control at the front of documents can greatly help in demonstrating this function. In addition, it may prove useful to create an AML/CFT calendar that schedules annual reporting, reviews, audits, training, senior management reports and other AML/CFT functions.

Prompts	Notes
Can you describe and demonstrate how your programme works to supervisors?	If you cannot explain how your programme works, this may result in negative comment from your supervisor. You must be able to articulate the findings of the risk assessment and how your programme addresses these findings. You will be expected to understand and describe the methodology used in your risk assessment and programme. For instance, you may be asked by supervisors how your top ML/TF inherent risks were identified, how your programme mitigated these risks and how you arrived at a residual risk rating.
How have you defined risk?	Risk is often described in terms of "likelihood" and "consequence". It can also be described as a function of "threat", "vulnerability" and "impact". Whatever description you use, you should make sure it aligns across your risk assessment and programme. Refer to the **NRA** and relevant **SRA** for more information on this topic.
Does your programme contain the PPCs to detect ML/TF and manage and mitigate ML/TF risk?	PPCs should be clear and should only apply to AML/CFT. If you decide to broaden the PPCs to incorporate other functions (e.g. sanctions), this will not be considered by supervisors or auditors.
Have you considered inherent risk? Does your programme clearly show how inherent risk was determined?	As part of your programme, you are expected to explain how you will mitigate your **inherent** risks. These are the ML/TF risks present before the application of controls and mitigation measures. Refer to the relevant **SRA** and the **AML/CFT Programme Guideline** for further information.
Have you considered residual risk? Does your programme clearly show how residual risk was determined?	You will be expected to assess your **residual** risk, the risk that remains after your controls are in place, as part of your programme. Be prepared to explain how you arrived at your residual risk ratings. Refer to the relevant **SRA** and the **AML/CFT Programme Guideline** for further information.
Is your programme both adequate and effective?	When evaluating your programme (and risk assessment), supervisors and auditors will want to explore both adequacy and effectiveness. Adequacy can be described as how compliant your written programme is with the various obligations of the Act. Effectiveness can be 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.
Does your programme have regard to any other factors provided for in regulation?	You will need to check that your programme complies with any regulations relevant to your business.
Does your programme explicitly deal with occasional transactions and occasional activities as defined in the Act?	We recommend that your programme PPCs address occasional transactions and activities. CDD requirements apply, as do various reporting thresholds.
Does your programme demonstrate a risk-based approach to prohibitions of customers?	Your PPCs should ideally demonstrate a risk-based approach that does not refuse or terminate business relationships with entire categories of customers that you assess as presenting higher ML/TF risk. Risk levels will vary by individual businesses within customer categories. However, prohibitions will ultimately be your business decision.

2. Staff Vetting

Prompts	Notes
Does your programme contain PPCs for staff vetting?	Your programme must contain PPCs for staff vetting. If you already have adequate and effective PPCs in place for staff vetting that are also suitable for AML/CFT purposes, you could include them in your programme. Suggested topics include: • How vetting is differentiated for senior managers, compliance officers and customer-facing roles • How vetting is applied when people change roles • How vetting is applied to temporary staff and/or contractors • Event-triggered vetting (e.g. adverse media about a staff member, an SAR is made in relation to an employee, or an employee fails to submit an SAR where one would be expected)
Do the PPCs cover police checks, media checks, PEP checks and other risk factors?	Your vetting PPCs may cover whether police and PEP checks have been undertaken, whether the person has lived in a high-risk country, or whether they have been subject to regulatory action. Your PPCs could also cover negative media that can be explained or discounted.

3. Training

Prompts	Notes
Does your programme contain PPCs for training?	Your programme must contain PPCs for training. Training not only equips you and your staff with the knowledge to combat ML/TF, it can also raise awareness of the topic across your business in general and help foster a culture of AML/CFT compliance.
Are your PPCs fit for purpose?	Training PPCs can include: • How the training package reflects your risk assessment • The frequency and delivery methods of training • The timing of review and updating of material • How training has/will adapt to fit trigger events, new technology or products and any emerging trends. For instance, does the training package reflect current conflict zones? • How and where training and testing is recorded and tracked • Whether training requirements cover temporary staff or contractors
Do your PPCs differentiate for senior managers, compliance officers and customer-facing roles?	Different levels of training may be necessary for customer-facing and more AML/CFT-focused roles within an organisation. For instance, the compliance officer should receive the highest levels of training due to their AML/CFT responsibilities.
Do the PPCs allow for staff changing roles, contractors, temporary staff or new employees?	Training should be made available for people moving into AML/CFT-related roles outside of the normal training cycle.
Who conducts the training?	Your AML/CFT training could be conducted by the compliance officer, in-house experts or a suitably qualified outside organisation. Supervisors (and auditors) may ask to see training material as part of a desktop review or on-site inspection.

4. Customer due diligence (CDD)

CDD is of vital importance to an adequate and effective AML/CFT regime. CDD is central to both the assessment and management of risk. We recommend that reporting entities pay extra attention to this aspect of their programme and demonstrate a risk-based approach.

Prompts	Notes
Do your CDD measures meet the requirements of the Act?	Your programme must contain PPCs for CDD. There are three types of CDD: simplified CDD, standard CDD, and enhanced CDD (EDD). Attention must be given to the different types of CDD you carry out and the circumstances under which different types of CDD are undertaken.
Do your CDD measures describe the circumstances where standard CDD is applied?	Standard CDD is likely to apply to most New Zealand customers. It involves the collection of identity information of the customer, any beneficial ownership of the customer and any persons acting on behalf of the customer. Verification measures need to be reasonable and based on the level of ML/TF risk. Refer to the **AML/CFT Beneficial Ownership Guideline** and **CDD fact sheets** for further information.
Does your programme set out the framework of your CDD processes?	Your programme should contain the following basics: • How your business will address the risks identified in your risk assessment and its approach to conducting CDD • What customer information/documents you require to conduct the various types of CDD and how you will verify this information • How you have incorporated CDD into your customer on-boarding processes, including the process that will determine when to conduct simplified, standard or enhanced CDD • How you will carry out EDD for higher-risk customers, transactions and activities • How you will establish whether a customer or beneficial owner/effective controller of a customer is a PEP • How you will ensure, where necessary, that your staff understand the definitions of "beneficial owner" and "effective controller" • How your CDD processes will identify your customers' beneficial owners or effective controllers • The timing and methods of identity verification • Circumstances where delayed verification of identity can be applied
Do the CDD elements of your programme reflect the **2013 Amended Identity Verification Code of Practice (IVCOP)?**	The IVCOP provides a "safe harbour" for reporting entities, meaning that following the code fully will be regarded as compliance with the Act's requirements. However, the IVCOP only applies to low- and medium-risk customers, and further CDD may be required for higher-risk customers. You should refer to the **IVCOP** for further information.
Do your CDD measures describe the circumstances where exceptions to IVCOP can be applied?	To comply with the IVCOP, a reporting entity must have appropriate exception handling procedures in place for circumstances where a customer demonstrates they cannot comply. Your PPCs will need to clearly define under what circumstances exceptions will occur and what the approval process is. If you make an exception, this should be recorded as part of your AML/CFT record keeping.

Prompts	Notes
Do your CDD measures describe the circumstances where prohibitions can, or must, be applied?	Among other matters, you must not establish or continue a business relationship with a customer if you are unable to conduct CDD in accordance with the Act. Your PPCs should cover these prohibitions. It may be useful to record the narrative of CDD efforts made (documents requested, people spoken to, emails sent) and the timeline of these efforts as part of your record keeping. Your PPCs could provide set timeframes for enacting the prohibitions and the circumstances for collecting CDD information before they come into force. For example, you may decide a 10 working day period to collect the necessary CDD before exiting the customer is sufficient, or if the customer repeatedly fails to engage with the CDD process. You must consider submitting an SAR if you are unable to conduct CDD. Other prohibitions apply to customer anonymity and shell banks.
Do your PPCs describe which customer types your organisation will not form a business relationship with?	You may wish to list customer types you will not have a relationship with. This will make it clear to staff, supervisors and auditors what is expected prior to undertaking CDD. For instance, you must prohibit relationships with shell banks and customers with false names and anonymity. You may wish to prohibit entities with bearer share ownership, known illegal businesses and individuals from FATF-defined high-risk and non-cooperative jurisdictions.
Do your programme PPCs define “material change” and describe how it will be addressed?	Your programme should cover how you will define and identify if there has been a material change in the nature or purpose of a business relationship with your customers. When this happens, according to the level of risk involved, you will need to conduct CDD at the appropriate level. There is no standard definition of material change, but it should reflect your ordinary course of business and your risk assessment.
Does your programme detail trigger events that will result in a review of CDD?	You need to identify triggers that will prompt a review of CDD. This could include new guidance material, submission of SARs, changes in risk ratings, adverse media, criminal activity or wider geopolitical events.
How does your programme deal with PEPs?	Your programme should describe how you will define, identify and deal with customers who are PEPs. For example, how you use the services of a commercial PEP list provider (if relevant), how your senior management will approve establishing or continuing business relationships with PEPs (or other high-risk customers), and how you will manage and mitigate the ML/TF risks associated with PEPs. This should align with the findings of your risk assessment where appropriate.
Does your programme provide details on the use of third parties to perform CDD (if applicable)?	If you are relying on third parties to undertake CDD duties, your PPCs must cover how this is done. Topics you may wish to include are: • Written service level agreements • Acknowledgement of consent • Levels of AML/CFT skill and knowledge of the third party • Testing schedules and results of your inspection of the third-party AML/CFT measures • Review of CDD undertaken by the third party • If the third party is overseas, whether they meet the minimum standards of the Act • How you will utilise the reliance functions of the Act

5. Simplified CDD

Prompts	Notes
Do your CDD measures describe the circumstances where simplified CDD is applied?	Simplified CDD can be conducted on a specified set of organisations, such as government departments, local authorities and certain listed companies. The list of simplified CDD organisations is contained in section 18 of the Act. According to the level of risk involved, you must also verify the identity of the person acting on behalf of these customers, and their authority to do so.

6. Enhanced CDD (EDD)

Prompts	Notes
Do your CDD measures describe the circumstances where EDD is applied?	EDD must be conducted in a number of specific situations as set out in the Act. EDD must also be conducted according to the level of risk presented by your customer and their activities based on your risk assessment and on customer types prescribed in the Act (e.g. trusts, companies with nominee shareholders, customers in high-risk jurisdiction, PEPs). EDD requires the collection and verification of the same information as standard CDD, as well as the collection and verification of information relating to the source of wealth of the customer or source of funds for the transaction/activity. Refer to the **AML/CFT Beneficial Ownership Guideline** and the **EDD Guideline**.
Do your EDD PPCs cover all aspects of the topic?	EDD can require extra time and effort. As such, it may prove useful for your business to have clear and defined PPCs for EDD measures. This could include: • Timing of EDD and documents used to meet EDD requirements • According to the level of risk involved, the degree to which you investigate source of wealth and source of funds • According to the level of risk involved, the levels of EDD for certain types of trusts • EDD in respect of submitting SARs and tipping off provisions • Record keeping of EDD efforts • Senior management sign-off for certain customers requiring EDD

7. Ongoing CDD

Not all risk factors associated with your customer will be apparent at the outset. They may emerge only once business relationships have been established.

Prompts	Notes
Does your programme contain PPCs for ongoing CDD?	Ongoing CDD on your customers is required by the Act and is part of your broader CDD obligations. How this is carried out will need to be covered by your PPCs with potential reference to the following: • Reviewing CDD when customer risk ratings increase or if they are identified as a PEP after being on-boarded or the nature and purpose of their business changes • Whether submission of SARs impacts on ongoing CDD • Whether PTR activity impacts on ongoing CDD • Whether customer activity is consistent with your knowledge of the nature and purpose of the business relationship • How ongoing CDD applies to material changes in business relationships • The role of ongoing CDD when there is evidence of false or insufficient customer information
Have you scheduled ongoing CDD using a risk-based approach?	The timing of the ongoing CDD could be based on the risk rating of the customer or the types of products/services they use. The timing could also be based on a class of customer or the industry they are associated with. Your PPCs should detail the reasons for ongoing CDD.

8. Account monitoring

This is also called transaction monitoring (TM) or activity monitoring. For the purposes of this document the abbreviation TM will be used.

Prompts	Notes
Does your programme contain PPCs for your TM system?	Your PPCs for TM should provide details on the methods used for TM (automated, manual or both), whether they are proportionate to your ML/TF risk, and how they are applied to your business. They should also describe how the alerts generated by your TM system are recorded, collated, analysed, reported and actioned. For small, low-risk reporting entities, their TM system will be fairly simple and straightforward.
If relevant, have you tested your TM thresholds and scenarios (sometimes referred to as rules)?	TM thresholds and scenarios should be tested on a regular basis to ensure they remain relevant to your business. Your TM rules should adapt to new products and services, updated guidance, supervisory direction, audit findings and self-identified vulnerabilities. Testing TM rules and scenarios can reduce the number of false-positive alerts generated by your system. This testing should be recorded as with other AML/CFT obligations. Again, for small, low-risk reporting entities, the TM testing will be fairly simple and straightforward.
Do your TM thresholds and scenarios reflect your risk assessment and guidance material?	TM systems are generally structured to generate alerts that indicate potential ML/TF activity. The design of your TM alerts should consider the following: • Findings of your risk assessment • Relevant guidance material, **SRAs** and **NRA** • Appropriate thresholds and trigger events • Patterns of ML/TF related activity • Recognised ML/TF scenarios • Identified ML/TF vulnerabilities • Recognised red flags (refer to **NRA, SRAs** and other domestic guidance as well as FATF, APG and AUSTRAC)
Can you describe the scope of your alerts and scenarios?	You may wish to provide a short description of your alert thresholds and scenarios. Overly broad TM rules can result in too many alerts being generated, which can mask genuine high-risk alerts. Too narrow and you may miss ML/TF activity.

9. Suspicious activity reports (SARs)

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.

Prompts	Notes
Does your programme contain adequate and effective PPCs to detect and report suspicious activity to the FIU?	Detecting and reporting suspicious activity is a core element of the Act. You must have PPCs for submitting SARs and they should address the following: • Forming suspicion based on objective and reasonable grounds • Providing grounds for suspicion in the SAR • Providing mandatory details as required by the Act and Regulations • Providing reasons why SARs are not submitted to the FIU • Whether suspicion was raised by staff or TM alerts • Whether business relationships will continue after submission of SARs • Circumstances when to submit SARs orally • Keeping adequate SAR records for five years Refer to the **SAR guidance** produced by the FIU for further information.
Does your programme contain adequate and effective PPCs to manage tipping off provisions contained in the Act?	It is an offence to provide an SAR or information related to an SAR to an unauthorised person. This is commonly referred to as tipping off. Your PPCs should be clear on how you will avoid this, and it should be communicated to your staff. We suggest you include this topic in your training material.
If relevant, does your programme contain adequate and effective PPCs to manage legal professional privilege and SARs?	Your PPCs should be clear on your rationale and processes around legal professional privilege and SARs. You should refer to industry-specific guidance for further information on this topic.
Who submits the SAR?	The person directly involved in the activity does not necessarily have to submit the SAR. It may prove easier for the compliance officer to be a central point of collation and for them to decide whether to submit SARs or not. This will help maintain consistency of judgement and reporting standards. Your PPCs will need to be clear on this matter.
Does your programme set out how you will submit SARs within the required three working day timeframe?	Your PPCs should detail how you escalate (or not) initial unusual activity to submission of an SAR. For instance, you could record the escalation in the following manner: • Date and description of unusual activity/transaction • Date noted or TM alert generated • Date and description of initial research and/or EDD measures (if relevant) • Date submitted to compliance officer (if applicable) • Description of why SAR is to be submitted • Description of why SAR is not to be submitted • Date compliance officer formally forms suspicion (if applicable) • Date SAR submitted to FIU • Date and reason rejected by FIU (if relevant) • Date of re-submission (if relevant) • Date and description of any follow-up SAR related action

Prompts	Notes
Does your programme set out how you will submit suspicious property reports under the Terrorist Suppression Act 2002?	Under the Terrorist Suppression Act if you deal with an individual or organisation who is matched appropriately on New Zealand's terrorist designation list, a suspicious property report (SPR) must be completed. If a match is made on another non-New Zealand terrorist designation list, you must submit an SAR. Refer to the **SAR guidance** and the Terrorist Suppression Act for further information.

10. Prescribed transaction reports (PTRs)

Prompts	Notes
If relevant, does your programme describe how you will collect, collate and submit PTRs?	Depending on the services you offer, you may have to submit PTRs. If so, you must have PPCs for the submission of these reports. PTRs must be submitted for international funds transfers of NZD $1,000 and over and large physical cash transactions of NZD $10,000 and over. PTRs must be submitted by ordering or beneficial institutions. Refer to FIU **PTR guidance** on how to submit PTRs. If you have any confusion about whether you have to submit PTRs, contact your supervisor or seek independent legal advice.
Does your programme set out how you will submit PTRs within the required 10-day timeframe?	PTRs must be submitted to the FIU within 10 working days of the transaction. Your PPCs will need to reflect how you will submit the PTRs – individually or in batches. Refer to FIU **PTR guidance** on how to submit PTRs.

11. Record keeping

Prompts	Notes
Does your programme describe how you will meet the record keeping requirements of the Act?	Your PPCs for record keeping must include the following: • How you will reconstruct transactions if required • How you will evidence the collection and verification of customers' identities • How you will manage retention and destruction of records Records must be in English (or a language that can be readily translated into English) and kept for a minimum of five years after a transaction/activity or after a business relationship has ended. The use of decision logs or diary notes may be useful to meet this obligation.
Have you kept a written record of activities, patterns of behaviour and other activities that may be associated with ML/TF?	The Act requires that your programme contain PPCs to examine, and keep written findings relating to activity that is likely by its nature to be related to ML/TF. You must also examine and keep written findings on activity that may result in SARs. This includes reasons why activities are escalated to an SAR and, just as importantly, the reasons why activities are not escalated. This includes complex, or unusually large transactions and unusual patterns of transactions that have no apparent economic or visible lawful purposes. You may want to consider the use of decision logs or diary notes to assist you meet this obligation. Refer to section 9 "Suspicious activity reports (SARs)" for further information.
Have you kept a written record of your dealings with countries with insufficient AML/CFT measures?	Your PPCs must set out how you will monitor, examine, and keep written findings relating to business relationships and transactions with countries that have insufficient AML/CFT systems. Your programme must include measures that restrict any dealings with these countries. For example, you may require senior management approval for transactions to or from these countries. Such decisions should be recorded in writing.

12. Manage and mitigate ML/TF risks

Prompts	Notes
Does your programme describe how you will manage and mitigate ML/TF risks	Your programme will need to demonstrate how you have addressed the risks identified in your risk assessment. This can include: • The process and methodology of assessing residual risk • Describing and assessing the strength of your mitigation measures • The role of a risk appetite statement (if you have one) It will prove useful to have your compliance officer being able to fully describe to supervisors and auditors how your risk assessment identifies and rates inherent risks, and how your programme mitigates those risks, arriving at residual risk ratings.
Does your programme detail how you will assess new products and technologies?	New products and technologies can present unknown ML/TF risks. You will need to assess their risks and vulnerabilities and incorporate your findings into your risk assessment and programme.

13. Monitor and manage compliance with the Act

Prompts	Notes
Does your programme describe how you will monitor and manage compliance with the Act?	Your PPCs need to cover how you will ensure the effective oversight and monitoring of your programme. These PPCs must be in place to ensure continued compliance with the Act. This could include the following: • 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
As new guidance is produced, or older guidance is refreshed, how will you keep your risk assessment and programme up to date?	Your compliance officer is responsible for monitoring changes to the Act and guidance material, and for reviewing the risk assessment and programme. Version control of your risk assessment and programme can be useful in these situations.
Does your programme contain information on how AML/CFT breaches and incidents are dealt with?	Your PPCs should describe the mechanism for dealing with breaches of the Act. Breaches of the Act may require remedial action and testing the effectiveness of your AML/CFT measures. Supervisors and auditors may also identify breaches and lack of compliance. If relevant, this may result in compliance officer feedback to senior management and the Board. Liaison with your AML/CFT supervisor will be key in dealing with breaches and non-compliance.

14. Products, transactions and activities that favour anonymity

Prompts	Notes
Have you given explicit thought to whether your products and services favour anonymity?	Your PPCs must indicate how you prevent anonymity. This could include how you deal with: • New or developing technologies or products that favour anonymity • Delivery methods or products/services that favour anonymity • Products sourced via third parties or intermediaries
What happens when you find that a product, transaction or activity favours anonymity?	Your PPCs should contain your actions to mitigate the ML/TF risk posed by anonymity. For instance, redesigning or cancelling products, undergoing remediation processes and reviewing relevant customer transactions and activities.