IN CONFIDENCE

Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT).

Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers

April 2017

Reserve Bank of New Zealand
Te Pūtea Matua

Important Information

This Sector Risk Assessment is intended to provide general and illustrative information to:

1. assist reporting entities in the sector supervised by the Reserve Bank to prepare and review their individual assessments of the risk of money laundering and the financing of terrorism under sections 58 and 59 of the Act, and

2. inform and assist others involved in AML policy making and supervision in New Zealand and elsewhere.

The Sector Risk Assessment is not intended to cover all money laundering and terrorist financing risks that may be specific to the circumstances of individual reporting entities. Quantitative data provided in Part 3 of the Sector Risk Assessment is sourced from Annual AML/CFT Reports provided to the Reserve Bank by the reporting entities it supervises under section 60 of the Act. The assessments and information in the Sector Risk Assessment relate solely to risks relating to money laundering and terrorism financing and do not reflect on the soundness of the sector, sub-sectors, or individual reporting entities.

Contents

IN CONFIDENCE

Executive Summary

Scope

1. This is the second edition of the Sector Risk Assessment (SRA) undertaken by the Reserve Bank of New Zealand (RBNZ) for anti-money laundering and countering financing of terrorism (AML/CFT) purposes. The RBNZ supervises registered banks, non-bank deposit takers (NBDTs) and life insurers for the purposes of the Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (the Act). The Department of Internal Affairs (DIA) and the Financial Markets Authority (FMA) periodically publish similar risk assessments for the sectors they supervise.

2. The SRA 2017 will assist the RBNZ AML/CFT supervisors in understanding the risks of money laundering (ML) and terrorism financing (TF) in the RBNZ sector. It will, in conjunction with other guidance documents produced by the AML/CFT supervisors, provide guidance to reporting entities on areas of ML and TF risks in their businesses.

Limitations

3. For consistency when comparing sub-sectors RBNZ did not take into account the adequacy or effectiveness of any ML/TF controls. The SRA 2017 is an assessment of potential **inherent** risk across each sub-sector and the sector as a whole. The SRA 2017 does not assess **residual** risk (the risk present after applying AML/CFT controls).

4. Each reporting entity is expected to determine the levels of ML/TF **inherent** risk in the context of its course of business. Once it has determined its **inherent** risk it can then apply its AML/CFT controls and determine its **residual** ML/TF risk.

5. The SRA 2017 has drawn on aspects of New Zealand Police Financial Intelligence Unit (FIU) typology reports and from the existing SRAs of the FMA and the DIA. In addition, the SRA 2017 uses guidance and reports from other jurisdictions and international organisations such as the Financial Action Taskforce (FATF) which is the inter-governmental body developing and promoting policies to combat ML/TF.

6. The SRA 2017 works on two distinct levels. It provides an assessment of ML/TF risk and identifies key ML/TF vulnerabilities and how they impact each sub sector. **A risk rating for ML/TF is not an indication of financial strength or stability of any financial sector or reporting entity within the sector.**

Assessment of Risk

7. ML/TF risk is assessed as High, Medium or Low and is based on available data, guidance and appropriately experienced professional opinion. The table below summarises the assessed potential inherent ML/TF risk of each sub-sector as a whole and its constituent parts.

Sub-sector	Inherent risk of ML/TF
Registered banks – overall inherent risk rating	High
Retail	High
Business/Commercial	High
Wholesale/Institutional	Medium
Non-Bank Deposit Takers – overall inherent risk rating	Medium
Deposit Taking Finance Companies	Low
Building Societies	Medium
Credit Unions	Medium
Life Insurers – overall inherent risk rating	Low

8. The overall **High** risk rating for banks is consistent with the characteristics of the banking industry in the absence of AML/CFT controls. This is to be expected given the relative size of the banking sub-sector, the large number of customers and the high number and value of transactions compared to other areas. Combined with the wide availability and easy accessibility of products and services and access to international financial systems the banking sub-sector presents a much greater risk of ML/TF than the other sub-sectors. In this edition of the SRA, we have improved our assessment by providing a breakdown of retail banking, business/commercial banking and wholesale/institutional banking. However, the overall risk rating of High for the banking industry remains unchanged.

9. The overall **Medium** risk rating for the NBDT sector reflects the relatively smaller size and complexity of this sub-sector compared to the banking sub-sector even though it has some similar products and services to the retail banks. However, the NBDT sector is vulnerable to a number of ML/TF factors and may present an attractive avenue for ML/TF. In this edition of the SRA, we have reduced our assessment of overall ML/TF risk within the Deposit Taking Finance Companies, and have increased our assessment of overall ML/TF risk within the Credit Unions. However, the overall risk rating of Medium for the NBDT sector remains unchanged.

10. The overall **Low** risk rating for the insurance industry remains unchanged and reflects the smaller size and relatively simple life insurance products and services covered by the Act. While assessed as having a Low risk of ML/TF the insurance sector has a number of industry specific typologies and has been highlighted internationally as being potentially vulnerable to a number of ML/TF activities.

Key Vulnerabilities

11. The SRA 2017 identifies 12 key ML/TF potential vulnerabilities which impact reporting entities in all three of the RBNZ sub-sectors and are in line with domestic and international experience. The vulnerabilities presented in the table below are in no particular order as each sub-sector will prioritise vulnerabilities differently. Specific vulnerabilities should be fully considered in a reporting entity's risk assessment.

Vulnerability	
Gatekeepers	Cards
TCSPs and shell companies	Anonymity
International Payments	High Risk Customers
Cash	High risk jurisdictions
International trade and trade based money laundering (TBML)	Typologies relating to Money Service Businesses (MSBs)
New Payment Technology (NPT)	Lack of ML/TF awareness

12. When undertaking their own risk assessments reporting entities should consider these 12 potential ML/TF vulnerabilities and how they impact on their business.

13. The FIU has produced a very useful guide (http://www.police.govt.nz/advice/businesses-and-organisations/fiu/goaml) for the submission of STRs. This guide contains a number of industry specific indicators and warnings of ML and TF activity. Reporting entities are recommended to refer to this guide when assessing ML/TF risk and establishing and maintaining AML/CFT programmes.

Predicate Offending

14. Taking direction from overseas experience and the reports of the FIU it is important that RBNZ reporting entities are aware of the full range of criminal offending that can lead to ML/TF activity. In particular, current AML/CFT thinking both domestically and internationally stresses a move away from a primary focus on drug offending and broadens the scope of AML/CFT to better address fraud, tax evasion and other crime.

15. For instance, while the FATF have identified that most criminal cash proceeds are from drug trafficking, the amounts involved are closely followed by smuggling, fraud, and corruption and people trafficking. In addition, the proceeds of crime from tax evasion, while hard to quantify, are believed to be significant.

Terrorist Financing (TF)

16. Given the increasingly important and dynamic nature of TF risk this topic is covered in a dedicated section of the SRA 2017. While terrorism is generally assessed as low within NZ it is prudent to provide guidance on the vulnerabilities and risks associated with the global issue of TF. This section reflects guidance from the FIU and from overseas agencies.

Importance of a Good Risk Assessment

17. A core element of a reporting entity's AML/CFT compliance is an adequate and effective risk assessment. The written risk assessment is the foundation of a proportionate risk-based approach (RBA) to AML/CFT. RBNZ expects each reporting entity to have a clear understanding of the inherent ML/TF risks it faces during the course of its business and the vulnerabilities to which it is exposed. An inadequate risk assessment will result in an inadequate and ineffective AML/CFT programme which will have a detrimental impact on a reporting entity's ML/FT control measures.

SRA 2011 and SRA 2017

18. The SRA 2017 compared to the SRA 2011 has the following key differences:

- It builds on the domestic experience gathered since the implementation of the Act.
- It uses a different methodology to assess ML/TF risk. Part Four of this document details the Methodology used.
- The concept of ML/TF vulnerability has been introduced as well as using a risk rating.
- TF is the subject of more detailed analysis.
- A wider range of domestic and international guidance has been used.

19. ML/TF risk questions have been formalised for the sector. Questions have been included in this document, for each reporting entity to use when next reviewing and updating their written risk assessment and AML/CFT programme.

SRA and NRA as a Trigger Event for Reporting Entities

20. Publication of this second edition of RBNZ's SRA and the NRA (refer paragraph 27) should be viewed by REs as a trigger for reviewing and, where necessary, updating their AML/CFT policies, procedures and internal controls. Reporting entities are expected to refer to section 58 (2)(g), section 58(3)(b), and s.59(1)(a) of the AML/CFT Act, paragraph 35 of the Risk Assessment Guideline, and paragraph 53 of the AML/CFT programme guideline for more information about how to incorporate the information contained in this document into their Risk Assessment and AML/CFT programme. The SRA 2017 should inform a reporting entity's risk management and mitigation.

Introduction

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

21. The Anti-Money Laundering and Countering the Financing of Terrorism Act 2009 (the Act) was passed in October 2009 and came into full effect on 30 June 2013. The purposes of the Act are:

    - To detect and deter ML and TF;
    - To maintain and enhance NZ's international reputation by adopting, where appropriate in the NZ context, recommendations issued by the FATF; and
    - To contribute to public confidence in the financial system.

22. Under Section 131 of the Act, one of the functions of each AML/CFT supervisor is to identify and assess the level of risk of ML/TF across all of the reporting entities that it supervises. This has been undertaken in the form of the SRA in 2011 and now in 2017.

Purpose of the SRA

23. This is the second SRA undertaken by RBNZ in relation to the ML/TF risks in its sectors and has the following purposes:

    - It assists the AML/CFT supervisors in their understanding of particular ML/TF risks within their sectors;
    - It provides guidance to reporting entities on the risks relevant to their sector or sub-sector and informs their risk assessment;
    - It contributes to the on-going FIU assessment of ML/TF risks in New Zealand (NZ) financial institutions;
    - It assists New Zealand in meeting FATF Recommendation 26 requiring countries to subject registered banks (and other financial institutions) to adequate AML/CFT regulation, licensing and supervision; and
    - The SRA is also consistent with Basel Core principles (BCP 8 - Supervisory approach and BCP 29 - Abuse of financial services) which states that supervisors should understand and monitor the risks to which the banking sector is exposed.

The Risk-Based Approach (RBA) Regime

24. The Act allows for a risk-based approach. In practice this means that reporting entities should consider the potential vulnerabilities outlined in this document as part of their own risk assessments, and consider whether these are priorities for their business to address and control. The purpose of a RBA is to minimise compliance costs and ensure that resources are targeted towards higher-risk, higher-priority areas. It is important to acknowledge that in a RBA regime reporting entities will not adopt identical AML/CFT policies, procedures or controls. Context is everything in regards to a RBA and no two reporting entities are exactly the same.

Three Levels of Risk Assessment

25. Three levels of AML/CFT risk assessment are undertaken in NZ; national, sector and individual reporting entity.

26. The following diagram outlines the inter-relationship of the risk assessment process:

27. **National Risk Assessment (NRA)** - The NRA gives an overview of ML/TF issues affecting NZ from a law enforcement perspective utilising information from suspicious transaction reports (STRs) and proceeds of crime asset recovery data. Information from government organisations, both domestic and international, also contributes to this assessment. The FIU also develops and maintains indicators of ML/TF and publishes the Quarterly Typology Reports (QTRs). It is **strongly recommended** that reporting entities refer to the NRA and the QTRs in order to gain a better understanding of ML/TF risk. The NRA contains information on how money is laundered, how ML/TF impacts NZ and ML/TF typologies.

28. **Sector Risk Assessment (SRA)** – The three AML/CFT supervisors have each produced sector risk assessments. The RBNZ SRA 2017 draws on a variety of sources, including annual AML/CFT reports made by reporting entities, RBNZ onsite visit experience, international guidance, FIU risk assessments and reporting entity risk assessments. On-going SRA work will be conducted by RBNZ in order to continually improve its understanding of the ML/FT risks associated with its sector and to inform reporting entities of risk indicators, trends and emerging issues. The SRA may be revised regularly, or on an ad-hoc basis, depending on how ML/TF risks affect the RBNZ sector.

29. **Risk Assessments written by Reporting Entities** - Section 58 of the Act requires all reporting entities to undertake an assessment of the risk of ML/TF in their business. The risk assessment must consider the nature, size and complexity of its business, products and services (including delivery methods), customers and any countries and/ or institutions dealt with in the course of its business. One of the factors that reporting entities must have regard to when developing their risk assessments is guidance material produced by their AML/CFT Supervisor and the FIU. The SRA 2017 forms part of the AML/CFT guidance material issued by the RBNZ. Reporting entities are encouraged to access international AML/CFT guidance; in particular the material produced by the FATF and the Asia Pacific Group on Money Laundering (APG).

Risk Appetite

30. Regardless of the assessed ML/TF risk and vulnerability ratings in the SRA 2017, when each reporting entity assesses its own ML/TF risk, consideration should be given to the level of risk it is willing to accept. A RBA recognises that there can never be a zero ML/TF risk situation and each reporting entity is expected to determine the level of AML/CFT control measures commensurate to the ML/TF risks to which it is exposed in order for those risks to be effectively mitigated. This is not a legislative requirement but may help reporting entities with their risk management.

31. The Act facilitates co-operation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies. RBNZ contributes to the administration of the AML/CFT regime by supervising compliance with the Act and monitoring and assessing levels of ML/TF risk across all of the reporting entities that it supervises. The SRA 2017 is part of this.

32. ML activity has the potential to result in very serious social harm, criminal, financial and reputational consequences. Terrorism, while recognised as low risk within NZ, has the potential for catastrophic consequences.

Stages of Money Laundering

33. 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 involve smaller amounts (see Terrorist Financing (TF) for further information).

- **Placement** occurs when criminals introduce proceeds of crime into the financial system. This might be done by breaking up large amounts of cash into less conspicuous 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 predicate offending.
- **Layering** occurs once proceeds of crime are in the financial system. Layering involves a series of conversions or movements of funds to distance or disguise them from their criminal origin. The funds might be channelled through the purchase and sale of investment instruments or be wired through accounts at various banks across the globe. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.
- **Integration** occurs once enough layers have been created to hide the criminal origin of the proceeds. This stage is the ultimate objective of laundering where 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.

RBNZ's AML/CFT Sector

Nature and Size of the RBNZ Sector

34. The RBNZ currently supervises 110 reporting entities including 24 registered banks, 14 life insurance providers, 27 NBDTs and 45 reporting entities who are the members of a designated business group (DBG). Six additional reporting entities ceased operations or had moved out-of-scope by the end of the year (30 June 2016), and 20 additional life insurers were assessed as wholly exempt from the AML Act.

35. There are currently 12 DBGs in RBNZ's sector, the majority of which have been created by large banking groups.

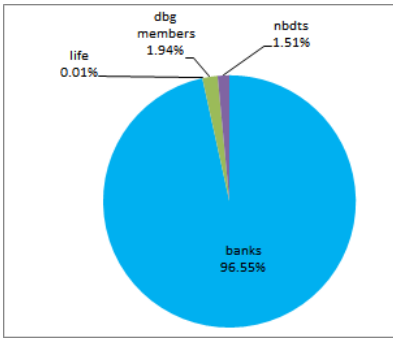
36. RBNZ has undertaken an assessment of the potential inherent ML/TF risks associated with each reporting entity that we supervise.

37. After aggregating the latest data from annual AML/CFT reports of reporting entities, we observed that NZ's registered banks handle the vast majority of the sector's transactions (see tables and diagrams below), with the large majority of transactions in the sector being domestic, rather than cross-border in nature.

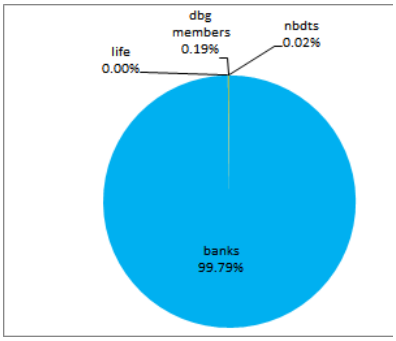
38. The information below is derived from AML/CFT Annual Report data received by the RBNZ in August 2016, for the year ending 30 June 2016.

	No. transactions processed during the year	$ transactions processed during the year	total customers
total	**4,169,293,612**	**$ 83,221,264,107,187**	**16,213,223**
banks	4,019,140,363	$ 83,033,535,695,955	11,760,415
life	345,033	$ 428,738,343	110,358
dbg members	78,235,235	$ 171,365,395,096	3,998,945
nbdts	71,572,981	$ 15,934,277,793	343,505
banks	96.40%	99.77%	72.54%
life	0.01%	0.00%	0.68%
dbg members	1.88%	0.21%	24.66%
nbdts	1.72%	0.02%	2.12%
total	**100.00%**	**100.00%**	**100.00%**

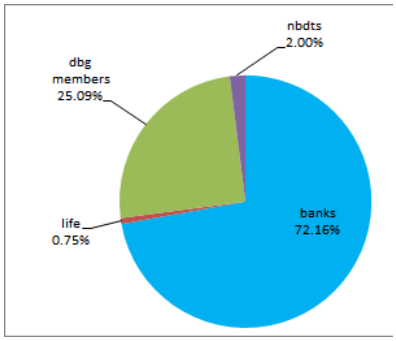
$ transactions p.a.



no. transactions p.a.



total customers



	No. transactions processed during the year	$ transactions processed during the year
International	1.44%	25.92%
domestic	98.56%	74.08%

39. RBNZ uses information taken from the AML/CFT Annual Reports to inform the nature, size and complexity section of the assessment of sub-sector risks (see Sector Risks – Banking, Sector Risks - Non-Bank Deposit Takers (NBDTs) and Sector Risks - Life Insurers).

Methodology

40. The SRA 2017 works on two distinct levels. The SRA provides an **assessment of ML/TF risk** and **identifies key potential ML/TF vulnerabilities.**

Methodology – Assessment of Risk

41. ML/TF risk for each sub-sector was assessed using the variables contained in s.58 (2)(a)-(f) of the Act and elaborated on in the Risk Assessment Guideline published by the AML/CFT Supervisors in June 2011. These variables include the nature, size and complexity of the reporting entity's business, its products/services, the channels it uses for delivery of products/services, its customer types, and the countries and institutions that it deals with. Assessing risk by these variables was done to help reporting entities use the SRA 2017 in their own ML/TF risk assessments.

42. For each of these variables a number of ML/TF factors were considered and helped guide the assessment of **inherent** ML/TF risk associated with each variable. This was done in combination with professional opinion, domestic and international guidance and the findings of the RBNZ Entity Risk Assessment (ERA). At the end of this process an overall assessment of **inherent** ML/TF risk was then assigned to each sub-sector using ratings of Low, Medium or High (see the table on page 6 of this document).

43. RBNZ decided not to consider the adequacy or effectiveness of ML/TF controls in the risk rating process and no judgements were formed on whether the risks present in a sector/sub-sector were effectively managed or mitigated. Reporting entities may have systems and controls that address some or all of the risks discussed in the risk assessment but the SRA 2017 does not identify or comment on activities undertaken by individual reporting entities.

44. The absence of an assessment of **residual** risk was a deliberate course of action designed to simplify the SRA process. Reporting entities, as part of their AML/CFT Programme, are expected to address the **inherent** risks identified in their Risk Assessment.

Methodology – Identification of Vulnerabilities

45. As part of the SRA 2017, 12 key ML/TF vulnerabilities were identified. The vulnerabilities were identified and selected during a series of RBNZ workshops based on subject matter expertise, supervision experience gained during onsite visits, and domestic and international guidance. The vulnerabilities were chosen for their commonality across RBNZ's sector and were kept few in number to assist reporting entities to understand the most significant ML/TF vulnerabilities in NZ.

Predicate Offending and STRs/SARs

46. It is important for reporting entities to understand the offending and criminal behaviour which leads to ML/TF. This is called predicate offending. However, reporting entities are not required to prove the predicate offence when investigating or reporting STRs/SARs. The FIU in its analytical work has paired the most common predicate offences and threats (domestic and international) with vulnerabilities, ML/TF phase (where applicable) and basic ML/TF typologies (see below).

Domestic

Threat		Phase	Description
Drug offending	Self- laundering; Laundering by close associates (smurfing etc.); Laundering by professional services; Possible access to international laundering networks	Predicate offending	Cash based
		Placement	Cash deposits, cash purchase of assets, cash remittance, co-mingling with business earnings
		Layering	Domestic transactions, may remit funds internationally, may use trusts, may use professional services – particularly in higher value cases
		Integration	Real estate, assets
		Other	Potentially higher value overall and more offenders involved
Fraud	Self-Laundering; Laundering by professional service providers	Predicate offending	Non-cash based
		Placement	Likely to occur through electronic transactions, potentially in the vehicle used to commit predicate offence (for example in business, company or market)
		Layering	Use of companies and business, likely to be professionally facilitated
		Integration	Real estate, assets
		Other	Potentially higher value per offender
Tax	Self-Laundering; Laundering by professional service providers	Predicate offending	Non-cash based
		Placement	Likely to occur through electronic transactions, potentially in the vehicle used to commit

Threat	Phase	Description
		predicate offence (for example in business, company or market)
	Layering	Nominees, trusts, family members or third parties etc.
	Integration	Professionals
	Other	Laundering of proceeds from tax offences
		Businesses
		Gambling

- The FIU estimates that NZD 1.35bn of domestic criminal proceeds are laundered in NZ per year. The social harm caused by the laundering and its associated offending is estimated at many times this figure.
- This estimate of domestic proceeds of crime relates principally to drug and fraud offending. The value of ML associated with tax evasion has not been established but is thought to be significant.
- The threat from drug offences results from the large volume and value of predicate offending, while the greater financial sophistication of fraud offenders leads to more complex ML which may make detection more difficult.
- Individual criminal entrepreneurs emerged as the greatest generator of proceeds of crime (both of drug crime and fraud) and as being associated with the most sophisticated ML methods.

International

Methods likely to be associated with high transnational threats		
Threat	**Specific Threats**	**Description of likely methods**
China	Drug offending connected to New Zealand	Remittance and alternative remittance; movement of funds through financial institution, designated non-financial businesses and professions (DNFBPs), businesses and assets. Trade-based laundering through merchandise trade.
	Corruption and other economic crime	Trade-based money laundering, remittance and alternative remittance, attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)

Methods likely to be associated with high transnational threats		
Australia	Organised criminal groups with trans-Tasman connections	Remittance and alternative remittance; movement of funds through financial institution, DNFBPs, businesses and assets. Trade-based laundering through merchandise trade.
	Tax evaders and other economic criminals	Trade-based money laundering using trade in services and legal structures.
Eastern Europe	Organised crime and economic criminals with no link to New Zealand	Use of legal structures and alternative payment platforms
USA	Organised crime	Remittance and alternative remittance; movement of funds through financial institution, DNFBPs, businesses and assets. Trade-based money laundering through merchandise trade.
	Economic criminals	Trade-based money laundering using trade in services and legal structures.
Terrorist financing	Groups raising capital from domestic sympathisers	Remittance and alternative remittance
South Asia and Middle East	International controllers	Remittance and alternative remittance, trade-based laundering
East and South-East Asia	Drug offenders with connection to New Zealand	Remittance and alternative remittance; movement of funds through financial institution, DNFBPs, businesses and assets.
	Economic criminals	Abuse of legal structures, movement of funds through financial institution, DNFBPs, businesses and assets, attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)

The most commonly cited estimate of the size of global money laundering is an estimate by the International Monetary Fund (IMF) to be 2-5% of global GDP.

Key Vulnerabilities – Summary

47. Key potential vulnerabilities identified in the SRA 2017 (with FIU input) impact across all of the RBNZ sub-sectors. The 12 vulnerabilities below are expanded upon in Appendices 2-13.

Vulnerability	Comment
Gatekeepers	This covers lawyers, accountants, real estate agents and other service providers. Gatekeepers are essentially those that 'protect the gates to the financial system'. Money launderers and terrorist financiers may seek out the advice or services of specialised professionals. Some ML/TF schemes have only been possible as a result of the assistance of skilled professionals to help disguise the source and ownership of funds.
Trusts and shell companies	The formation and management of legal entities and structures for ML/TF purposes is a well-recognised vulnerability. NZ's open business environment and common use of trusts is highly vulnerable to ML/TF abuse. This also includes NZ-registered offshore finance companies. All shell companies and trusts, including family trusts, should be considered highly vulnerable to ML/TF activity. Reporting entities are prohibited from establishing or continuing business relationships involving shell banks. A New Zealand person cannot provide or offer to provide financial services unless registered for that service under the Financial Service Providers (Registration and Dispute Resolution) Act 2008.
International payments	The value, volume and velocity of money moving through this channel continue to present ML/TF opportunities. Combined with other ML/TF vulnerabilities this presents a high risk of ML/TF.
Cash	Cash continues to be an easy and versatile method of transferring value. Use of money mules, cash couriers and bulk movements of cash are inherently vulnerable to ML/TF. Use of cash to purchase high value goods represents an easy method of transferring value and disguising/ concealing the proceeds of crime. Cash intensive businesses lend themselves to all phases of ML and give the impression that ML transactions are normal licit transactions. Use of cash to facilitate tax evasion, especially when combined with cash intensive businesses, is also a ML risk.
International trade and TBML	The nature, size and complexity of international trade and trade-related finance arrangements lends itself to abuse for ML/TF purposes. While not easily measurable, trade based money laundering (TBML) is believed to be occurring on a large and global scale and is difficult for authorities to combat due to its cross-border nature.
New payment technology (NPM)	Rapid development of technology may create vulnerabilities that emerge faster than ML/TF controls can respond. For instance ML/TF via internet and online banking presents a quick and easy anonymous, cross border channel which moves funds faster than enforcement can keep up with. This vulnerability also includes Alternative Banking Platforms and e-currencies.

Vulnerability	Comment
Cards	This includes credit cards, cash passports, open and closed loop cards, pre-paid cards and gift cards such as iTunes cards. This vulnerability will have some overlay with NPM.
Anonymity	Anonymity is a key vulnerability for ML/TF. This can take the form of identity fraud and false documentation, anonymous products/services, disguised beneficial ownership, persons on whose behalf a transaction is conducted, non-face-to-face Customer Due Diligence, use of intermediaries and abuse of electronic verification.
High risk customers	This category includes politically exposed persons (PEPs) and their relatives/close associates (RCAs), trusts, non-profit organisations (NPOs), high risk occupations, high risk jurisdictions, intermediaries, high value customers and people in control of multinational organisations with high risk commercial-industrial operations.
High risk jurisdictions	Countries with weak or insufficient AML/CFT measures present a clear ML/TF risk as do countries associated with high degrees of bribery and corruption, tax evasion, TF, conflict zones and organised crime. Countries which border high risk jurisdictions may also present significant risk.
Money Service Businesses (MSBs) (see Note below).	This typology is of particular concern in relation to jurisdictions with weak AML/CFT controls, jurisdictions that are conflict zones or that use methods of moving value outside of the regulations and licensing requirements of New Zealand.
ML/TF awareness	Increasing and developing knowledge of the ML/TF environment assists with AML/CFT measures. Reporting entities and AML Compliance Officers need to promote an AML/CFT knowledge culture. Training and maintaining situational awareness is important in addressing this vulnerability. In any assessment of risk, ML/TF awareness is required to ensure that assessment is valid and robust.

48. While the table provides an overview of key vulnerabilities it is important to note that they do not operate in isolation but in combination, resulting in a compounding risk of ML/TF. In addition the vulnerabilities listed do not operate within a vacuum. Context is essential in identifying and determining the degree of ML/TF vulnerability. This can be done by reporting entities when they undertake an effective risk assessment.

49. For instance, a reporting entity may be assessed as presenting a low inherent risk of ML/TF with little vulnerability as part of its ordinary course of business. However, if it does not have adequate or effective ML/TF awareness or it has exposure to cash intensive businesses it could leave itself open to criminal activity.

50. As NZ's AML/CFT environment matures it is likely that ML/TF activity may be displaced from higher risk reporting entities with strong AML/CFT controls, to those with weaker or less effective AML/CFT controls or those reporting entities outside of the Act and regulations.

51. Vulnerabilities have been colour coded for each sub-sector (see table below). Vulnerability ratings have been kept simple to assist reporting entities prioritise their responses. Reporting entities are strongly recommended to consider each vulnerability when assessing the ML/TF risk specific to their ordinary course of business; even if that business has been assessed as presenting an overall lower inherent risk of ML/TF.

Vulnerability Colour	Vulnerability Rating
	Likely to be a vulnerability for the reporting entity
	Possibly a vulnerability for the reporting entity
	Unlikely to be a vulnerability for the reporting entity

52. Where a reporting entity does not provide products/services that are open to these vulnerabilities, or they do not have certain customer or business types then the vulnerability rating will be lower. For instance, a wholesale bank which does not accept or use cash will have a very low vulnerability to cash.

53. It should be noted that RBNZ recognises that under a RBA there is no such thing as a 'zero risk' and it would be counterproductive and overly burdensome to try to attain it. The SRA 2017 should inform a reporting entity's risk management and mitigation, including risk reduction, risk prevention, risk avoidance, risk transfer, risk sharing, risk tolerance or appetite and risk retention.

54. Note: Money Service Businesses (MSBs) or Money Value Transfer Services (MVTS) are included in the list of vulnerabilities as a typology and not as an indication of the industry as a whole.

Sector Risks – Banking

Registered Banks – Overall Risk Rating

Retail	Business/commercial	Wholesale/Institutional	Overall inherent risk
High	High	Medium	High

55. See table above for the risk assessment for each of three sub-categories of banking.

56. **The ML/TF vulnerability questions posed in this section are not exhaustive and a risk assessment should be tailored to fit the reporting entity's course of business.**

57. Banks may be used at all stages of ML/TF. Because of the wide availability and ease of accessibility of products and services the banking sector, as in most other countries, is considered a primary avenue for ML/TF. In NZ the assessment of **High** risk can be attributed to the trillions of dollars and billions of transactions that flow through the banking sector to a wide variety of customers domestically and internationally. The value, volume and velocity of banking transactions provide an environment which conceals, disguises or obfuscates the proceeds of crime.

58. The **High** rating for Retail and Business/Commercial banking is consistent with domestic and international experience and expectations given their wider exposure to ML/TF vulnerabilities. The consequences of such vulnerabilities can be wide ranging and result in significant social harm, financial, reputational and even political impact. The **Medium** risk rating for Wholesale/Institutional banking reflects the sub-sectors less vulnerable products and services and relatively lower exposure to higher risk customers.

Nature, Size and Complexity

59. There are 24 registered NZ banks with nine of those operating as branches of overseas incorporated banks. The important part that registered banks play in the financial sector in New Zealand, coupled with the relative complexity of their products and business models and exposure to international financial systems, are the primary factors in the overall **High** risk rating.

60. Based on AML/CFT Annual Report data for the year to 30 June 2016 over four billion transactions were handled by NZ registered banks, representing over 95% of all transactions in the sector. The banks handled fund movements valued in excess of NZD$83 trillion, representing approximately 99% of the total funds handled across the sector.

61. Of the 24 registered banks, the five largest banks were responsible for handling approximately 90% of the volume and value of transactions during the year.

62. The five largest banks were responsible for handling approximately 80% of the value of all international payments made through any bank during the year.

63. There are over 11.7 million accounts held by individuals, families, trusts, social groups and businesses at the registered NZ banks. This represents approximately 70% of customers in the RBNZ sector.

Products and Services

64. Banks in NZ offer a wide range of products and services. In providing general banking facilities, banks offer a number of cash intensive products which have a high risk of being used to launder money. Proceeds from criminal activity have traditionally taken the form of physical currency at the placement stage of ML/TF. Placement of the proceeds of crime in the banking sub-sector also occurs when criminal proceeds can be co-mingled with legitimate business takings before depositing into accounts.

65. Cash intensive products and services include quick-drop deposit facilities (e.g. Smart ATMs), over-the-counter services such as depositing or withdrawing cash (including those by unidentified third parties), sales and purchases of foreign exchange and purchase of reloadable cash card products. Banks offer a wide range of products and services and it is beyond the remit of this assessment to list and assesses each of them. Reporting entities should assess the ML/TF vulnerabilities associated with each of their products/services and consider:

    - Are they highlighted by guidance as high risk?
    - Do they support the physical movement of cash?
    - Do they allow for international funds transfers?

Channels of Delivery for Products and Services

66. Non-face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Non face-to-face channels of delivery include internet banking, the use of intermediaries and the use of professional services/gatekeepers. Reporting entities should assess the ML/TF vulnerabilities associated with the channels of delivery:

- Do they facilitate anonymity?
- Does the channel depend on intermediaries?
- Is the channel new or untested?

Customer Types

67. Reporting entities need to be aware of the ML/TF risks associated with customers. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types. This can include certain occupations or industry links, whether they are individuals or legal persons, whether they are a Trust or if they have known criminal connections. Access to banking facilities by non-residents (see Customer Types - below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for operating an account in NZ.

68. The use of banking facilities by customers who are PEPs also heightens ML/TF risk due to their potential exposure to fraud, bribery and corruption. Likewise, high net worth customers pose a higher risk due to the larger amounts they have available to deposit or invest and the ease of fund movement through private banking type facilities. Banks in NZ offer services to all these types of customers. Also of concern is the ability of non-customers using the banking system, for example by depositing cash into accounts held by other persons or companies, or one-off transactions such as currency exchange or wire transfers.

Country Risk

69. Country risk comes from dealing with persons, entities or countries in jurisdictions with poor or insufficient AML/CFT measures. Consideration should also be given to the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition a reporting entity should consider whether the country is a conflict zone and if the country is known for the presence of, or support of, terrorism and/or organised people trafficking.

70. Information on higher risk countries can be found from a number of information sources including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC), Basel AML index, and open source media. Reporting entities will need to gain their own level of comfort when assessing country risk. AML Compliance Officers will be expected to develop and maintain situational awareness around this topic and incorporate it into the AML/CFT Programme.

Institutions Dealt With

71. Transaction accounts are maintained on a bank's behalf between domestic banks and between domestic banks and foreign banks. These accounts are used for international trade and investment, settlement, fund transfer facilities, the clearing of foreign items and to gain access to jurisdictions where a NZ bank has no physical presence.

72. International transactions have the potential to increase the risk of ML/TF occurring. Generally banks international transactions flow through **correspondent banking** (Nostro and Vostro) accounts. A variety of activities are able to be accessed through correspondent banking accounts including nested and payable- through services. This may attract criminals to set up shell companies or banks abroad to engage in those activities. International cheque processing or bundling of money orders provide opportunities for launderers to pass off transactions as those of the originating bank thus bypassing monitoring similar to retail customer accounts.

73. Nested accounts or institutions offering payable through facilities provide further opportunities to disguise the underlying customer. Such relationships may serve to shield details of individuals through the pooled accounts at the financial institution level. The risk is reduced where overseas institutions have strong AML/CFT requirements, providing the underlying customer details are not shielded by a customer acting as a nominee.

Additional Vulnerabilities or Typologies

74. These specific vulnerabilities and typologies are provided as examples. Reporting entities are expected to assess their own business specific vulnerabilities and to keep abreast of current guidance. For instance, via the RBNZ newsletter and the FIU Quarterly Typology report.

- **Deposit quick drop facilities (including Smart ATMs)** – The ease of use and anonymity afforded by these services are considered to present a high level of ML/TF risk for retail banks. This type of service has been highlighted both domestically and internationally as an area of concern. While RBNZ recognises that this service provides greater customer convenience and quicker deposit of funds the deposit of cash by unidentified persons remains a key vulnerability of this service.

- **High value dealers** – These customer types present a high ML/TF risk. Certain occupations and industries attract a higher risk rating for parts of the banking sub-sector. These customer types include a broad spectrum of occupations and industries including real estate agents, cash intensive businesses, bullion dealers, car/motorbike dealers, jewellers, and higher risk global industries such as arms manufacturing and commodity mining.

Sector Risks - Non-Bank Deposit Takers (NBDTs)

Non-Bank Deposit Takers – Overall Risk Rating

Deposit taking finance companies	Building Societies and Cooperatives	Credit Unions	Overall inherent risk
Low	Medium	Medium	Medium

75. See table above for the risk assessment for each of three NBDT sub-categories.

76. The **Low** risk rating for deposit taking finance companies recognises that they do not typically have the cash intensive products and services that other sub-sectors may have, but they do have a reasonable level of transactions by value and volume. Building societies and cooperatives operate in a similar way to registered banks hence the **Medium** risk rating, although international transactions are rated as a lower ML risk for this sub-sector. Credit unions are rated as having a **Medium** risk of ML. While domestically focussed they are exposed to domestic ML/FT risks and high risk customers and in some instances operate at similar or higher volumes of transactions as a small bank.

Nature, Size and Complexity

77. The prudential regulation of NBDTs is carried out under the Non-bank Deposit Takers Act 2013 and associated regulations. NBDTs are entities that make regulated offers of debt securities (as defined in the Non-bank Deposit Takers Act 2013) and who carry on the business of borrowing and lending money or providing financial services, or both. Many NBDTs operate in a similar nature to registered banks by providing a range of financial services including accepting deposits and lending funds. (Non-deposit taking finance companies are covered in the SRA produced by the DIA).

78. Currently there are 26 registered NBDTs. This includes NZ building societies, deposit-taking finance companies, and credit unions.

79. According to AML/CFT annual reports, NBDTs handled over 71.5 million transactions during the year to 30 June 2016, valued at approximately $15.9 billion. Over 343,000 customer accounts were counted by the NBDTs.

80. Despite the large size of some of the credit unions and finance companies, the NBDT sub-sector constitutes a very small portion of the RBNZ sector in terms of annual turnover values.

Products and Services

81. Deposit taking finance companies receive a lower risk rating due to less exposure to cash intensive products and services. A number of the deposit taking finance companies are specialist lenders in areas such as rural finance, asset based lending or property finance. Funds loaned or received through products such as debentures, are likely to be through electronic means rather than physical cash.

82. Building societies and credit unions offer a similar range of cash intensive products and services to the core activities of retail banks. Products identified in the NBDT sector for over-the-counter services include depositing of cash, foreign exchange business and the purchase of reloadable cashable cards. The potential misuse of general deposit type accounts for the purposes of ML/TF at NBDTs are similarly to the risks in the banking sector. Term deposit accounts are lower risk products due to the inflexible nature of completing deposits and withdrawals which may mean the proceeds of crime are not immediately available.

83. International transactions make up a relatively small proportion of transactions in the NBDT sub-sector. The number of transactions with overseas institutions through deposit taking finance companies is higher than in building societies and credit unions. This is mainly from payments being made to other countries rather than receipt of funds into NZ. That said, international funds are accepted into New Zealand via the NBDT sector.

84. Although wire transfers in the NBDT subsector are generally completed through NZ banks or money remittance services, the receipt and payment of funds by wire transfer through NBDTs is still a risk. Wire transfer transactions on behalf of non-customers also increase ML/TF risk where due diligence has not been undertaken or a profile of expected transactions has not been established. The DIA address similar risks in its SRA in relation to money remittance services.

85. Personal and business lending, including property or asset finance lending, are not often perceived as risky areas for ML/TF in the industry but can be higher risk activities. Criminals can obtain a loan by fraudulent means then pay off the loan with the proceeds of crime making the loan appear legitimate. The funds from the loan may then be used however the criminal wishes.

86. In addition there is a risk that assets purchased with illicit funds may be used as security to obtain clean funds/loans from reporting entities in this sub-sector. Alternatively illicit funds or criminal proceeds may be used for early repayment of a loan funding a legitimate asset purchase. The opportunity for ML/TF in this area occurs where loan repayments are able to be made in cash, where third party payments are made and where the source of funds for cash payments is unclear.

87. Deposit taking finance companies are involved in a significant proportion of lending activities, including property finance and leasing of high value machinery or other assets. Personal and mortgage lending are common in retail banks and NBDTs.

88. The FMA has produced an SRA that covers ML/TF risks associated with the issuing of securities. Securities offered in the NBDT sector include debenture stock, subordinated notes, preference shares, or term and redeemable shares. Substantial amounts can be invested through investment products. The risks associated with these types of securities are reduced by the length of time the instrument is usually held. The ability to sell or exchange the security increases the ML/TF risk. Factors that make this area of business riskier for ML/TF purposes are where the purchase of these products is able to be made using cash and/or where the items are held by the customer for short periods of time prior to maturity.

Channels of Delivery

89. Non-face-to-face application for, and delivery of, products/services is regarded as being more vulnerable to ML/TF activity than face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with the channels of delivery (see Sector Risks – Banking). Non face-to-face channels of delivery include the use of intermediaries, use of the internet, brokers and the use of professional services/gatekeepers.

Customer Types

90. NBDT reporting entities should ask themselves about the ML/TF vulnerabilities associated with particular customer types (see Sector Risks – Banking).

91. Building societies and credit unions require membership of the entity for customers to access services. Credit unions include small community or industry organisations and generally focus on the supply of financial services to members associated with a particular community, geographical location, or employer. Despite membership requirements NDBTs still need to be aware of domestic risks and the risks presented by PEPs, non-residents customers and organisations such as trusts, charities and non-profit organisations.

92. NBDTs should be wary of illicit funds being mingled with legitimate proceeds of business or personal wealth sources by any customer type. This is particularly pertinent when considering the predicate offence of tax evasion.

Country Risk

93. A significant proportion of transactions (over 95% for both value and volume) in the NBDT sector are domestic payments. The majority of customers are likely to be NZ resident individuals, although some overseas resident customers are to be expected resulting in overseas payments. Onsite supervisory visits and annual report data suggest international transactions account for only a minimal percentage of the volume and value of transactions in the NBDT sector.

94. International transactions make up a very small proportion of transactions in the NBDT subsector. The number of transactions with overseas institutions through deposit taking finance companies is higher than in building societies and credit unions. This is mainly from payments being made to other countries rather than receipt of funds into NZ.

Institutions Dealt With

95. NBDTs normally have relationships with banks to facilitate transactions.

Sector Risks - Life Insurers

Life Insurers – Overall Risk Rating

Life Insurers	Overall inherent risk
Low	Low

96. Life insurance has one single overall risk rating.

97. The RBNZ is the prudential regulator and supervisor of all insurers carrying on insurance business in NZ, and is responsible for administering the Insurance (Prudential Supervision) Act 2010. RBNZ is also the AML/CFT supervisor for the life insurance part of this sub-sector. Life insurers are assessed as lower risk entities for AML/CFT purposes. However, certain life insurance policies, typically those with a cash surrender value or investment features, are potential ML/TF vehicles. There is currently little evidence of ML at present in the form of STRs although limited reporting is not necessarily an indication that ML is not taking place.

98. FATF has produced a document for the Insurance Sector called 'Risk-based approach Guidance for the Life Insurance Sector' October 2009. Reporting entities in the Insurance sub-sector are recommended to reference this document as part of their AML/CFT risk assessment and programme. Reporting entities should also consider reviewing the SRA produced by the FMA for additional information on the risks associated with investment schemes.

Nature, Size and Complexity

99. Assessment of risk in the life insurance subsector mainly focuses on ML. The sub-sector is predominantly made up of limited liability companies with both small and medium scale operations. A number of businesses in this sector have some relationship with either another insurer or another financial institution. Many of them are also branches or affiliated with an insurance entity based overseas.

100. A few Life Insurers operate as general insurers as well. However, general pure risk insurance is currently excluded from the obligations of the Act. The AML/CFT Regulations also allows some exemptions for certain types of products or transactions. Reporting entities should seek independent advice if they are unsure whether the exemptions apply to all, or part, of their business.

101. There are over 30 licensed insurers that carry on life insurance business in New Zealand. During 2016, the majority of these were able to apply one or more exemptions in the AML/CFT Regulations, in order to reduce unnecessary compliance costs for low risk services. After taking into account the exemptions, nine life insurance providers were captured by the Act during 2016.

102. Annual report data indicates approximately 429,000 transactions were handled during the year to 30 June 2016. This illustrates that only a small number of life insurance providers are wholly captured by the Act, and these reporting entities therefore constitute a small portion of the RBNZ's reporting entities.

Products and Services

103. The use of the life insurance industry for ML/TF is more likely at the layering and integration phase of the money laundering cycle rather than placement. Suspicion may be raised at the time of commencing the policy, during the life of the policy when premium payments are made or when payment is made by the insurer. Life insurance may be attractive to launderers as the resulting payments from insurers may attract less attention than receiving large payments from other sources. There is also significant integration with other parts of the financial sector with the potential to use facilities to make and receive payments.

104. Singular large initial policy payments, multiple payments from unrelated/unknown sources and on-going premium payments (domestic and international) can increase the ML/TF risk. This may be intensified where payments are made periodically in addition to those expected when setting up the policy. Furthermore, if over-payments are made, there is potential for the additional funds to be reclaimed as clean funds from the insurer. Excessive payments (including by third parties) on policies or accounts that are close to maturity should raise questions.

105. The risk of investment components in life insurance products being exploited by criminals comes from a number of factors. Most notable is the ability to build up a cash value on the policy that can be redeemed. Surrendering such policies allows access to legitimised funds that may not raise questions from external parties.

106. Because of the economic value of certain products they may potentially be used as collateral for accessing legitimate funds or loans from financial institutions. Suspicion may be triggered where any requests are made for confirmation or certification that funds are invested with an insurer.

Channel of Delivery

107. Of particular concern in the ML/TF context is the way customers can access products and services in the life insurance industry through indirect distribution channels. The provision of products to customers via intermediaries, and other methods where the policy issuer does not have face-to-face contact with the customer, has anonymity risks.

Customer Types

108. A factor that may increase the ML/TF risk is that the policyholder/customer may not be the ultimate beneficiary of the policy. The beneficiary of the policy may sometimes be changed during the life of the policy and this may not be known until payment is required. There is also potential for a secondary market in life insurance policies whereby policy owners can sell the benefit of the policy to a third party.

109. Third parties may be involved in the payment of premiums or at maturity of the policy. With payment of premiums, concerns may be raised where there are multiple sources contributing to the premium payments of a customer. The risk is further heightened where the premium payments are significant in value, particularly where this does not correspond to the profile of the customer.

Country Risk

110. A significant proportion of transactions in the life insurance sector are domestic payments. The majority of policy holders are likely to be NZ resident individuals though some overseas resident policyholders are to be expected resulting in overseas payments. AML/CFT Annual Report data suggests that during the year to 30 June 2016 international transactions accounted for less than 1% of the volume and value of transactions in the life insurance sector.

Institutions Dealt With

111. The FATF has indicated that the **reinsurance industry** is a potential area for enabling ML. For instance, new or existing life insurance and reinsurance businesses may be set up by launderers to conceal criminal proceeds. This is done through the provision of policies to associates and the reinvesting of those illicit funds in reinsurance contracts. Both the insurance and reinsurance company may have been established or used as a cover for ML with the proceeds of crime mingled with legitimate business activities.

112. The risk of ML in the life insurance sector increases when transactions take place with insurance and reinsurance entities where the ownership appears to be obscured or the authenticity of the business may be questioned.

Specific Vulnerabilities or Typologies

113. RBNZ is unable to comment on every individual or specific product and service. Reporting entities should consider how the risk of ML/TF translates to their own products, services and channels in their own risk assessment. A non-exhaustive list of red flags for life insurers includes:

- The early termination of an insurance product, especially at a cost to the customer (while this may be common it should be considered in combination with other red flags);
- Use of a 'free look period' to return premiums within a set number of days;
- Making over-payment/s on a policy, then asking for a refund especially if directed to an apparently unrelated third party or unfamiliar bank account;
- The transfer of the benefit of an insurance product to an apparently unrelated beneficiary;
- The purchase of an insurance product that appears to be inconsistent with a customer's needs;
- A customer who wishes to fund its policy using pay¬ments from a third party or from another country, particularly high-risk jurisdictions;
- Any unusual method of payment, particularly by cash or cash equivalents;
- The purchase of an insurance product with structured amounts;

- The reluctance by a customer to provide identifying information when purchasing an insurance product, or the providing of minimal or seemingly fictitious information;
- Paying a large "top-up" into an existing life insurance policy;
- A customer who usually purchases small policies, sud¬denly requests a large lump-sum contract;
- Purchasing one or more single-premium policies, then cashing them in a short time later;
- Premiums being paid into one policy, from different sources;
- Customer is more interested in learning about cancellation terms than the benefits of the policy;
- Channelling payments via offshore banks; and
- Purchasing policies which are inconsistent with the buyer's age, income, employment or history.

Terrorism Financing (TF)

114. The terrorism threat that New Zealand itself faces is rated as 'low' by the international community. However, the FIU reports that NZ is still exposed to threats relating to TF overseas, including the potential for financiers of overseas groups within NZ, and overseas based groups who may seek to use NZ as a conduit for funds. The FIU have produced a QTR on this topic.

115. Despite the low levels of TF risk it is prudent for all RBNZ reporting entities to consider the potential vulnerabilities associated with TF and the potential red flags that may indicate TF activity.

116. TF funding covers a wide range of terrorism related activity including operational funds, equipment, salaries and family compensation, social services, propaganda, training, travel, recruitment and corruption. **It is not necessary for reporting entities to identify the purpose of TF. Any potential TF related information must be reported to the FIU as soon as possible. RBNZ reporting entities reporting TF activity must ensure it is accurate, timely and treated with urgency and sensitivity.**

117. RBNZ reporting entities should consider not only high risk countries but also their neighbouring countries as TF often involves the movement of funds across borders. For instance, the UK NRA 2015 identifies Turkey, East Africa (especially areas surrounding Somalia) and the Persian Gulf as TF transit countries/regions. As such in this section the term 'high risk jurisdictions' covers both high TF risk countries and their neighbours. Reporting entities may find it useful to access other overseas guidance on this topic. For example AUSTRAC's 'Building a profile – Financial characteristics associated with known foreign terrorist fighters and supporters.'

Nature of TF

118. The characteristics of TF can make it difficult to identify. Transactions can be of low value, they may appear as normal patterns of behaviour and funding can come from legitimate as well as illicit sources. However, the methods employed to monitor ML can also be applicable for TF as the movement of those funds often relies on similar methods to ML.

119. Internationally the TF process is considered to typically involve three stages:

- raising funds (through donations, legitimate wages, selling items or criminal activity);
- transferring funds (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell); and
- utilising funds (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses).

120. Given the global nature of TF and the constantly changing nature of international tensions and conflicts, the risks associated with TF are highly dynamic. As such, reporting entities need to ensure that their CFT measures are current, regularly reviewed and effective. It is important that reporting entities maintain situational awareness and effective transaction monitoring (TM) systems which incorporate dynamic TF risks as well as the more static risks associated with ML.

121. The value of funds moved through the international system in connection to TF is likely to be much lower than other forms of illicit fund flows. However, if funds connected to TF were to be associated with NZ financial institutions it would likely have a disproportionate effect on NZ's reputation rather than financial integrity. In addition, outside of the obvious harm caused by TF, any NZ reporting entity associated with this activity would be subject to reputational repercussions and could be subject to potential civil and even criminal sanction.

NZ Banking Sub-Sector as Conduit for TF

122. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorist financiers. Overseas groups may seek to exploit NZ as a source or conduit for funds to capitalise on NZ's reputation as being low risk for TF. For instance, funds originating in or passing through NZ may be less likely to attract suspicion internationally.

123. The banking sub-sector continues to be the most reliable and efficient way to move TF funds. TF through the banking sector can be small-scale and indistinguishable from legitimate transactions. TF could involve structured deposits of cash into bank accounts followed by wire transfers out of NZ. It could also involve banks being used by remittance agents to send funds overseas. More complex methods could see NZ business, NPO and charity accounts being used as fronts for sending funds offshore through the banking sector. Stored value cards (including credit cards or cash passports) can be used to courier or access cash overseas, especially cards which enable withdrawals from international ATMs or allow multiple cards to be linked to common funds (see TF Indicators and Warnings (I&W) section below for further red flags).

124. Given the difficulty with detecting TF, reporting entities' TM systems and procedures (manual and electronic) play a key role in detecting TF activity. Furthermore the banking sector's knowledge of their customers and their customer's expected financial transaction activity is vital in determining whether or not TF activity is potentially taking place.

NBDT and Insurers

125. This subsector shares many of the vulnerabilities of the banking sector (refer above) with the potential to be perceived as an easier avenue for TF due to assumptions by criminals that they have less developed CFT measures. There is little domestic or international evidence to link life insurance products with TF. However, there is overseas reporting that links simulated traffic accidents and associated insurance compensation (life and general insurance) with TF.

Money Service Businesses (MSB)

126. MSBs are recognised internationally as presenting TF risk and RBNZ reporting entities should be aware of the risks associated with them. To some extent MSBs offer a degree of anonymity (refer: paragraph 47 of this document) and an easy method of moving funds to countries that may have little or no formal banking structure, high levels of corruption and poor CFT measures. **However, many communities and countries rely on the flow of funds using MSBs and AML/CFT responses to the risks presented by MSBs should be proportionate and reflect RBA**. This reflects the official RBNZ statement on this topic dated 28 January 2015.

Non-Profit Organisations (NPO) and Charities

127. The use of NPOs and charities is an internationally recognised TF typology. NPOs can be used to disguise the movement of funds to high-risk regions and funds raised for overseas humanitarian aid can be co-mingled with funds raised for TF. NPOs can also easily and legitimately access materials, funds and networks of value to terrorist groups. In addition, funds sent overseas by charities with legitimate intentions can also be intercepted when they reach their destination country.

128. The FATF report that NPOs most at risk of abuse are those engaged in 'service' activities which are operating in close proximity to an active terrorist threat. Funds sent to high risk jurisdictions for humanitarian aid are at increased risk of being used for TF if they are sent through less-established or start-up charities and NPOs. Some donors may willingly provide donations to support terrorist groups, while other donors, and the charities themselves, may be coerced, extorted or misled about the purpose of funding. However, it is important to consider this TF vulnerability in the context of the NZ environment and that this will not apply to the vast majority of NZ charities and NPOs.

Cash Couriers

129. TF risk associated with cash couriers is assessed internationally as high. This method of TF may be undertaken by multiple individuals and involve smuggling cash across porous borders to high risk TF jurisdictions. Bulk cash smuggling can also be utilised. To this end the presence of high value bank notes, such as the 500 euro note, which facilitates the easy transportation of large amounts of funds, may be an indicator of TF (as well as ML). For example, the 500 euro note was removed from sale in the UK due to its overwhelming use in organised crime.

NZ Shell Companies

130. The FIU reports that overseas groups have demonstrated a desire to use NZ shell companies for activities similar to TF (see below). As such RBNZ reporting entities should not immediately discount NZ companies from suspicion of TF as a matter of course. For instance in 2009 NZ shell companies were connected to an attempt to ship arms from North Korea in violation of UN sanctions. It is suspected that the arms in this case were en route to Iran and potentially destined for use by one of Iran's paramilitary/insurgent customers.

FATF and TF

131. TF continues to be a priority issue for FATF. They have published numerous papers on the topic including; *Terrorist Financing typologies report* (2008), *Terrorist Financing in West Africa* (2013), Risk of Terrorist Abuse in Non-Profit Organisations (2014) and *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* in 2015. This attention reflects global concern and signals the need for RBNZ reporting entities to give TF due consideration in their assessment of ML/TF risk.

TF Indicators and Warnings (I&W)

132. ML and TF share many I&W or red flags. The following I&W may assist reporting entities in the difficult task of drawing a link between unusual or suspicious activity and TF. The list is not exhaustive and RBNZ reporting entities are encouraged to identify I&W which may occur in their course of business as part of their risk assessment.

- Red flags which may occur within the RBNZ sector include:
- Structured cash deposits and withdrawals along with IFTIs to high-risk jurisdictions, potentially at multiple branches of the same reporting entity;
- Multiple customers and/or occasional transactions by non-customers conducting IFTIs to the same beneficiary located in a high-risk jurisdiction;
- A customer conducting fund transfers to multiple beneficiaries located in high-risk jurisdictions;
- A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions;
- Transfer of funds between business accounts and personal accounts inconsistent with the type of account held and/or the expected transaction volume for the business;
- Large cash deposits and withdrawals to and from NPO accounts;
- Individuals and/or businesses transferring funds to listed terrorist entities or entities reported in the media as having links to terrorism or TF;
- Funds transfers from the account of a newly established company to a company selling dual use items (see Proliferation and Dual Use Items below, and Appendix 14:);
- Multiple low-value domestic transfers to a single account and cash deposits made by multiple third parties;
- A sudden increase in account activity, inconsistent with customer profile;

- Multiple cash deposits into personal account described as 'donations' or 'contributions to humanitarian aid' or similar terms;
- Transfers through multiple accounts followed by large cash withdrawals or outgoing fund transfers overseas;
- Multiple customers using the same address/telephone number to conduct account activity;
- Proscribed entities or entities suspected of terrorism using third-party accounts (for example, a child's account or a family member's account) to conduct transfers, deposits or withdrawals;
- Use of false identification to establish NZ companies;
- Pre-loading credit cards, requesting multiple cards linked to common funds or purchasing cash passports/stored value cards prior to travel in order to courier cash overseas;
- Customers taking out loans (banks and NBDT) and overdrafts with no intention or ability to repay them or using fraudulent documents;
- Customers emptying out bank accounts and savings;
- Customers based in or returning from conflict zones;
- Evidence of payments from insurance fraud simulating traffic accidents; and
- Customers converting small denomination bank notes into high denomination notes, potentially in a different currency (especially US Dollars, Euro's or Sterling).

Emerging TF Risk

133. FATF has highlighted the need for forward looking analysis in respect to TF given the dynamic risk environment. Areas of potential risk are:

- Foreign terrorist fighters (FTFs) and Foreign Terrorist Supporters (FTSs)
- Fundraising through social media and new payment products and services
- Exploitation of natural resources

134. The extent to which these avenues have been exploited for TF purposes is unclear and, while these activities may not have an immediate association with RBNZ reporting entities, their potential impact on TF should be noted.

135. The dynamic nature of the TF environment necessitates that reporting entities, especially in the banking sub-sector due to its global reach and ease of fund transfers, should ensure that their AML Compliance Officers maintain situational awareness in relation to this topic. Reporting entities should also ensure that, in the face of evolving TF typologies, their AML/CFT measures are both adequate and effective. This should be reflected in relevant AML/CFT documentation and evidenced by regular testing and validation. While the likelihood of TF in NZ may be small compared to other jurisdictions the consequences of such activity remain significant.

Proliferation and Dual Use Items

136. Since RBNZ's first edition of the SRA in 2011, the FATF have revised their AML/CFT Recommendations to cover not only AML/CFT but also the financing of the proliferation of weapons of mass destruction. There is currently no evidence to suggest that RBNZ reporting entities are involved in financing proliferation activities. However, included in 'proliferation' are dual use items or technologies and NZ is not immune from abuse in this sector. While having a very low likelihood of occurrence the potential consequences, as with TF, could be catastrophic.

137. Dual use items are also called 'strategic' or 'controlled goods' and can be used for both peaceful and military aims. Many of these items can be produced, sourced and manufactured in NZ. Such items may not be exported from NZ unless an export licence or permission has been obtained from the Secretary of Foreign Affairs and Trade. A list of strategic goods can be found on the Ministry of Foreign Affairs and Trade (MFAT) website and the Security Intelligence Service (SIS) have produced a booklet on the topic at nzsis.govt.nz/assets/media/NZSIS-WMD-pamphlet.pdf.

138. RBNZ reporting entities, where relevant to their course of business, need to be aware of the wider proliferation context when considering their AML/CFT measures. In particular this may have an overlap with sanctions requirements. Appendix 7 contains a FATF-sourced table of general dual-use items and proliferation risk factors which may be encountered by reporting entities.

Appendix 1: Typology Summary

Typologies, or methods and techniques, of ML/TF are many and varied. Some of the more robust and recognised typologies are included in the table below and are taken from the FIU and APG research documents. The list is not exhaustive and it is recommended that reporting entities and their AML Compliance Officers make themselves familiar with the typologies that impact on their course of business.

Bribery and Corruption	Association with corruption (bribery, proceeds of corruption & instances of corruption undermining AML/CFT measures): Corruption (bribery of officials) to facilitate money laundering by undermining AML/CFT measures, including possible influence by politically exposed persons (PEPs)- e.g. investigating officials or private sector compliance staff in banks being bribed or influenced to allow money laundering to take place.
Cash conversion/ currency exchange	Currency exchanges / cash conversion: used to assist with smuggling to another jurisdiction or to exploit low reporting requirements on currency exchange houses to minimise risk of detection - e.g. purchasing of travellers cheques to transport value to another jurisdiction.
Cash couriers	Cash couriers / currency smuggling: concealed movement of currency to avoid transaction / cash reporting measures.
Structuring	Structuring (smurfing): A method involving numerous transactions (deposits, withdrawals, transfers), often various people, high volumes of small transactions and sometimes numerous accounts to avoid detection threshold reporting obligations.
Cards	Use of credit cards, (and also cheques, promissory notes etc): Used as instruments to access funds held in a financial institution, often in another jurisdiction.
High value items	Purchase of portable valuable commodities (gems, precious metals etc.): A technique to purchase instruments to conceal ownership or move value without detection and avoid financial sector AML/CFT measures – e.g. movement of diamonds to another jurisdiction.
High value assets	Purchase of valuable assets (real estate, race horses, vehicles, etc.): Criminal proceeds are invested in high-value negotiable goods to take advantage of reduced reporting requirements to obscure the source of proceeds of crime.
Commodity exchanges	Commodity exchanges (barter): Avoiding the use of money or financial instruments in value transactions to avoid financial sector AML/CFT measures - e.g. a direct exchange of heroin for gold bullion.
Wire transfers	Use of Wire transfers: to electronically transfer funds between financial institutions and often to another jurisdiction to avoid detection and confiscation and to lengthen the audit trail.

Underground banking/ Alternative remittance	Underground banking / alternative remittance services (hawala/hundi etc.): Informal mechanisms based on networks of trust used to remit monies. Often work in parallel with the traditional banking sector and may be outlawed (underground) in some jurisdictions. Exploited by money launderers and terrorist financiers to move value without detection and to obscure the identity of those controlling funds.
Trade based ML	Trade-based money laundering and terrorist financing: usually involves invoice manipulation and uses trade finance routes and commodities to avoid financial transparency laws and regulations.
Gambling	Gaming activities (casinos, horse racing, internet gambling etc.): Used to obscure the source of funds – e.g. buying winning tickets from legitimate players; using casino chips as currency for criminal transactions; using online gambling to obscure the source of criminal proceeds.
NPOs	Abuse of non-profit organisations (NPOs): May be used to raise terrorist funds, obscure the source and nature of funds and to distribute terrorist financing.
Capital Markets	Investment in capital markets: to obscure the source of proceeds of crime to purchase negotiable instruments, often exploiting relatively low ML/TF reporting requirements.
Co-mingling	Co-mingling (business investment): A key step in money laundering involves combining proceeds of crime with legitimate business monies to obscure the source of funds.
Shell companies	Use of shell companies/corporations: a technique to obscure the identity of persons controlling funds and exploit relatively low reporting requirements.
Offshore businesses	Use of offshore banks/businesses, including trust company service providers: to obscure the identity of persons controlling funds and to move monies away from interdiction by domestic authorities.
Trusts	Use of nominees, trusts, family members or third parties etc.: to obscure the identity of persons controlling illicit funds.
Foreign banks	Use of foreign bank accounts: to move funds away from interdiction by domestic authorities and obscure the identity of persons controlling illicit funds.
ID fraud	Identity fraud / false identification: used to obscure identification of those involved in many methods of money laundering and terrorist financing.
Gatekeepers	Use "gatekeepers" professional services (lawyers, accountants, brokers etc.): to obscure identity of beneficiaries and the source of illicit funds. May also include corrupt professionals who offer 'specialist' money laundering services to criminals.
New payment technology	New Payment technologies: use of emerging payment technologies for money laundering and terrorist financing. Examples include cell phone-based remittance and payment systems.

Appendix 2: ML/TF Vulnerabilities[1]

Gatekeepers

Comment

- Professional 'gatekeepers' such as lawyers, accountants, trust and company service providers (TCSPs) and real estate agents have long been identified as a ML/TF vulnerability. In addition, the consequences if professional services are being abused by ML/TF have the potential to be high. Currently only TCSPs are covered by the AML/CFT Act 2009 (see Trusts and Shell Companies section).Trusts and Shell Companies
- Lawyers, accountant's real estate agents and other service providers currently remain outside the AML/CFT Act and are particularly vulnerable to ML/TF abuse. Phase 2 of the AML/CFT Act should rectify this position.
- The involvement of a professional gatekeeper can provide launderers with the impression of respectability, legitimacy and/or normality especially in large transactions. It also provides a further step in the laundering chain which frustrates detection and investigation.
- Professionals may also allow launderers to access services and techniques that they would not ordinarily have access to. This may be as simple as making introductions (e.g. to open an account) or facilitating setting up structures such as trusts.
- Vulnerabilities in the legal profession (which also apply to accountants) include the use of client accounts, trust accounts, purchase of real estate (this would also apply to other purchases of large assets and businesses), creation of trusts and companies, management of trusts and companies, setting up and managing charities and managing client affairs. While each of these areas are legitimate services these services may be exploited by money launderers and/or terrorist financiers.
- The use of intermediaries, such as brokers, present a number of ML/TF vulnerabilities. The increased risk stems from the ability of intermediaries to control the arrangement and the sales environment in which they may operate.
- Use of intermediaries may also circumvent some of the due diligence effectiveness by obscuring the source of the funds from third parties. For some reporting entities, the use of intermediaries may be their sole distribution channel and for others it may account for an increasing market share leaving them open to ML/TF risk.
- FIU analysis indicated that 26% of Asset Recovery Unit cases involved gatekeepers. However, while these cases were a minority of the cases, they accounted for over 62% of the value of the assets restrained in the sample of cases.
- The FIU also reports on the attractiveness of the real estate sector to money launderers. The value of the sector, the volume of sales and the low level of detection capacity make the real estate sector highly vulnerable to layering and integration of criminal proceeds.
- The FIU highlighted this vulnerability (ML/TF through professional's client accounts and ML/TF through the use of 3rd party intermediaries) in two QTRs which can be found on their website.

[1] The vulnerabilities listed here are derived from number of sources. The vulnerabilities are based on the knowledge and experience of the RBNZ AML team in conjunction with information from the FIU , SRA's from the NZ AML/CFT Sector Supervisors and international guidance from the FATF/APG and comparable jurisdictions (for example AUSTRAC, FinCEN, FinTRAC, UK FCA) in addition to open source media.

Appendix 3: Trusts and Shell Companies

Comment

- The attraction of trusts is their ability to hide beneficial ownership or involvement of criminals in transactions and to create a front behind which criminals may mask their activity.
- Using shell companies to conduct ML transactions assists criminals to conceal the involvement of natural persons as the company conducts transactions while beneficial ownership or effective control of the company is hidden behind nominee directors and/or shareholders. Reporting entities are prohibited from establishing or continuing business relationships involving shell banks..
- NZ company structures and trusts are attractive to launderers as NZ's reputation as a well-regulated jurisdiction may provide a veneer of legitimacy and credibility. It is easy and inexpensive to register companies and set up trusts in NZ which are essentially disposable and cheaply replaceable. In addition, registration on the Financial Service Provider Register (FSPR) provides a veneer of legitimacy but creates no requirement to adhere to AML/CFT requirements.
- At the integration phase, trusts can be an effective means of dispersing assets while retaining effective control and enjoying the proceeds of criminal offending.
- During layering, trusts and other legal entities may be used to create complex legal structures. Such legal structures obscure the involvement of the natural persons connected to the predicate offending. Trustees may be used as intermediaries in laundering transactions, which may allow especially complex and effective laundering where the trustee service is provided by professional service providers.
- NZ's settlor-based tax regime also makes NZ foreign trusts (offered to overseas customers as an asset protection vehicle) an attractive vehicle for tax evasion. This market offers opportunity for money launderers and tax evaders to layer or hold assets in NZ trusts.
- NZ's foreign trusts are vulnerable to tax evasion and ML. They can be used as a vehicle for international transactions by an overseas launderer giving the appearance of a transaction involving NZ. This may make the transaction appear benign by trading on NZ's reputation, or may simply obscure the money trail by adding the complexity of tracing money internationally.
- Of particular note are NZ-registered Offshore Finance Companies which present a ML/TF vulnerability and should be subject to close attention. The FIU notes that NZ-registered companies, often those acting as alternative banking platforms, have been implicated in numerous incidents of international offending.
- The FIU notes that trusts are used to attempt to hide and protect the ownership of property by offenders and that bank accounts held for the trust receive criminal proceeds which are used to repay mortgages on the property. Trusts were especially popular in drugs cases and were most commonly abused by criminal entrepreneurs, although they were also used in several organised crime cases. In a sample of Asset Recovery Unit cases analysed by the FIU,

46% of cases, representing 50% of the value of restrained assets in the sample, involved trusts.

- The FIU highlight this vulnerability in two QTRs which can be found on their website.
- Given all the above all shell companies and trusts, including foreign and family trusts, should be considered highly vulnerable to ML/TF activity.

Appendix 4: International Payments

Comment

- International payments through the mainstream financial sector appear to be the primary means for launderers and terrorist financiers to move illicit funds offshore. This movement of funds can constitute either layering or integration. In addition, they can constitute placement of cash proceeds of crime, especially in the case of remitters.
- Transactions involving countries with limited or no ML/TF controls will present a higher risk. The use of wire transfers to move funds cross-border relatively quickly is recognised internationally as one of the most common methods to launder funds.
- Wire transfers between jurisdictions can obscure the source of funds, particularly where information on the originator of the transaction is incomplete or absent. Whilst international wire transfers are more likely to attract suspicion, domestic transfers are not free of risk.
- Moving funds transnationally may allow criminals to complicate investigations by creating a complex money trail and creating jurisdictional hurdles for law enforcement agencies. Transactions, including occasional transactions, may be structured below reporting/identification thresholds to avoid detection.
- ML/TF via international payment may be easily combined with other ML/TF methods such as trade-based laundering, use of professional services, use of intermediaries and the use of trusts and companies.
- Entities engaged in international payments are often involved in foreign currency exchange and accept cash. Some entities conducting international payments, such as brokers, may be perceived as prestigious and therefore low risk.
- International payments may facilitate the use of money mules to create layers and obscure the money trail. For example, transnational payments to a money mules' account followed by cash withdrawal and the remittance of that cash.
- Payments between companies for goods or services may facilitate the flow of funds between criminals in different jurisdictions and or create layers in laundering or terrorist financing schemes (see International Trade and Trade Based Money Laundering (TBML) section).
- ML/TF risks may relate to the jurisdictions the wire transfer comes from or passes through as well as the parties to the transaction and the accompanying information message.
- Transactions through NZ may be one of many stops in a transaction path in an effort to disguise the country of origin and give the appearance of clean funds from a lower risk jurisdiction. Risks may include opportunities for deletion or substitution of information in the corresponding message to circumvent ML controls.
- Money launderers may use NZ businesses to move funds in order to escape detection in their own jurisdiction. Third parties may be based in overseas locations with reduced or no ML/TF requirements. Some countries also have secrecy laws or conventions that prevent the underlying beneficiary or source of funds being identified.
- Premium payments made via companies in offshore financial centres may shield the origin of the funds. Similarly requests for redemption of products by an organisation or person in another country may cause suspicions.
- The FIU highlighted this vulnerability (wire transfers) in a QTR which can be found on their website.

Appendix 5: Cash

Comment

- Citing Payment NZ analysis, the FIU reports an increased circulation of high value cash, concurrent with declining use of cash in retail, but increased use in the hidden economy. In addition, the FATF continue to highlight ML through the physical transportation of cash as a key typology.
- Crime such as drug dealing and converting stolen property generally generates proceeds of crime in cash. Cash remains popular for ML/TF activity as it:
  - is anonymous and does not require any record keeping
  - is flexible allowing peer to peer transactions
  - can be used outside of formal financial institutions
  - stores the value of the proceeds of crime outside of the financial sector
  - facilitates the transfer of proceeds – either between parties or geographical locations
- Cash does have some disadvantages due to its bulk and need to be physically transported. In addition it is likely to increase the risk of detection – either through arousing the suspicion of financial institutions (as large cash transactions are uncommon and often associated with illicit purchases) or being discovered by authorities.
- Broadly, placement of cash criminal proceeds must occur either through deposits or comingling with legitimate cash; or transported offshore to where cash can be more easily placed through either deposits or comingling. The FIU highlighted this vulnerability (co-mingling with business revenue) in a QTR which can be found on their website.
- The FIU reports multiple instances where individuals not involved in the predicate offending have been used to physically move cash (to act as cash couriers), particularly to physically transport cash internationally.
- The FIU reports that offending using cash is highly visible and transactions involving cash are known to be highly represented in STR reporting. Many reporting entities, including in some instances entire industries such as real estate agents, report STRs exclusively, or near exclusively in relation to cash transactions.
- Cash is used to purchase assets, such as vehicles or real estate and to conduct transactions through remittance channels (particularly international transactions). Cash can also be laundered via cash mules or transported via cash couriers.
- Other ML/TF vulnerabilities presented by cash include:
  - smurfing by dispersing placement through multiple cash deposits
  - refinement into higher denomination notes or specific currencies
  - cash intensive business proving opportunity for all three ML phases
  - being used in casinos
  - using anonymous deposit drop boxes or deposit capable ATMs
- Customers with foreign currency accounts may conceal illegitimate funds generated overseas by depositing cash within that account allowing easy conversion, transfer and access to the funds.

Appendix 6: International Trade and Trade Based Money Laundering (TBML)

Comment

- The World Trade Organisation values trade finance at $US10 trillion a year. In terms of ML risk FATF, the World Bank and others consider this a high risk area.
- TBML is an attractive method of hiding large values of proceeds of crime. The sheer volume of trade, both in terms of value and number of transactions provides launderers and terrorist financier's ample opportunity to hide the movement of illicit funds.
- Trade in services may be particularly attractive as it does not require movement of any physical goods, and the value of services can be very subjective. Thus "phantom" trades in services in particular may offer an attractive combination of (relative) ease and difficulty to detect an unusual trade amongst the volume of similar services traded internationally.
- TBML also provides an option to move funds between jurisdictions, while avoiding the AML/CFT controls that may hinder other forms of payments through the financial system.
- TBML also targets and takes advantage of differences in jurisdictions' legal systems, regulations and controls.
- International trade is inherently complex with long supply lines and multiple parties involved which create numerous opportunities for launderers/terrorist financiers to exploit vulnerabilities.
- Simple schemes to move illicit funds can involve collusion to under or over invoice or make phantom/sham trades. False invoicing can involve the manipulation and duplication of invoices or deliberate over/under valuing of goods.
- Systems for trade financing can also be used to move illicit funds. Some examples are:
    - documents, such as letters of credit, created through trade can be used by the launderer to establish the legitimacy of funds
    - direct loans from exporter to importers may be an attractive explanation for movement of capital internationally, especially where loans are made between shell companies and/or both entities are controlled by the same party(ies)
    - use of credit from financial institutions may create opportunities especially where credit for trade is extended across borders as CDD may be difficult. Mixing proceeds with credit from financial institutions may also complicate asset forfeiture as the institution may make claim on any assets forfeited or restrained
- Factoring is where a factoring house essentially buys the importer's debt to the exporter, creating opportunity for fraud and ML. For example, the factoring house may unknowingly be used to act as a mechanism for alternative remittance that may avoid detection by AML/CFT controls.
- Forfeiting, the buying and selling of importers' debt, can also create opportunities for laundering where the value of the debt is inflated through collaboration.
- TBML can occur through the movement of goods through countries for no sound economic reason or without any goods moved at all.

Appendix 7: New Payment Technology

Comment

- New payment technologies (some more mainstream than others) can increase the opportunities for ML/TF, in particular where they allow criminals to exploit developments that breakdown the barriers posed by international borders, or facilitate new anonymous means of payments between individuals.
- Australian typology reporting in 2010 acknowledged electronic banking as one of the most common ways used to launder funds.
- New payment technologies may exacerbate vulnerabilities in traditional channels by circumventing, hampering or defeating AML/CFT controls. For example, payments online allowing non-face-to-face transactions.
- Technology that can be accessed remotely anywhere in the world, can move funds quickly and allows the quick reintegration of the proceeds of crime back into the financial system will be attractive to launderers and terrorist financiers.
- New payment technologies may increase anonymity in other ways, for example by allowing more person to person transactions outside of the regulated financial sector or placing a layer between individuals undertaking transactions and reporting entities.
- Money launderers and terrorist financiers may be attracted by the speed and convenience of new payment technology enabled transactions. Criminals can exploit the borderless nature of the internet whereby there are difficulties regulating financial services that operate online.
- Some new payment technology vulnerabilities are:
    - Open loop stored value instruments which may be used overseas (see Cards section for further information).
    - Online payments facilitates offered by traditional financial sectors, such as banks and money remitters, particularly if the standard of AML/CFT compliance cannot be maintained in relation to these products
    - Online payment systems; particularly those that facilitate peer-to-peer payments or obscure purchases of valuable assets from financial institutions
    - Remitters offering money transfers to countries that provide e-wallets on phones.
    - e-currency, particularly Crypto-currencies such Bitcoin (see Anonymity section for further information)
- FATF have produced guidance in this vulnerability – Money Laundering Using New Payment Methods October 2010 - though, by its nature, the risk environment for NPT is dynamic and guidance will develop accordingly.

Appendix 8: Cards

Comment

- This vulnerability includes credit cards, cards attached to current accounts, prepaid cards/pressie cards, cards such as iTune or Google Play cards and currency cards/ cash passports.
- Cards are a high ML/TF risk product evidenced by their presence in many international ML/TF case studies.
- Risks associated with credit cards are balance payments made in cash, particularly large payments, and payments made by third parties. Multiple payments on the same day or at various locations may indicate potential ML.
- A method of blurring the origin of funds is for customers to load or overpay their credit cards followed by a request for refunds. In this manner the returned funds are from a 'clean' and 'legitimate' source.
- Credit cards may also be used for cash advances which are then used for wire transfers to high risk jurisdictions. In addition, credit cards can be loaded via overpayment with large amounts of funds and taken overseas and withdrawn from ATMs or used to purchase high value goods with very little chance of being intercepted.
- Prepaid electronic money cards for domestic use offer similar benefits to customers that credit cards do. Because they offer the ability to load funds through a variety of means they have an increased risk of use in ML/TF. It is not always necessary to have a bank account with an institution offering pre-paid cards.
- Some pre-paid debit cards have similar risk characteristics to credit cards, whilst others are restricted to a certain retailer or do not allow cash withdrawals.
- Pre-paid travel cards are available that can be loaded with and provide access to funds in currencies other than the NZ dollar. These may be particularly susceptible to being loaded with illicit funds and sent overseas to use or trade. Multiple purchases of cards may be an indicator of this type of activity.
- Customers and non-customers can access foreign exchange pre-paid cards at bank branches.
- Persons operating accounts can be acting on behalf of customers as nominees with multiple persons having access to cards on an account. This also provides anonymity.
- Non-bank credit cards (also referred to as stored value instruments) can also be used to transfer funds overseas via open loop global card networks, cash withdrawal options and the purchase of valuable assets.
- Cash passports may be reloaded with cash in structured amounts to avoid reporting thresholds. Likewise cash withdrawals can be made worldwide in a variety of currencies in a structured manner.

Appendix 9: Anonymity

Comment

- Anonymity is highly desirable for ML/TF purposes. Any products, services, business relationships or channels of delivery that facilitate anonymity or the disguising of identity or ownership represents a high ML/TF risk.
- Anonymity does not only apply to beneficial owners but also to those who have control or authority to act on an account.
- The following items (not exhaustive in nature) all provide varying degrees of anonymity. Reporting entities should carefully consider their use in the ordinary course of business and what AML/CFT measures should be deployed:
    - Drop boxes/Smart ATMs – provide a high degree of anonymity and an easy method to place the proceeds of crime into the banking system
    - Intermediaries – use of third parties to mask and disguise the identity of beneficial owners or those with executive control is a common typology
    - Non-face-to-face channels of delivery – a lack of direct contact between reporting entities and customers make it easier to use fraudulent or uncertified identity documents. Use of overseas documents in a non-face-to-face relationship also presents ML/TF risk
    - Shell-companies – NZ is an easy country to do business in and offers quick and simple establishment of companies. This can be abused by creating companies for criminal purposes (see Trusts and Shell Companies section)
    - Trusts – NZ has a large number of trusts (including family trusts) which are widely considered internationally as a well-known method of providing anonymity (see Trusts and Shell Companies section)
    - Safety Deposit Boxes – while not a common typology in NZ the use of deposit boxes has been linked in international reporting to organised crime and the hiding of the proceeds of crime
    - E-currency – E-currency, particularly crypto-currencies (e.g. Bitcoin) have not been observed in significant numbers in ML/TF cases and where it has been used the value of funds has been relatively low. However, the products and channels of delivery associated with this typology present a dynamic ML/TF risk. Where CDD policies are unclear and reporting entities knowledge of this topic is low this may allow anonymity and subsequent abuse for ML/TF purposes
    - Use of electronic banking - Where transactions occur without face-to-face contact with the reporting entity, criminals can use accounts set up by other persons, nominees or shell companies as a front for their activities. Electronic banking facilities often can be established in circumstances where it is difficult to verify the persons operating the account as distinguished from the account opener

- Determining and verifying the true identity of the customer is one of the most important AML/CFT measures that reporting entities must undertake. Shortfalls in this area represent the highest ML/TF risk.
- The FIU highlighted this vulnerability (via use of intermediaries and use of crypto-currencies) in two QTRs which can be found on their website.

Appendix 10: High Risk Customers

Comment

- There are numerous vulnerabilities associated with customers who represent the primary source of ML/TF risk for reporting entities. Every effort should be made to ensure CDD is carried out as required by the Act and in line with a RBA that is both robust and proportionate.
- Given the importance of CDD, reporting entities need to be mindful of the vulnerability of identity fraud and the use of uncertified or counterfeit identity documents.
- Reporting entities should establish whether the customer is a Politically Exposed Person (PEP) or a Relative and/or Close Associates (RCA) of a PEP. If they are then enhanced due diligence will be required. However, not all PEPs carry the same risks depending on the country the PEP is from, where they are located and the position of power or funds the person holds or controls. For very high risk PEPs extra AML/CFT measures will be needed.
- Foreign PEPs may use banking facilities in other countries to launder funds away from scrutiny in their home jurisdiction using the NZ banking system. The position of power of PEPs and the control they may exert in their home country means that it may be easier for them to access the proceeds of crime. Such funds may be diverted from legitimate sources or may be the result of corruption or bribery.
- Facilities provided to higher net worth customers, particularly those with dedicated customer representative relationships, can be misused for ML if transactions are rarely questioned because of the higher value of the business to the reporting entity.
- Trusts are internationally recognised as being vulnerable to ML/TF activity and are considered a high risk customer type. Refer to the Trusts and shell companies section for more information.
- Certain occupations or businesses are also considered high risk depending on their exposure to ML/TF vulnerabilities. For example, customers involved in arms manufacturing, extraction industries, high value and cash intensive businesses, casinos etc. In addition to the ML/TF opportunities, criminals may be attracted to businesses because its industry provides access to other facilitators of crime. For example, the FIU report that transport businesses, pharmacies and bars may all be used to facilitate the trafficking and sale of illicit drugs.
- Businesses, particularly cash businesses, have long been identified as being vulnerable to ML/TF activity. They are a particularly attractive option for obscuring the money trail at placement and layering phases. The classic technique of mingling cash proceeds with cash takings from a business to place funds in financial institution establishes a legitimate origin for the cash and reduces detection by a financial institution.
- Small cash intensive businesses may also be attractive to criminals as they may also be expected to have less sophisticated AML/CFT awareness.
- At the layering stage, moving funds through business accounts may be used to avoid suspicion or to place a layer between the financial institution and the individual involved. Use of a business controlled by a third party may also effectively obscure the involvement of beneficial criminal owners in a particular transaction.

Appendix 11: High Risk Jurisdictions

Comment

- When a reporting entity conducts their risk assessment they need to assess how their business may be vulnerable to ML/TF because of the countries they deal with. However, there is no universally agreed definition of a high risk country, but when undertaking this assessment a reporting entity should consider:
    - countries subject to sanctions, embargoes or similar measures
    - countries identified as lacking adequate AML/CFT systems/measures or controls
    - countries identified as having supporters of terrorism or the financing of terrorism
    - countries identified as having significant levels of corruption and/or organised crime
    - countries identified by credible sources as being tax havens
    - countries that are materially associated with production and/or transnational-shipment of illicit drugs or people trafficking
- The Act does not prohibit business relationships or transactions with persons/organisations based in high risk countries.
- The use of wire transfers to move funds cross-border relatively quickly is recognised internationally as one of the most common methods to launder funds.
- When dealing with a high risk jurisdiction ML/TF factors to consider include:
    - whether the country has laws that make it illegal to launder money or finance terrorism
    - whether the country's legislative framework puts obligations on financial institutions for CDD, account monitoring, STRs and record keeping similar to those set out in the Act
    - whether the country has an established and effective AML/CFT supervisory regime
    - whether the country has membership of the FATF or a FATF style regional body (FSRB), for example, the Asia/Pacific Group on Money Laundering (APG)
    - has the country been subject to any recent independent assessment of the country's AML/CFT systems/measures (i.e. a FATF mutual evaluation)
    - whether there are any public concerns raised about a country's AML/CFT systems/measures
- RBNZ reporting entities should consider not only high risk countries but also their neighbouring countries as ML/TF activity can involve the movement of funds across the border. For instance, the UK NRA 2015 identifies Turkey, East Africa (especially areas surrounding Somalia) and the Persian Gulf as TF transit countries/regions. As such reporting entities may wish to consider 'high risk jurisdictions' to cover both high ML/TF risk counties and their neighbours.
- For further guidance refer to the Sector Supervisors Countries Assessment Guideline July 2012.

Appendix 12: Money Service Businesses (MSBs)

Comment

- This vulnerability relates to alternative remittance, defined by FATF as money transfer services outside of the formal or licensed financial sector. For the purposes of the SRA 2017 this typology includes examples of foreign currency exchange.
- This vulnerability concerns the use of MSBs as a typology of ML/TF. It does not highlight the MSB industry as a ML/TF risk as a whole.
- Determining the size and nature of the MSB sector is difficult as alternative remitters may not comply with the requirement to register as a financial service provider and alternative remittance may operate as part of another financial entity (such as foreign exchange or more formal remittance).
- FATF have classified alternative remittance into three categories:
    - Traditional Hawala and similar service providers - Providers may establish traditional services within emerging or existing ethnic communities. These services increase and strengthen ties to other regions allowing remittance through traditional and established networks. These services were found to be lower risk provided that they are properly regulated.
    - Hybrid designated non-financial businesses or professions (DNFBPs) and alternative remittance providers - DNFBPs may expand their services to offer alternative remittance. The FATF found that these types of services are more vulnerable to abuse as they are more likely to remain poorly regulated.
    - Criminal Alternative Remittance Providers - The final type of service identified by the FATF was criminal alternative remittance providers. These are alternative remittance networks established or expanded to serve criminals and/or circumvent controls. Criminal alternative remittance providers are by nature high risk and may be connected to complex specialised money laundering networks managed by offshore international "controllers". The FATF found that these types of networks may be expanding internationally and are a growing concern.
- Easy access to services to convert currency is attractive to money launderers. Exchanging funds for an easily exchangeable and transportable currency, often at a variety of institutions, allows for funds to be moved into other countries without questions that may be raised from electronic transactions or wire transfers.
- Criminals may exchange low value foreign currency notes for higher value denominations that are more easily transportable. This is sometimes referred to as refining.
- Despite their decline in use traveller's cheques appear in international case studies of ML. Foreign currency drafts provide an easy method of removing funds from the country and little information is generally required about the recipient.

- An important consideration with MSBs is their role in supporting vulnerable and hard to reach populations. Financial exclusion based purely on a category of customer, product or jurisdiction is not in line with the FATF Recommendations. RBNZ supervised entities are expected to apply a RBA to MSBs and mitigate the ML/TF risks in a proportionate manner. The FATF has released a number of guidelines in relation to MSBs.
- The RBNZ has issued a statement on this topic contained on the RBNZ website. rbnz.govt.nz/news/2015/01/statement-about-banks-closing-accounts-of-money-remitters

Appendix 13: Lack of ML/FT Awareness

Comment

- Vulnerability from low awareness compounds the inherent vulnerability of some ML/TF risks. While many reporting entities consider themselves at a low risk of ML/TF activity their lack of awareness of some topics may make them more vulnerable to abuse by launderers and terrorist financiers. The role of the AML Compliance Officer is key in managing this. Listed below are examples of potential vulnerabilities. There are many others and AML Compliance Officers are encouraged to explore and consider the ML/TF risks pertinent to their organisation in the course of its business.
- **Example 1 - High value goods and services**: Buying and selling high value assets offers a wide variety of options at the placement and layering stages. Transactions involving assets can be an attractive option by-passing interaction with the financial sector and AML/CFT reporting entities. Criminals also target businesses that are unlikely to reject purchase transactions. The FIU highlighted this vulnerability in a QTR which can be found on their website.
- **Example 2 - Real-estate**: The use of real estate to integrate and layer criminal proceeds has been well established by international typology reports. The FIU also highlighted this vulnerability in a QTR which can be found on their website. In 2007 a FATF typology study on real estate identified the following areas of opportunity for launders:
    - use of complex loans or credit finance
    - use of gate-keeper professionals, to access financial services, to facilitate transactions through client trust accounts, or to act as intermediaries in transactions
    - use of corporate vehicles, such as off-shore companies, trusts, shell companies, and property management companies
    - manipulation of the appraisal or valuation of property
    - use of mortgages, such as funding mortgages with proceeds of crime
    - use of income generating property to co-mingle criminal proceeds.
- To increase awareness, there are a number of agencies and organisations which provide open source guidance and information. Those listed below are a good place to start:
    - NRA and SRA
    - FIU Quarterly Typology reports and STR guidance
    - AML Supervisors' Guidance material
    - Asia Pacific Group (APG) typology reports
    - Financial Action Task Force (FATF) guidance and best practice material
    - FATF 40 Recommendations and Interpretive Notes

- AUSTRAC guidance and training material
- United Nations Office on Drugs and Crime (UNODC) guidance documents

- One role of the AML Compliance Officer is to act as a conduit between senior management and operational staff to ensure that AML/CFT is actioned and understood at all levels of an organisation. They will also be a key element in the provision of training, identification of industry specific red flags and anticipating new and emerging threats.
- Developing, maintaining, demonstrating and evidencing situational awareness is a vital responsibility of the AML Compliance Officer and the reporting entity as a whole. As such keeping across ML/TF related current affairs, media, typologies and research is expected from AML Compliance Officers.

Appendix 14: General Dual Use Items and Proliferation Risk Factors

Taken from the *FATF Report - Proliferation Financing Report* 2008

Nuclear	Chemical	Biological	Missile and delivery
Centrifuges	Scrubbers	Bacterial strains	Accelerometers
High-speed cameras	Mixing vessels	Fermenters	Aluminium alloys
Composites	Centrifuges	Filters	Aluminium powders
'Maraging' steel	Elevators	Mills	Gyroscopes
Mass spectrometers	Condensers	Presses	Isostatic presses
Pulse generators	Connectors	Pumps	Composites
X-ray flash apparatus	Coolers	Spray dryers	'Maraging' steel
Pressure gauges	Precursors	Tanks	Homing devices
Ignition	Pumps	Growth media	Oxidants
Vacuum pumps	Reactors		Machine tools
	Heat Exchanges		

"Given that the sources of funding for WMD proliferation can be legal or illegal, well-known indicators or "red flags" for money laundering may be relevant in cases where the source of funds is illegal. However, the risk of proliferation financing is more likely to be present in cases where the source of funds is legal but the end-user or type of goods involved is intended to be obscured. " FATF

- Weak AML/CFT controls and/or weak regulation of the financial sector.
- Weak or non-existent export control regime and/or weak enforcement of existing export control regime.
- Non-party to relevant international conventions and treaties regarding the non-proliferation of weapons of mass destruction.
- Lack of implementation of relevant United Nations Security Council resolutions (UNSCRs).
- The presence of industry that produces WMD components or dual-use goods.
- A relatively well-developed financial system or an open economy.
- The nature of the jurisdiction's export trade (volumes and geographical end-users).
- A financial sector that provides a high number of financial services in support of international trade.

- Geographic proximity, significant trade facilitation capacity (e.g. trade hub or free trade zone), or other factors causing a jurisdiction to be used frequently as a trans-shipment point from countries that manufacture dual-use goods to countries of proliferation concern.
- Movement of people and funds to or from high-risk countries can provide a convenient cover for activities related to proliferation financing.
- Lack of working coordination between the customs authority and the export licensing authority of a specific jurisdiction.
- A jurisdiction that has secondary markets for technology.

Appendix 15: Glossary

Anti-Money Laundering/Countering Financing of Terrorism (AML/CFT) Act 2009

AML	Anti-Money Laundering
APG	Asia Pacific Group on AML
AUSTRAC	Australian Transaction Reports and Analysis Centre
BCR	Border Cash Report
BO	Beneficial Owner
CBR	Correspondent Banking Relationship
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism
CPRA	Criminal Proceeds (Recovery) Act 2009 (NZ)
CTR	Cash Transaction Report
DBG	Designated Business Group
DNFBP	Designated Non-Financial Business or Profession
EDD	Enhanced Due Diligence
Egmont	International body of FIUs
FAFT	Financial Action Task Force
FATF 40	FAFT 40 recommendations for AML/CFT and Proliferation
FinCEN	Financial Crimes Enforcement Network (USA)
FINTRAC	Financial Transactions and Reports Analysis of Canada
FIU	Financial Intelligence Unit (hosted by NZ Police)
FSRB	FATF Style Regional Body (APG is a FSRB)

FTRA	Financial Transaction Reporting Act 1996 (NZ)
goAML	FIU reporting system for STRs
I&W	Indicators and Warnings (of ML/TF)
IDVCOP	Identity Verification Code of Practice
IFTI	International Fund Transfer Instruction
MER	Mutual Evaluation Report
ML	Money Laundering
MSB	Money Service Business (including oing customer applications fro new products)re of the exemptions in the AML/CFT Regulations. an appear legitimate.rather remitters)
N&P	Nature and Purpose of business
NBDT	Non-Bank Deposit Taker
NBNDT	Non-Bank Non-Deposit Taker
NCC	National Coordination Committee (NZ)
NRA	National Risk Assessment
PAOBO	Person acting on behalf of
PEP	Politically Exposed Person
POWBATIC	Person on whose behalf a transaction is carried out
PPC	Policy, Procedure and Controls
PTR	Prescribed Transaction Report
QA	Quality Assurance
RA	Risk Assessment
RCA	Relative or Close Associate (of a PEP)

RE	Reporting Entity
Regs	AML/CFT Regulations
s.57	Contains minimum requirements for AML/CFT Programme
s.58	Risk Assessment
s.59	AML/CFT audit requirements
s.60	AML/CFT Annual Report requirements
SPR	Suspicious Property Report (incl. in Terrorism Suppression Act 2002 - NZ)
SRA	Sector Risk Assessment
STR	Suspicious Transaction Report
STR/SAR	Suspicious Transaction Report/Suspicious Activity Report
SVI	Stored Value Instruments
TBML	Trade Based Money Laundering
TF	Terrorist Financing
TM	Transaction Monitoring
UNODC	United Nations Office on Drugs and Crime
WMD	Weapon of mass destruction (financing of proliferation)
1LOD, 2LOD…	First line of defence, second line of defence…

Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Methodology for Sector Risk Assessment.

For Registered Banks, Non-Bank Deposit Takers, and Life Insurers
Reserve Bank of New Zealand

April 2017

Reserve Bank of New Zealand
Te Pūtea Matua

Sector Risk Assessment (SRA) Methodology

As discussed in Part 4 of this document, the SRA 2017 provides an assessment of ML/TF risk and identifies key potential ML/TF vulnerabilities:

1. Methodology – Assessment of risk
2. Methodology – Identification of vulnerabilities

The Concept of Risk

Risk in the SRA 2017 is aligned with the current international standard and the Financial Action Task Force (FATF) guidance. The SRA 2017 does not assess threats. The SRA looks at each potential vulnerability separately. This approach has been adopted to keep the SRA 2017 simple and user friendly.

The SRA 2017 utilises relevant aspects of the FATF guidance (and other international guidance) to ensure a methodologically sound approach to assessing ML/TF risk. It works on two distinct levels. The SRA provides an **assessment of ML/TF risk** and **identifies key ML/TF vulnerabilities** and how they impact each sub sector. Where there are specific vulnerabilities, weaknesses or typologies of note are also highlighted.

The SRA 2017 is one of the decision-making tools RBNZ uses to plan and focus its AML/CFT supervisory activities with the aim of carrying out RBNZ's statutory functions in an effective and efficient way.

The SRA 2017 informs and supports RBNZ's AML/CFT supervisory objectives. Primary amongst these objectives is the detection and deterrence of ML/TF and the administration of justice through RBNZ's expertise in AML/CFT supervision.

ML activity has the potential to result in very serious social harm, criminal, financial and reputational consequences. TF, while recognised as an unlikely event in NZ, has the potential for catastrophic consequences. Given the considerable harm caused by organised crime, tax evasion and fraud and the increased presence of global TF RBNZ has a low tolerance for predicate criminal offending.

Methodology – Assessment of Risk

ML/TF risk for each sub sector section was assessed using the framework of variables listed in s.58 (2) (a)-(f) of the Act and the Risk Assessment Guidelines (see a-f below). This was done to assist reporting entities in using the SRA 2017 in their own risk assessment:

a. Nature size and complexity of business;
b. Products/services;
c. Channels of delivery of products/services;
d. Customer types;
e. Country risk; and
f. Institutions dealt with (if relevant).

For each of these variables a number of ML/TF questions were posed. The responses to these questions helped guide the assessment of inherent risk for each variable in combination with structured professional knowledge coupled with domestic and international guidance, and the findings of the Enterprise Risk Assessment (ERA) – see ERA section below.

Weightings were deliberately not assigned to the ML/TF questions and their answers due to the highly variable nature of each sub-sector and the individual financial institutions within them. When reporting entities consider their own risk assessment they may find value in assigning greater importance to certain ML/TF variables to obtain a more accurate picture of their business specific AML/CFT environment.

An explicit part of the risk rating process was to consider the consequences for each sub-sector of ML/TF activity based on the potential for harm. This took into consideration the size of the sub-sector, the importance of the sub-sector to the NZ financial sector and potential reputational damage. These judgements were necessarily qualitative in nature due to the wide variance in ML/TF consequence across individual reporting entities.

Because the RBNZ did not consider the adequacy or effectiveness of ML/TF controls in the risk rating process, no judgements were made to whether the risks present in a sector/sub-sector are adequately managed or mitigated. Reporting entities may have systems and controls that address some or all of their ML/TF risks but the SRA 2017 does not identify or comment on individual entities within the sub-sectors. At the end of this process an overall assessment of inherent ML/TF risk was then assigned to each sub-sector using ratings of Low, Medium or High.

Methodology – Identification of Vulnerability

As part of the SRA 2017, 12 key ML/TF vulnerabilities were identified. The vulnerabilities were selected during a series of RBNZ workshops based on subject matter expertise, domestic experience gained during onsite visits and both domestic and international guidance. The vulnerabilities were chosen for their commonality across the RBNZ supervisory sector and were deliberately kept few in number to assist reporting entities understand the ML/TF environment in NZ .

The assessment of vulnerability was undertaken by RBNZ via a Delphi process (see below) to ensure reliability. These findings were then combined with structured professional judgement and data from the RBNZ Enterprise Risk Assessment (ERA – see below). RBNZ then assigned severity ratings for the 12 key vulnerabilities for each sub-sector.

The Delphi technique is a quantitative exercise aimed at reaching a consensus. For the SRA 2017 opinions were gathered from RBNZ experts during workshops in an iterative process of answering questions. After each round the responses were summarised and redistributed for discussion in the next round. Three rounds were used in the SRA 2017.

Consultation with Other AML/CFT Sector Supervisors

RBNZ, as one of the three AML/CFT supervisors, is in regular contact with the Department of Internal Affairs (DIA) and Financial Markets Authority (FMA). During the production of the SRA 2017 formal feedback and input was sought from the supervisors.

Consultation with FIU

Consultation with the FIU occurred on an on-going basis during the production of the SRA 2017. Communication, feedback, input and the exchange of information between the RBNZ and FIU was comprehensive and robust.

Risk Appetite – Reporting Entity

Regardless of the assessed ML/TF risk and vulnerability ratings in the SRA 2017 when reporting entities assess their own ML/TF risk consideration should be given to the level of risk they are willing to accept. A risk-based approach (RBA) recognises that there can never be a zero risk situation and reporting entities must determine the level of ML/TF exposure they can accept. This is not a legislative requirement but may help reporting entities in their risk management.

Information Sources

The SRA 2017 has drawn together information from a number of sources. This includes:

- AML/CFT findings from the RBNZ Banks, Payments and AML team (BPA) – experience and knowledge from the RBNZ AML/CFT subject matter experts;
- AML/CFT findings from RBNZ reporting entities – ML/TF experience direct from NZ banks, NBDTs and Insurance entities;
- Overseas experience – such as Australian Transaction Reports and Analysis Centre (AUSTRAC) and Financial Crimes Enforcement Network (FinCEN -USA);
- Multinational organisations – such as FATF and APG; and
- Industry specific information – such as the Basel Index and the Wolfsberg Principles. The Basel AML Index is an annual ranking assessing country risk regarding ML/TF. The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly ML/TF.

This information is supplemented by local information, particularly AML/CFT annual report data. Consideration was given to other data sources available to the AML/CFT supervisors including summary Suspicious Transaction Report (STR) data and information provided by the FIU, as well as industry expertise, knowledge and experience from internal and external resources relevant to the sector. The SRA 2017 also considered the findings of the other supervisors about risks when they are reasonably similar.

Qualitative and Quantitative Data

The SRA 2017 used a combination of qualitative and quantitative data collected and collated from numerous sources of information. The qualitative judgements of AML/CFT professionals and key stakeholders were an essential aspect of the data collection process. Qualitative data included data from STRs, the RBNZ ERA, Asset Recovery Unit data and criminal justice statistics. Quantitative data included expert assessments through structured questions, interviews, workshops and other assessment tools. This is in line with FATF, IMF, Worldbank and Organisation for Security and Cooperation Europe (OSCE) methodologies.

Baseline Monitoring – Annual Report Data

Baseline monitoring, which utilises AML/CFT annual report data, assists RBNZ in keeping track of issues across RBNZ's AML/CFT sector on an on-going basis, and can selectively follow-up any increased risks and help guide RBA based supervisory action. Baseline monitoring can also assist RBNZ measure the effectiveness or pro-activeness of its AML/CFT supervision providing an indication of levels of compliance within each reporting entity. This assists decision-making on the appropriate frequency and intensity of RBNZ AML/CFT supervision.

Limitations

The following limitations to the SRA 2017 process were identified:

- information on ML in NZ is still limited, though with less reliance on international typologies and guidance to identify risks;
- reporting entities have varying degrees of understanding of AML/CFT legislation, and the ML/TF risks in their business, therefore the perception of ML/TF may not be fully developed in a reporting entities AML/CFT risk assessment;
- insufficient availability of detailed data and information to inform some risk areas; and
- variable quality of data that informs the Risk Assessment across some of the sub sectors.

ML/TF Vulnerability Questions

These questions do not represent an exhaustive list of all potential questions. These questions were targeted at the sub-sector reporting level and used by RBNZ to determine ML/TF risk.

Reporting entities are encouraged to consider these questions and incorporate them into their Risk Assessment process.

ML/TF Questions – Nature, Size, Complexity

Nature, Size And Complexity Of Sub-Sector	Notes
Which transactions have a value or volume or velocity that could potentially mask suspicious activity?	The larger and more complex business is the quicker it can facilitate transactions and the more potential scope there is for suspicious transactions to be masked.
Does the complexity of our business make AML/CFT measures and investigations difficult to implement?	Greater complexity can result in reduced adequacy and effectiveness of AML/CFT measures and investigations.
Does the size of our business make AML/CFT measures difficult to implement?	Large organisations may have difficulty tailoring their AML/CFT measures to meet multiple requirements.
Is the nature of our business recognised as being associated with a known ML/TF vulnerability?	Refer to the NRA and SRA. Also refer to the FIU Quarterly Typology Report and Sector Supervisor guidance material and newsletters. Also refer to FATF, APG, Egmont Group or other trusted AML/CFT sources. In addition, reference can be made to comparable jurisdictions and their AML/CFT guidance such as AUSTRAC in Australia.
Could the inclusion of our corporate data or AML/CFT annual report data provide useful context during the assessment of ML/TF risk?	An assessment of risk requires context. Without metrics to add context the assessment is potentially flawed. Corporate data is an important aspect of a risk assessment. For instance, if a product type is potentially vulnerable to ML/TF, corporate data can indicate how many of its customers have this product, how many of these customers are high risk, what jurisdictions are these customers in.

ML/TF Questions – Products/services

Products/Services Provided by Sub-Sector	Notes
Which of our products/services are identified as heightened risk by the AML/CFT supervisors?	Refer to the NRA and SRA. Also refer to the FIU Quarterly Typology Report and Sector Supervisor guidance material and newsletters.
Which products/services have been identified as presenting heightened ML/TF risk by AML/CFT international guidance?	Refer to FATF, APG, Egmont Group or other trusted AML/CFT sources. In addition, reference can be made to comparable jurisdictions and their AML/CFT guidance such as AUSTRAC in Australia.

Products/Services Provided by Sub-Sector	Notes
Which products/services support physical cash deposit and/or withdrawal? Consider 'placement' phase of ML/TF.	Cash is still very much a favoured method of ML/TF. The ease of movement without audit trail makes it highly vulnerable to ML/TF activity.
Which products/services be redeemed or traded for cash?	Liquidity is a highly sought after element for ML/TF activity.
Which products allow international funds transfers? i.e. movement of cash across borders using credit cards or cash passports	If the product/service enables cash to withdrawn in a jurisdiction outside of NZ this may be considered a ML/TF risk.
Which services enable international funds transfer? i.e. IFTIs	If the service enables funds to be sent to a jurisdiction outside of NZ, especially those with weal AML/CFT controls, this may be considered a ML/TF risk.
Which products/services support payments to and from third parties or non-customers (this does not include the settlement of securities)	This can disguise the beneficial ownership or executive control of funds.
Which products/services support transactions 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.
Are the products/services highly liquid, support early redemption and conversion to cash or equivalent value?	Liquidity is a highly sought after element for ML/TF activity.
Do the products/services allow high volumes and high values of transactions?	The value, volume and velocity of transactions is a key I&W.
Do the products/services operate using commission based remuneration?	There is the potential for a conflict of interest between effective AML/CFT measures and commercial gain. This may lead to AML/CFT measures being ignored or reduced in order to gain/maintain business.
Do the products/services provided in this sub-sector support pooling of funds?	This can disguise the beneficial ownership of funds.
Does the sub-sector target products/services to off shore customers?	Having customers off shore may expose the reporting entity to ML/TF risks that are beyond their control; especially in connection with countries with weak AML/CFT regimes and high levels of corruption or bribery and organised crime.

ML/TF Questions – Channels of Delivery (including customer applications for new products)

Channel of delivery used by sub-sector	Notes: This not only applies to the delivery of products and services but also the means by which a customer may apply for them.
Does the channel used for delivery provide anonymity?	Anonymity is highly sought after by criminal elements and threat actors to facilitate ML/TF.
Does it depend on intermediaries?	This may result in the customer identity, beneficial owner or executive controller not being transparent to the reporting entity.
Does it remove or minimise face-to-face contact with the customer?	Less face to face interaction with a customer increases vulnerability to ML/TF activity.
Is it targeted to off shore customers?	Having customers off shore may expose the sub-sector to ML/TF risks that are beyond their control; especially in connection with conflict zones and their borders, countries with weak AML/CFT regimes and high levels of corruption or bribery and the presence of significant levels of organised crime.
Can a third party utilise this channel?	This may result in the customer identity, beneficial owner or executive controller not being transparent to the reporting entity.

ML/TF Questions – Customer Type

Customers of the sub-sector	Notes
Which customers have an ownership structure that is generally transparent?	Overly complex and non-transparent structure may mask ML/TF activity.
Which customers have a high risk occupation?	Some occupations can have greater vulnerability to ML/TF. For instance, arms manufacturing, cash intensive business owners, jewellers, high value goods dealers.
Which customers operate on a global scale?	High levels of transactions with high risk overseas jurisdictions.
Which customers reside in a high risk jurisdiction?	See county risk questions.
Has international guidance identified some customers as presenting a higher ML/TF risk? For instance, PEPs?	PEPs and their relatives and close associates (RCAs) can mean greater vulnerability to ML/TF. Other things to consider are association with organised

Customers of the sub-sector	Notes
	crime, tax evasion, fraud, bribery and corruption, people trafficking and drug offending.
Which customers are registered or regulated by a Government or industry body?	Explore whether the AML/CFT measures are adequate and have been subject to over sight e.g. FATF evaluation or effective supervision.
Which customers are trusts, shell companies, charities, NPOs or companies with nominee shareholders or shares in bearer form?	These customer types have been identified as presenting a high level of ML/TF risk.
What is the nature and purpose of the business relationship with the customer?	Is the proposed business relationship in line with what the entity would expect, based on the outcome of its CDD? This is a particularly important topic as it greatly assists with STRs and investigations.
Which are the high wealth customers? What are their sources of wealth/funds? Are they connected to high risk industries?	Without establishing the legitimate origin of a higher-risk customer's source of wealth and source of funds, entities cannot be satisfied that they are not being used to launder the proceeds of crime. Again the importance of CDD and determining the nature and purpose of the business relationship come to the fore.

ML/TF Questions – Country Risk

Country Risk faced by sub-sector	Notes
Are there transactions/dealings with countries that have weak or ineffective AML/CFT measures?	Refer to FATF or APG.
Which countries present a general ML/TF risk?	Refer to FATF, APG (and other FSRBs) and Basel Index. However, when using these sources of information it is advisable to still exercise critical thought and consider the wider context.
Which countries have a high degree of organised crime or drug related crime?	Refer to UNODC and trusted media sources. The presence of a high level of organised crime is an important consideration in country risk.
Which countries have a high degree of corruption and bribery?	Refer to Transparency International for perceived corruption index information.
Which countries have been identified as high risk countries for ML/TF predicate offending?	This could involve fraud, tax evasion, drug related offending, bribery, corruption, extortion, kidnapping, human trafficking and high value theft.

Country Risk faced by sub-sector	Notes
Are the countries dealt with conflict zones or jurisdictions with significant terrorism activity?	Open source media will provide information on this. Refer to TF section for more information.
Do the countries border conflict zones?	Movement of funds into conflict zones across borders is an identified ML/TF issue. Refer to TF section for more information.
Do the countries border countries with weak AML/CFT measures?	Cross border movement of funds may be an issue where one jurisdiction has strong controls while their neighbour has poor controls.

ML/TF Questions – Institutions Dealt With

Institutions dealt with by the sub-sector	Notes
Have any of the institutions we deal with/transact through been directly subject to negative media related to ML/TF?	An in-depth Google search may assist as will referencing trusted media sources. Negative media may be explained (also called dispositioning) and may not necessarily result in a higher assessment of ML/TF risk.
Have the institutions dealt with been subject to regulatory action or negative AML/CFT findings from recognised and trusted sources; domestic and international?	Consult FATF, APG, FIU, UNODC and trusted media sources for information on this topic.
Does the institution dealt with have suitable AML/CFT controls and supervision for AML/CFT compliance?	Due diligence will be required to determine level of comfort with an institutions AML/CFT measures.
Do we have a correspondent banking relationship (CBR)?	CBRs are recognised internationally as presenting a higher risk of ML/TF.

Source Documents List

All of the following are open source documents used in the production of the SRA 2017. They can be accessed via a simple internet search with some documents available on multiple sites.

- FATF Report – Terrorist Financing FATF Report to G20 Leaders – Actions Being Undertaken by the FATF – November 2015
- FATF Report – Emerging Terrorist Financing Risks – October 2015
- FATF Report – Financing of ISIL – February 2015
- FATF Report – Guidance for a Risk Based Approach - The Banking Sector – October 2014
- FATF Report – Risk of Terrorist Abuse in Non-Profit Organisations – June 2014
- FATF Report – Virtual Currencies: Key Definitions and Potential AML/CFT Risks – June 2014
- FATF Report – Guidance for a Risk Based Approach - Prepaid Cards, Mobile Payments and Internet Based Payment Services – June 2013
- FATF Report – Money laundering and terrorist Financing Vulnerabilities of Legal professionals – June 2013
- FATF Guidance – National Money Laundering and Terrorist Financing Risk Assessment – February 2013
- FATF Recommendations – International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation – February 2012
- FATF Report – Money Laundering Using New Payment Methods – October 2010
- FATF Report – Money Laundering Using Trust and Company Service providers – October 2010
- FAFT Report – Risk Based Approach - Guidance for the life Insurance Sector – October 2009
- FATF Report – Money Laundering and Terrorist Financing in the Securities Sector – October 2009
- FATF Report – Proliferation Financing Report – June 2008
- FATF Report – Money Laundering and Terrorist Financing Through the Real Estate Sector – June 2007
- Asia Pacific Group (APG) – APG Yearly Typologies Report - 2015
- Asia Pacific Group (APG) – APG Yearly Typologies Report – 2014
- Asia Pacific Group (APG) – Trade Based Money Laundering Typologies – July 2012
- Asia Pacific Group (APG) – New Zealand Mutual Evaluation Report (MER) 2010

- United Nations Office on Drugs and Crime – Risk of Money Laundering through Financial Instruments – 2nd Edition – 2013
- Organisation for Security and Co-operation in Europe (OSCE) – OSCE Handbook on Data Collection in support of Money Laundering and Terrorism Financing National Risk Assessments - 2012
- HM Treasury and Home Office - UK national risk assessment of money laundering and terrorist financing – October 2015
- HM Treasury and Home Office – Anti –money laundering and counter terrorist finance supervision report 2013-14 – Updated March 2015
- Financial Conduct Authority (UK)– Anti-money laundering annual report – 2012/12 – July 2013
- Financial Services Authority (UK) – Banks' management of high money-laundering risk situation (How banks deal with high risk customers (including politically exposed persons), correspondent banking relationships and wire transfers) – June 2011
- International Association of Insurance Supervisors - CP 28: AML and CFT – Basic Level Module – 2006
- International Association of Insurance Supervisors – Guidance Paper No. 5 - Guidance Paper on AML and CFT – October 2004
- Basel institute on Governance - AML Index – August 2014
- Basel Committee on Banking Supervision – Core principles for Effective Banking Supervision – September 2012
- AS/NZS ISO 31000:2009 Risk Management- Principles and guidelines
- AS/NZS ISO 4360:2004 Risk Management
- FINTRAC – Guidance of the Risk based Approach to Combatting Money Laundering and Terrorist Financing – May 2015
- FINTRAC – FINTRAC Typologies and Trends Reports – (multiple)
- Department of the Treasury/Justice/Homeland Security/Federal Reserve/ US Postal Service – U.S Money Laundering Threat Assessment – December 2005
- AUSTRAC – Methodologies Brief 01– Building a Profile: Financial Characteristics Associated with Known Foreign Terrorist Fighters and Supporters – December 2015
- AUSTRAC – Strategic analysis brief: Use of business express deposit boxes to avoid reporting requirements - 2015
- AUSTRAC - Terrorism Financing in Australia - 2014
- AUSTRAC – Typologies and Case Studies Report – 2014

- AUSTRAC – Typologies and Case Studies Report – 2013
- AUSTRAC – Money Laundering in Australia – 2011
- The Egmont Group of FIUs – 100 Cases from the Egmont Group (date unknown)
- The Egmont Group of FIUs – FIUs and Terrorist Financing Analysis Report (date unknown)
- New Zealand Police Financial Intelligence Unit (FIU) – National Risk Assessment of Money Laundering and Terrorist Financing 2016 (Draft)
- New Zealand Police Financial Intelligence Unit (FIU) – National Risk Assessment of Money Laundering and Terrorist Financing 2010
- New Zealand Police Financial Intelligence Unit (FIU) – National Risk Assessment of Money Laundering and Terrorist Financing 2010 - Support Document
- New Zealand Police Financial Intelligence Unit (FIU) – Quarterly Typology Reports (multiple and on-going)
- Department of Internal Affairs (DIA) – Sector Risk Assessment Guides (multiple) – April 2014
- Department of Internal Affairs (DIA) – Sector Risk Assessment – March 2011
- Financial Markets Authority (FMA) - then Securities Commission – Sector Risk Assessment – March 2011
- Reserve Bank of New Zealand – AML/CFT News and Updates (multiple)
- Reserve Bank of New Zealand – AML/CFT Questions and Answers
- Reserve Bank of New Zealand (with the DIA and FMA) - Beneficial Ownership Guideline – December 2012
- Reserve Bank of New Zealand (with the DIA and FMA) - Countries Assessment Guideline – July 2012
- Reserve Bank of New Zealand (with the DIA and FMA) - AML/CFT Programme Guideline – December 2011
- Reserve Bank of New Zealand (with the DIA and FMA) - Risk Assessment Guideline – June 2011
- Reserve Bank of New Zealand – Sector Risk Assessment For Registered Banks, Non-Bank Deposit Takers and Life Insurers – March 2011