Te Tari Taiwhenua
Internal Affairs

New Zealand Government

Phase 2 Sector Risk Assessment

December 2017

NOTE: This sector risk assessment is intended to provide a summary and general overview. It does not assess every risk relevant to the covered sectors. It does not set out the comprehensive obligations under the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 and associated AML/CFT regulations and codes of practice. It does not constitute, nor should it be treated as, legal advice or opinion. The Department of Internal Affairs accepts no liability for any loss suffered as a result of reliance on this publication.

Contents

Executive summary

Scope

1. This Sector Risk Assessment (SRA) is the first anti-money laundering and countering financing of terrorism (AML/CFT) risk assessment undertaken by the Department of Internal Affairs (DIA) for reporting entities covered by Phase 2 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act). Under Phase 2 of the Act, DIA will supervise designated non-financial businesses and professions (DNFBPs) – lawyers, conveyancers, accountants, real estate agents, and trust and company service providers – who carry out, in the ordinary course of business, activities defined in the Act. Phase 2 also covers high-value dealers (HVDs) and the New Zealand Racing Board (NZRB).
2. The Phase 2 SRA has two functions: it will help DIA AML/CFT supervisors in understanding the risks of money laundering (ML) and terrorism financing (TF) in the Phase 2 sectors, and it will help the Phase 2 sectors meet their AML/CFT obligations.
3. This includes identifying, monitoring and mitigating ML/TF risks, and reporting suspicious or unusual activity to the New Zealand Police Financial Intelligence Unit (FIU). **This will be in conjunction with industry-specific guidance documents produced by DIA.** The Reserve Bank of New Zealand (RBNZ) and the Financial Markets Authority (FMA) have published similar risk assessments for the sectors they supervise[1].
4. All countries are exposed to illicit international money flows. The global nature of ML/TF is reflected in the work of the Financial Action Task Force (FATF) based on input from experts across the globe. The FATF Recommendations form the basis of international efforts to counter ML/TF, and New Zealand, via products such as the Phase 2 SRA, is working towards implementing the recommendations in a way that is tailored towards its own ML/TF risks.
5. The Phase 2 SRA is separated into two parts: the SRA itself and the SRA support document. The SRA can be read on its own and will provide reporting entities with an overview of their key AML/CFT risks and vulnerabilities. The support document contains all appendices for the SRA and covers more technical aspects, including the risk assessment process and methodology, and details on significant vulnerabilities and high-risk factors.
6. A companion document to the SRA – AML/CFT Risk Assessment and Programme: Prompts and Notes for DIA reporting entities – provides some direction and basic supervisory expectation to help DIA reporting entities in meeting the minimum requirements of the Act. DIA recommend that reporting entities' AML/CFT compliance officers (compliance officers) be familiar with this document.

Limitations

7. For consistency when comparing sectors, DIA did not consider the adequacy or effectiveness of any ML/TF controls. The Phase 2 SRA is an assessment of **inherent** risk across each sector. The Phase 2 SRA does not assess **residual** risk.
8. Inherent risk is the assessed ML/TF risk before any controls or mitigation measures have been put in place. Residual risk is the assessed ML/TF risk after any controls or mitigation measures have been put in place.
9. Reporting entities are responsible for determining their individual levels of inherent ML/TF risk in the context of their ordinary course of business. Once they have determined their inherent risk, they can then apply their AML/CFT controls and determine their residual ML/TF risk.
10. The Phase 2 SRA has drawn on aspects of the FIU's current National Risk Assessment (NRA 2017)[2], FIU Quarterly Typology Reports, and the existing SRAs of DIA, FMA and RBNZ. In addition, the Phase 2 SRA uses guidance and reports from other jurisdictions and international organisations such as the Asia Pacific Group (APG) and the FATF, which are inter-governmental bodies developing and promoting policies to combat ML/TF.
11. This document is designed to give Phase 2 reporting entities guidance on AML/CFT and to help them meet their obligations under the Act. The Phase 2 SRA works on two distinct levels: it provides an assessment of ML/TF risk, and it identifies key ML/TF vulnerabilities and how they impact each sector. **A risk rating for**

[1] FMA. (2017). Anti-Money Laundering and Countering Financing of Terrorism Sector Risk Assessment 2017. http://bit.ly/2jTH2Pg RBNZ. (2017). Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers. http://bit.ly/2hPOaIa

[2] The NRA 2017 is due to be published in early 2018.

ML/TF is not an indication of instability or criminality of any business type or reporting entity within the sector.

Implementation period

12. The Phase 2 SRA includes reporting entities that are not yet covered by the Act. Sectors will be added to the Act in a staggered manner with implementation dates for the Phase 2 entities as follows:

Sector	Implementation date
Lawyers	1 July 2018
Conveyancers	1 July 2018
Accountants	1 October 2018
Real estate agents	1 January 2019
New Zealand Racing Board	1 August 2019
High-value dealers	1 August 2019

13. Between the time this SRA is released and the time that the Act is implemented for all the Phase 2 sectors, DIA may update the SRA to better reflect our understanding of the AML/CFT environment.

14. Trust and company service providers are not covered in this Phase 2 SRA. They were already covered in part during Phase 1 of the Act, and they will be covered in more detail in the revised Phase 1 SRA due for publication in early 2018.

Assessment of risk

15. ML/TF risk is assessed using a 5×5 risk matrix in line with the DIA Enterprise Risk Management Tool (see Appendix 1). The ratings (high, medium-high, medium and low) are based on available data, guidance and structured professional opinion. The table summarises the assessed **inherent** ML/TF risk of each sector[3].

Sector – Phase 2	Inherent risk of ML/TF
Lawyers	Medium-high
Accountants	Medium-high
Real estate agents	Medium-high
High-value dealers	Medium-high
New Zealand Racing Board	Medium-high
Conveyancers	Low

Sector – Phase 1	Inherent risk of ML/TF
Money remitters	High
Trust and company service providers	High
Casinos	Medium-high
Currency exchangers	Medium
Cash storage	Medium
Cash transport	Medium
Non-bank non-deposit taking lending	Low
Financial leasing	Low
Non-bank credit cards	Low
Factoring	Low
Debt collection	Low
Payroll remittance	Low

16. It is worth emphasising that the ratings in both SRAs do not consider risk controls or mitigation measures that are in place in reporting entities or across the sectors. This assessment of **residual** risk is not part of the SRA.

17. The legal, accountancy and real estate sectors are known as designated non-financial business and professions (DNFBPs) or more commonly as "gatekeepers". Gatekeepers refers to the role they play in providing services and products that can be used to facilitate the entry of illicit funds into the legitimate financial system. For instance, legal persons and legal arrangements are at risk of abuse by money launderers and terrorism financiers, and are often used in ML/TF schemes. In addition, real estate is commonly used as an investment vehicle for concealing and laundering criminal proceeds. Gatekeepers provide three principle opportunities for criminals:

[3] The risk ratings are compared with the 2011 Phase 1 SRA risk ratings. The Phase 1 ratings have been adjusted to fit the current Enterprise Risk Management Tool.

- Providing an impression of respectability and normality
- Frustrating detection and investigation of ML/TF
- Providing access to specialist services and techniques

18. The FATF 40 Recommendations specifically highlight gatekeepers as presenting ML/TF risk. Adopting the FATF Recommendations is one of the purposes of the Act, and this SRA will help New Zealand meet those recommendations.
19. The overall **medium-high** risk rating for lawyers is consistent with the characteristics of the legal industry in the absence of AML/CFT controls. This is to be expected given the relatively large size of the sector, the "gatekeeper" role it plays and the number and the types of customers it has. The legal sector risk rating reflects its wide availability and easy access to numerous high-risk products and services.
20. The overall **low** risk rating for the conveyancing sector reflects the smaller size and limited products and services covered by the Act. Although the risk rating is low, this sector has a number of industry-specific ML/TF typologies.
21. The overall **medium-high** risk rating for the accounting sector reflects the large size of the sector, its "gatekeeper" role, and its provision of a wide number of products and services. The accountancy sector is vulnerable to a number of ML/TF factors and may present an attractive avenue for ML/TF.
22. The overall **medium-high** risk rating for real estate agents is consistent with the characteristics of the real estate industry in the absence of AML/CFT controls. This is to be expected given the size of the sector, the wide availability and easy accessibility to services, the types of customers and the nature and high-value of transactions compared to other areas. In addition, the real estate sector has been highlighted internationally and domestically as being vulnerable to ML/TF activities.
23. The overall **medium-high** risk rating for the NZRB sector reflects its size, ease of access and demographic spread coupled with its higher risk products and services. The gambling and betting sector is recognised as being vulnerable to a number of high-risk ML/TF activities and industry specific risk factors.
24. The overall **medium-high** risk rating for HVDs is consistent with the use of high-value commodities in the laundering of criminal funds. This is to be expected given the size of the sector, the wide availability and desirability of high-value assets and commodities, the types of customers and the potential nature and high-value of transactions compared to other areas. In addition, the HVD sector has been highlighted internationally and domestically as being vulnerable to ML/TF activities.

Key vulnerabilities and high-risk factors

25. The Phase 2 SRA identifies 10 key ML/TF vulnerabilities and high-risk factors in line with domestic and international experience. Reporting entities should consider these vulnerabilities and high-risk factors **regardless** of the overall ML/TF risk of their business.
26. **When considering their own risk assessments, reporting entities should consider the vulnerabilities and high-risk factors and how they impact on their business.**
27. The vulnerabilities and high-risk factors presented in the list below are in no particular order, as each sector will prioritise them differently. **DIA strongly recommend that reporting entities are familiar with the vulnerabilities and high-risk factors described in full in Appendix 8.**
    - Trusts, shell companies and other legal arrangements
    - International payments
    - Cash and liquidity
    - Client accounts[4]
    - New payment technologies
    - Real estate
    - Anonymity and complexity
    - High-risk customers and jurisdictions
    - Politically exposed persons (PEPs) and high net worth individuals
    - Lack of ML/TF awareness

Predicate offending

28. The term "predicate offence" describes the offences underlying ML/TF activity. Taking direction from overseas experience and the findings of the NRA 2017, it is important that Phase 2 reporting entities are aware of the full range of criminal offending that can lead to ML/TF activity. The NRA 2017 stresses a move away from a focus on drug offending and broadens the scope of AML/CFT to better address fraud, tax evasion and other crime.

[4] The term client account and trust account refer to the same thing and are used interchangably in this document.

Domestic and international money laundering threat

29. The FIU estimates that NZD $1.35 billion is generated annually for laundering. This figure excludes transnational laundering of overseas proceeds and laundering the proceeds of domestic tax evasion. The transactional value of ML and the harm caused by ML and predicate offending is likely to be significantly more than this figure. New Zealand faces an unknown scale of ML generated from overseas proceeds of crime. The International Monetary Fund estimates that approximately 2–5% of global GDP (approximately USD $2 trillion) is the proceeds of crime.
30. Two key threat areas identified by the FIU are:
    - Specific transnational organised crime groups in which criminal offending is overseas but the group is linked to New Zealand
    - Overseas launderers and terrorism financiers not generally connected to New Zealand who may seek to misuse complex structures, such as a combination of New Zealand and offshore trusts, companies and charities

Terrorism financing

31. Given the increasingly important and dynamic nature of TF risk, this topic is covered in a dedicated section of the Phase 2 SRA and in Appendix 10. Although TF risk is assessed as low in New Zealand, it is prudent to provide guidance on the vulnerabilities and risks associated with the global issue of TF.

Importance of a good risk assessment

32. A core element of a reporting entity's AML/CFT regime is an adequate and effective risk assessment. The risk assessment is the foundation of a proportionate risk-based AML/CFT framework. DIA expects that reporting entities have a clear understanding of the ML/TF risks they face during the ordinary course of business and the vulnerabilities they are exposed to.

Part 1: Introduction

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

33. The Anti-Money Laundering and Countering 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 New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the FATF
    - To contribute to public confidence in the financial system
34. Under section 131 of the Act, one of the functions of each AML/CFT supervisor is to assess the level of risk of ML/TF across all the reporting entities that it supervises. To meet this responsibility, DIA has produced the Phase 2 SRA in 2017.

Purpose of the Phase 2 SRA

35. This is the first SRA produced by DIA in relation to the ML/TF risks in the Phase 2 sectors and has the following roles:
    - To help AML/CFT supervisors understand ML/TF risks within their sectors
    - To provide guidance to reporting entities on the risks relevant to their sector and to inform their risk assessments
    - To contribute to the ongoing FIU assessment of ML/TF risks in New Zealand
    - To meet the FATF Recommendations which require countries to adequately assess ML/TF risk and for gatekeepers (and other reporting entities) and provide adequate AML/CFT regulation and supervision

Three levels of risk assessment

36. Three levels of AML/CFT risk assessment are undertaken in New Zealand: national, sector, and individual reporting entity.
37. **National risk assessment (NRA)** – The NRA 2017 gives an overview of ML/TF issues affecting New Zealand from a law enforcement perspective using information from suspicious transaction reports (STRs), suspicious activity reports (SARs), and Asset Recovery Unit data. Information from government organisations, both domestic and international, also contributes to this assessment. The FIU develops and maintains indicators of ML/TF

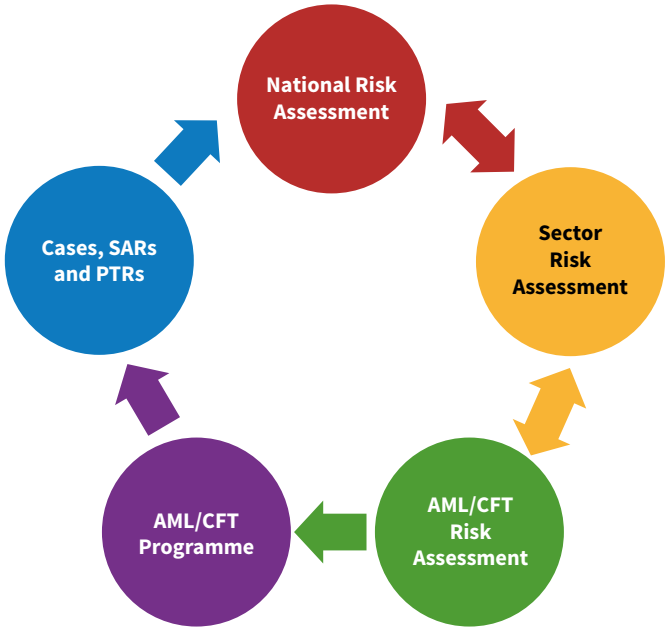
and publishes Quarterly Typology Reports. DIA recommends that reporting entities and staff with AML/CFT duties refer to the NRA 2017 and the Quarterly Typology Reports[5] to gain a better understanding of ML/TF. The NRA 2017 contains information on how money is laundered and how ML/TF impacts New Zealand. It also identifies the different types of "threats" (domestic and international) and how they exploit ML/TF vulnerabilities.

38. **Sector risk assessment (SRA)** – The AML/CFT supervisors have each produced a risk assessment for their own sectors. The Phase 2 SRA draws on a variety of sources including consultation with industry, communication with representative bodies, AML/CFT supervisory experience, international guidance, FIU risk assessments and Phase 1 reporting entity risk assessments. **DIA will conduct ongoing SRA work to continue to improve its understanding of the risks associated with the Phase 2 sectors, and inform reporting entities on risk indicators, trends and emerging issues.** The Phase 2 SRA may be revised regularly or on an ad-hoc basis, depending on how ML/TF risks affect the sectors.

39. **Reporting entity risk assessment** – 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 following:
    - The nature, size and complexity of its business
    - The products and services provided
    - The methods of delivery of these products and services
    - The types of customers they have
    - The countries they deal with
    - The types of institutions they deal with
    - Any other factors provided for in regulation

40. DIA encourage reporting entities to access international AML/CFT guidance, in particular the material produced by the FATF, APG and the Australian Transaction Reports and Analysis Centre (AUSTRAC – the organisation responsible for AML/CFT in Australia).

41. The following diagram outlines the inter-relationship of the risk assessment processes and how each informs the other. It shows the flow of cases, SAR and prescribed transaction report (PTR) data to the FIU and the mutually supportive sharing of information between the different types of risk assessment.



How reporting entities should use the SRA

42. All reporting entities should read the Executive Summary, Parts 1 to 5 and Part 12. This will help them understand the scope of the Phase 2 SRA and its limitations. Each reporting entity must review their sector-specific assessment (Parts 6 to 11) covering general risks and industry characteristics associated with ML/TF (noting that individual reporting entities will vary from the sector average). **More detailed "red flags", ML/TF typologies and potential mitigation will be included in later industry-specific guidance.**

43. The SRA will help reporting entities understand where DIA has identified vulnerabilities and higher-risk areas within the sector. If reporting entities operate in more than one sector, they must review and apply all relevant risk assessments.

44. Regardless of the ML/TF risk ratings in the Phase 2 SRA, when reporting entities assess their own ML/TF risk they should consider what level of risk they are willing to accept, sometimes referred to as "risk appetite".

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

45. *The AML/CFT Risk Assessment and Programme: Prompts and Notes* for DIA reporting entities document has been produced as a companion to the SRA to help reporting entities in meeting the requirements of the Act. These prompts and notes have been designed primarily for DIA-supervised small and medium-sized businesses and provide direction and supervisory expectation.
46. The prompts and notes contained in this document are not meant to replace critical thought or proper understanding of the ML/TF risks faced by reporting entities. They are not a "tick box exercise" but rather provide a framework for adequate and effective assessment and mitigation of risk. They do not constitute legal advice. After reading this guidance, if you still do not understand your obligations, you should seek legal advice, or contact your AML/CFT supervisor.

The risk-based regime

47. The regime introduced under the Act enables AML/CFT activities to be based on risk. The purpose of this risk-based approach is to make sure AML/CFT measures are proportionate, and reasonable resources are targeted towards high-risk and priority areas.
48. It is important to understand that in a risk-based regime not all entities will adopt the same AML/CFT controls. Context is everything and no two reporting entities are the same. Nor does it mean that a single incident of ML/TF invalidates the adequacy or effectiveness of a reporting entity's AML/CFT controls.
49. A risk-based regime recognises that **there can never be a zero-risk situation,** and reporting entities should determine the level of ML/TF exposure they can tolerate. This is not a legislative requirement but may help reporting entities in their risk management.

Stages of money laundering

50. It is worthwhile returning to some of the basics of ML/TF before considering ML/TF risk. ML is generally considered to take place in three phases: placement, layering and integration. TF shares many of the characteristics of ML but may also involve legitimate funds and usually involves smaller amounts.
    - **Placement** occurs when criminals introduce proceeds of crime into the financial system. This might be done by breaking up large amounts of cash into smaller sums that are then deposited directly into an account, or by purchasing shares or by loading credit cards. In some offences, such as fraud or tax evasion, placement is likely to occur electronically and may be inherent in the 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 various accounts across the world. 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: 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.

Other relevant legislation

51. **Crimes Act 1961** – Essentially, money laundering means concealing or disguising the proceeds of an offence. An "offence" means any offence (or any offence described as a crime) that is punishable under New Zealand law. Refer to section 243 of the Crimes Act for further details.
52. **Criminal Proceeds (Recovery) Act 2009 (CPRA)** provides for a civil restraint and forfeiture regime. Although this regime was in force at the time of the NRA 2010, data was only available on the initial six months of actions taken under the CPRA. The NRA 2017 findings have drawn on actions since the commencement of the CPRA.
53. **Financial Action Task Force (FATF)** – While not legislation, the FATF 40 Recommendations and 11 Immediate Outcomes represent a global standard of AML/CFT. Compliance with and demonstrated effective use of these standards are an important part of New Zealand's international reputation and ability to combat ML/TF. New Zealand will be evaluated on these standards and outcomes in 2020.

Part 2: Phase 2 AML/CFT sectors

Nature and size of the Phase 2 sectors

54. Although the Financial Transaction Reporting Act 1996 (FTRA) has been in place for 20 years, Phase 2 entities have not been subject to annual report obligations that would normally inform this section of the SRA. In future iterations of this document annual report data will provide an increasingly clearer picture of the nature and size of the Phase 2 sectors.

55. **Lawyers and conveyancers:** This sector comprises approximately 7,115 lawyers in firms and 992 sole practitioners giving 1,919 businesses. Of the 1,919 businesses, DIA anticipate approximately 1,570 expected reporting entities. The figures do not include overseas-based NZ lawyers, 'in-house' lawyers or barristers. The size distribution of businesses is approximately: 'Small' (1-19 employees): 981 (51%); 'Medium' (20-99 employees): 904 (47%); 'Large' (100+ employees): 34 (2%).

56. **Accountants:** This sector comprises approximately 2,000 'Approved Practice Entities (in various legal forms) and a further approximately 433 book-keepers and Certified Practising Accountants, giving a total of 2,433 businesses. Of these 2,433 businesses, DIA expect approximately 2,220 to be reporting entities. The size distribution of businesses is approximately: 'Small': 1,782 (73%); 'Medium': 549 (23%); 'Large': 102 (4%).

57. **Real estate agents:** This sector comprises approximately 15,000 licensed real estate agents operating in New Zealand. Half of these are employees of franchises. Currently, there are 860 real estate companies with an active licence and 148 agencies operating as sole traders.

58. **NZRB:** NZRB report they provide racing and sports betting services to approximately 180,000 account-based customers online, over the phone, on-course and across 700 retail outlets and touch points (ranging from a standalone TAB (Totalisator Agency Board) outlet through to a self-service facility).

59. **High-value dealers:** Given the size, nature and diversity of this sector and its previous and continued unregulated nature, it is difficult to get an accurate picture of the nature and size of this sector.

Part 3: Methodology

60. The Phase 2 SRA works on two levels: it provides an assessment of ML/TF risk, and it identifies key ML/TF vulnerabilities. For a more detailed explanation of the methodology, please refer to Appendix 1.

Methodology – assessment of risk

61. DIA assessed ML/TF risk for each sector using the variables contained in section 58(2)(a)–(f) of the Act and in the *Risk Assessment Guideline*[6]. The six variables are:
    - Nature, size and complexity of the business
    - Products/services
    - Methods for delivery of products/services
    - Customer types
    - Country risk
    - Institutions dealt with (if relevant)

62. For each of these variables, DIA considered a number of ML/TF questions. The responses to these questions helped guide the assessment of **inherent** risk for each variable. This was done in combination with structured professional knowledge, domestic and international guidance, and input gathered during consultation. At the end of this process, DIA assigned an overall assessment of inherent ML/TF risk to each sector using ratings of low, medium, medium-high or high (see Appendices 2 to 7).

63. To simplify the SRA process, DIA did not assess **residual** risk. Reporting entities, as part of their AML/CFT programme, are expected to address the **inherent** risks identified in their AML/CFT risk assessment.

Methodology – identification of key vulnerabilities and high-risk factors

64. For the Phase 2 SRA DIA identified five key vulnerabilities and five high-risk factors, which were informed by the NRA 2017 and structured professional knowledge. Selection was based on subject matter expertise, supervisory experience, domestic and international guidance and their relative commonality across the sectors.

[6] http://bit.ly/2iL7Spp

Part 4: Predicate offending and SARs

65. Predicate offences are the crimes underlying ML/TF activity and it is important that the various types of predicate offence are understood. The tables below are taken from FIU research.

Domestic threat

Threat	Action	Phase	Description
Drug offending	• Self-laundering • Laundering by close associates • Laundering by professional services and HVDs • 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, high-value commodities
		Nature of offending	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 (e.g. in business, company or market)
		Layering	Use of companies and business, likely to be professionally facilitated. Movement of funds offshore through complex networks set up by professional ML facilitators
		Integration	Real estate, assets
		Nature of offending	Potentially higher-value transactions of illicit funds per offender; wide variety of predicate offending
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 predicate offence (e.g. in business, company or market)
		Layering	Nominees, trusts, family members or third parties etc. Movement of funds offshore through complex networks set up by professional ML facilitators. Also via gambling and co-mingling with apparently legitimate businesses
		Integration	Reinvestment in professional businesses, real estate, high-value commodities
		Nature of offending	Business vehicles most commonly used to commit predicate offence

International threat

Threats	Description of likely methods
Drug offending connected to New Zealand	• Remittance and alternative remittance • Movement of funds through financial institution, DNFBPs, businesses and assets • Trade-based laundering through merchandise trade
Corruption and other economic crime	• Trade-based laundering • Remittance and alternative remittance • Attempts to seek safe haven (either in person as fugitives or to store proceeds while maintaining control from offshore)
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 laundering using trade in services and legal structures
Organised crime and economic criminals with no link to New Zealand	• Use of legal structures and alternative payment platforms
Organised crime	• Remittance and alternative remittance • Movement of funds through financial institution, DNFBPs, businesses and assets • Trade-based laundering through merchandise trade
Groups raising capital from domestic sympathisers – TF	• Remittance and alternative remittance
International controllers	• Remittance and alternative remittance • Trade-based laundering
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) • Trade-based laundering using trade in services and legal structures

66. The FIU reports that organised crime groups have access to ML networks that can be sophisticated and hard for law enforcement to combat. They are likely to seek to abuse New Zealand structures to carry out criminal activity, launder proceeds, and act as a conduit to move and layer criminal funds. New Zealand's reputation as a stable, low-risk country is likely to be exploited and degraded by overseas offenders abusing the financial system and New Zealand companies and trusts.
67. Drug offending generates large amounts of cash and may involve fairly simple ML methods. The greater financial sophistication of fraud offenders can lead to more complex ML, which may make detection more difficult. This is exacerbated by under-reporting by the victims of fraud. Individual criminals are assessed as the greatest generator of proceeds of crime (both of drug crime and fraud) and as being associated with the most sophisticated ML/TF methods.
68. The FIU has produced a useful guide for the submission of STRs – *Suspicious Transaction Guideline 2013*[7] – which will be updated for SARs. The guideline contains many indicators and warnings, or red flags, of ML/TF activity that reporting entities should consider when assessing ML/TF risk.

[7] http://bit.ly/2zxU4Jj

Part 5: Key ML/TF vulnerabilities and high risk factors

Key vulnerabilities

69. The key Phase 2 ML/TF vulnerabilities identified below impact in varying degrees on each of the Phase 2 sectors. Reporting entities are encouraged to consider applicable vulnerabilities (detailed in Appendix 8) when conducting their risk assessment.

Vulnerability	Comment
Cash and liquidity	Cash continues to be an easy and versatile method of transferring value. This includes the use of money mules, cash couriers and bulk movements. Also, the purchase of high-value goods with cash is an easy method of transferring value and disguising/concealing the proceeds of crime. Cash-intensive businesses, where its use is considered normal, lend themselves to all phases of ML. Customers that use cash or highly liquid commodities in their businesses, present a significant risk of ML/TF.
New payment technologies	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, easy and anonymous movement of funds across cross-borders. This vulnerability also includes alternative banking platforms and e-currencies.
Real estate	Professional services required for real estate transactions can occur across most of the Phase 2 sectors (apart from HVDs and NZRB). Real estate is a high-value asset often used domestically and internationally to launder and invest criminal proceeds. Real estate poses significant ML/TF vulnerability across the Phase 2 sectors.
Anonymity and complexity	Anonymity/complexity can take the form of identity fraud, anonymous products, disguised beneficial ownership or executive control, persons on whose behalf a transaction is conducted, non-face-to-face customer due diligence (CDD), use of intermediaries and abuse of electronic verification.
Lack of ML/TF awareness	Phase 2 sectors do not have a history of AML/CFT awareness. Not being able to recognise ML/TF is a significant vulnerability that leaves a reporting entity open to misuse for ML/TF. Reporting entities need to promote an AML/CFT culture and increase and develop their knowledge of the ML/TF environment.

Key high-risk factors

70. The key Phase 2 ML/TF high-risk factors identified below impact in varying degrees on each of the Phase 2 sectors. Reporting entities are encouraged to consider applicable high-risk factors (detailed in Appendix 8) when conducting their risk assessment.

High-risk factor	Comment
Trusts, shell companies and other legal arrangements	The uses of nominee directors and shareholders, shell companies, limited partnerships, or trusts to create complex legal structures and conceal beneficial ownership are well-recognised ML/TF typologies. New Zealand's open business environment, its registration requirements for financial service providers operating offshore, and the common use of trusts make this activity especially vulnerable to ML/TF. In particular, shell companies and trusts should be considered high-risk.
International payments	The value, volume and velocity of money moving through the international payment systems continues to present ML/TF opportunities. Facilitating or receiving international payments, combined with other ML/TF vulnerabilities, presents a high-risk of ML/TF.
Client accounts	A client account, or trust account, is attractive to criminals as it can facilitate access to the wider financial system, help conceal ownership of criminally derived funds, and provide a link between different ML phases and typologies. Providing or managing client accounts presents ML/TF risk.
High-risk customers and jurisdictions	Certain customers are considered high-risk – for example, trusts, non-profit organisations, remitters* and cash-intensive businesses. Criminals may be attracted to certain businesses because they provide access to other facilitators of crime such as transport or high-value commodities. Countries with weak/insufficient AML/CFT measures, high degrees of bribery and corruption, tax evasion, TF, conflict zones and organised crime present a clear ML/TF risk. High-risk customers from high-risk countries compound ML/TF risk.
PEPs and high net worth individuals	This category includes politically exposed persons (PEPs) and their relatives/close associates, high net worth customers, and people in control of multinational organisations. PEPs, especially in combination with high-risk countries, present a range of ML/TF risks with the potential for far-reaching and serious consequences.

*Note: Remitters are included in the list of high-risk factors as a typology and not as an indication of the industry as a whole.

71. Key vulnerabilities and high-risk factors do not operate in isolation but in combination, resulting in a compounding risk of ML/TF. Context is essential in identifying and determining the degree of ML/TF vulnerability and risk. For instance, a reporting entity may be assessed as presenting a low inherent risk of ML/TF as part of its ordinary course of business. However, if it does not have adequate or effective AML/CFT awareness, this vulnerability could leave it open to abuse by not recognising ML/TF activity when it occurs.
72. DIA encourage reporting entities to research their own business-specific vulnerabilities and risks, and to have regard to current guidance – for example, via DIA newsletters and the FIU Quarterly Typology Reports.
73. The following table shows the key ML/TF vulnerabilities and high-risk factors for each Phase 2 sector.

Vulnerability/high-risk factor	Lawyers	Conveyancers	Accountants	Real estate agents	New Zealand Racing Board	High-value dealers
Cash and liquidity					✓	✓
New payment technologies					✓	✓
Real estate	✓	✓	✓	✓		
Anonymity and complexity	✓		✓	✓	✓	✓
Lack of ML/TF awareness	✓	✓	✓	✓	✓	✓
Trusts, shell companies and other legal arrangements	✓	✓	✓	✓		
International payments	✓		✓	✓		
Client accounts	✓	✓	✓	✓		
High-risk customers and jurisdictions	✓		✓	✓		
PEPs and high net worth individuals	✓		✓	✓		

Part 6: Sector risks – lawyers

Overall inherent risk: Medium-high

Both domestic and international evidence and guidance highlight the ML/TF risks presented by the legal sector. The easy access and wide geographic spread of legal services, coupled with lawyers' gatekeeper role and use in every phase of ML/TF and in many different ML/TF typologies, means this sector presents a medium-high inherent risk of ML/TF.

74. Lawyers will be covered by the Act from 1 July 2018. Industry specific guidance has been produced for this sector.

75. Lawyers in New Zealand offer a wide range of services, many of which are attractive to criminals to launder their proceeds of crime. Lawyers may be complicit in the ML/TF activity, they may be wilfully blind or corrupt, they can be unwittingly involved, or they can be entirely innocent and unknowingly involved.

76. Lawyers may be used at all stages of ML/TF. Because of its wide availability and the ease of accessing products and services, the legal professional sector is a well-recognised avenue for ML/TF, with demonstrated involvement evidenced by FIU data.

77. The medium-high risk rating is consistent with international experience and expectations, given lawyers' exposure to ML/TF vulnerabilities. The consequences of such vulnerabilities can be wide ranging and result in significant financial, reputational and even political impact.

78. The FIU reports that between the commencement of the FTRA and December 2015 it received 174 STRs from lawyers. Inclusion into the Act will require this sector to fully embrace AML/CFT.

79. DIA recognise that lawyers carry out a diverse range of activities and as a result some generalisations have been made.

Nature, size and complexity

80. Lawyers need to hold a practising certificate from the New Zealand Law Society to practise in New Zealand. Lawyers can operate as sole practitioners, within law firms or as in-house lawyers. Lawyers must be approved by the New Zealand Law Society to operate a trust account. The services provided by lawyers are widely available in New Zealand.

81. The legal sector comprises approximately 7,115 lawyers in firms and 992 sole practitioners giving 1,919 businesses. Of the 1,919 businesses, DIA anticipate approximately 1,570 expected reporting entities. The figures do not include overseas-based NZ lawyers, 'in-house' lawyers or barristers. The size distribution of businesses is approximately: 'Small' (1-19 employees): 981 (51%); 'Medium' (20-99 employees): 904 (47%); 'Large' (100+ employees): 34 (2%).

82. The legal profession can provide criminals access to expertise and facilities they would not have themselves, which can create an environment that conceals, disguises or hides the proceeds of crime. Legal professionals add respectability to transactions and activities, and there is a perception that legal professional privilege will delay, obstruct or prevent investigation or prosecution by authorities. Involvement of a lawyer also provides a further step in the chain of transactions and activities.

83. Lawyers have professional obligations under the Lawyers and Conveyancers Act 2006 and the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008. These obligations include:
    - Not assisting any person in an activity the lawyer knows to be fraudulent or criminal
    - Not knowingly assisting in the concealment of fraud or crime
    - Disclosing information that relates to the anticipated or proposed commission of a crime punishable by imprisonment for three years or more

84. These professional obligations may assist with the AML/CFT regime. However, their primary purpose is not to detect and deter ML/TF but to maintain confidence in the legal sector and to protect consumers of legal services.

Products and services

85. Along the spectrum of products and services offered by the legal professional sector the FATF has identified a number of ML typologies:
    - Misuse of client accounts
    - Property purchases
    - Creation of companies and trusts
    - Management of companies and trusts
    - Managing client affairs and making introductions
    - Certain types of litigation
    - Creation of charities and non-profit organisations
86. Most of these typologies are reflected in the ML/TF vulnerabilities and high-risk factors identified in this SRA. It is beyond the scope of this assessment to list and assess every service provided by legal professionals in depth. However, reporting entities, as part of their risk assessment process, should assess the ML/TF vulnerabilities and high-risk factors associated with each of their products/services.
87. Lawyers who operate a trust account are also subject to oversight from the New Zealand Law Society. A lawyer's trust account may be audited by the New Zealand Law Society but the primary aim is to ensure proper conduct in respect of protecting clients' money and to minimise risk to the Lawyers' Fidelity Fund rather than AML/CFT.
88. The following table lists four main vulnerabilities and five main predicate offences that were identified (via STRs) by legal professionals during consultation with the FATF.

FATF – Vulnerability	FATF – Predicate offence
Purchase and sale of real estate	Corruption and bribery
Formation, merger, acquisition of companies	Fraud
Formation of trusts	Tax crimes
Providing company or trust services	Trafficking in drugs
	Unexplained levels of cash/private funding

89. The broad range of professional services offered by lawyers can enable money launderers to manage all their financial and business affairs in one place. For instance, a money launderer can arrange for a professional to set up a company or trust and then also act, or arrange for a third-party to act in a proxy role, including acting as a trustee. With the fiduciary role appearing legitimate, the money launderer can conduct a range of criminal activities or asset transfers at arm's length from both regulatory and law enforcement agencies. Tracking and tracing the beneficial owner is time consuming and information on beneficial ownership may be difficult to find.
90. As a barrister cannot receive or hold money or other valuable property for or on behalf of another person, they are not permitted to operate a trust account. Accordingly, barristers cannot hold fees in advance as these are deemed to be trust funds until an invoice is issued for work and services undertaken.
91. **Legal professional privilege** – The Act does not require any person (lawyer or otherwise) to disclose any information that the person believes, on reasonable grounds, is a privileged communication. Further guidance on this matter is included in industry-specific guidance.

Methods of delivery

92. Non-face-to-face application for, and delivery of, products/services are more vulnerable to ML/TF activity than face-to-face delivery. Reporting entities should assess the ML/TF vulnerabilities associated with the methods of delivery. Non-face-to-face methods of delivery include overseas on-boarding of clients, the use of intermediaries and the use of other professional services/gatekeepers.

Customer types

93. Lawyers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 8: Key ML/TF vulnerabilities and high-risk factors). Access to legal services and activities by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for operating in New Zealand.
94. The use of legal services and activities by 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 invest and the ease of fund movement through New Zealand facilities.

Country risk

95. Country risk comes from dealing with persons or entities in jurisdictions with poor or insufficient AML/CFT measures. Lawyers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, lawyers should consider whether the country is a conflict zone or if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Lawyers should consider not only higher-risk countries but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.
96. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[8]

Institutions dealt with

97. Lawyers will have exposure to a number of different institutions, including other gatekeepers. Lawyers, depending on the services and advice they provide, should also consider reviewing the SRAs produced by the FMA and RBNZ for additional information on the ML/TF risks when dealing with the financial and banking sector.
98. Where multiple gatekeepers act as intermediaries in a chain for the same customer(s), activity or transaction, this is a significant ML/TF vulnerability.

[8] http://bit.ly/2hOTHPk

Part 7: Sector risks – conveyancers

Overall inherent risk: Low

The values and potential velocity of conveyancing activity and exposure to the high-risk real estate sector present ML/TF vulnerabilities. However, conveyancers' limited exposure to high-risk products/services, and their interaction with generally lower-risk customers and institutions, means this sector presents a low inherent risk of ML/TF.

99. Conveyancers will be covered by the Act from 1 July 2018. Industry specific guidance has been produced for this sector.

100. The low risk rating for conveyancers considers that they do not typically provide the range of services that other gatekeeper sectors may have. However, they do have a reasonable level of ML/TF risk due to the size of transactions by value and exposure to the real estate sector.

101. The specialist knowledge needed to complete a real estate transaction means that almost all New Zealand real estate transactions are facilitated by an experienced lawyer or conveyancer. In particular, the requirement from Land Information New Zealand (LINZ) to transfer titles online significantly limits access by laypersons, including money launderers, to conduct real estate transactions without a gatekeeper professional. LINZ reports that almost no title transfers are conducted by laypersons.

Nature, size and complexity

102. The legal sector comprises approximately 7,115 lawyers in firms and 992 sole practitioners giving 1,919 businesses. Of the 1,919 businesses, DIA anticipate approximately 1,570 expected reporting entities. Many of these will provide conveyancing services.

103. The NZ Society of Conveyancers (NZSOC) is the professional body representing conveyancing practitioners in New Zealand. Its role is to represent, promote and regulate the conveyancing profession. The Lawyers and Conveyancers Act 2006 came into force on 1 August 2008, which provides the framework for the Conveyancing Profession in New Zealand. Within this sector there are currently 19 conveyancing firms in New Zealand.

Products and services

104. As with lawyers, conveyancers can provide criminals access to expertise and facilities they would not have themselves, which can create an environment that conceals, disguises or hides the proceeds of crime – for instance, the use of client accounts. The involvement of a conveyancer can add respectability to transactions and activities, and also adds a further step in the chain of transactions and activities to frustrate investigation by law enforcement.

Methods of delivery

105. 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 methods of delivery.

106. LINZ operates an electronic registration service. Only lawyers and conveyancers are able to register to use the service. Upon the exchange of final settlement, the vendor's lawyer releases the title and the purchaser's lawyer will submit the registration for the title.

107. LINZ obligations require photo identification for the purchaser (driver licence or passport). The identification must be verified but not necessarily by the lawyer. However, the lawyer must be satisfied that the identity is correct. LINZ conducts audits, and lawyers are required to hold records for seven years. Purchasers and sellers can submit written registration in certain situations.

Customer types

108. Conveyancers need to know their customers and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 8: Key ML/TF vulnerabilities and high-risk factors). Access to conveyancing services and activities by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF. The use of conveyancing services and activities by 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 invest and the ease of fund movement through New Zealand facilities.

Country risk

109. A significant proportion of transactions in the conveyancing sector are domestic payments. Most customers are likely to be New Zealand residents, although some overseas resident customers are to be expected, resulting in overseas payments and pay-outs.
110. Country risk comes from dealing with persons or entities in jurisdictions with poor or insufficient AML/CFT measures. Conveyancers should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, conveyancers should consider whether the country is a conflict zone or if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Conveyancers should consider not only higher-risk countries but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.
111. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme.
112. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[9]

Institutions dealt with

113. Conveyancers will have limited exposure to different institutions and other gatekeepers. They may wish to review the SRAs produced by the FMA[10] and RBNZ[11] for additional information on the ML/TF risks when dealing with the financial and banking sector.
114. Where multiple gatekeepers act as intermediaries in a chain for the same customer(s), activity or transaction, this is a significant ML/TF vulnerability.

Part 8: Sector risks – accountants

Overall inherent risk: Medium-high

The easy access and wide geographic spread of accounting services, coupled with accountants' gatekeeper role and use in every phase of ML/TF and in many different ML/TF typologies, means this sector presents a medium-high inherent risk of ML/TF.

115. Accountants will be covered by the Act from 1 October 2018. Further industry-specific guidance will provide more detail on the risks and vulnerabilities of this sector.
116. Accountants may be used at many stages of ML/TF. Because of their wide availability and the ease of accessing products and services, the accountancy sector is a well-recognised avenue for ML/TF. The medium-high rating is consistent with international experience and expectations given accountants' exposure to ML/TF vulnerabilities. The consequences of such vulnerabilities can be wide-ranging and result in significant financial and reputational impact.
117. DIA recognise that accountants are not all the same and the activities they carry out are diverse. For the purposes of this SRA, some generalisations have been made.
118. The FIU reports that between the commencement of the FTRA and December 2015 it received seven STRs from accountants. Inclusion into the Act will require the accountancy sector to fully embrace AML/CFT obligations, especially as the risk of money launderers using the accountancy sector is likely to increase as it becomes more difficult to launder money through traditional financial institutions.
119. As it is not a requirement for accountancy service providers to be registered, it may be difficult to identify all potential reporting entities. Many accountancy service providers will be unfamiliar with regulation beyond their professional standards. Many are also not members of a professional or industry body.

[9] http://bit.ly/2hOTHPk

[10] http://bit.ly/2jTH2Pg

[11] http://bit.ly/2hPOaIa

120. It is hard to define who falls within the accountancy sector. Unlike lawyers, who are required to hold a practising certificate, anyone can establish an accountancy firm. The majority of people in the accountancy sector operate as either sole practitioners or in small firms, with a range of qualifications, experience and skills.

Nature, size and complexity

121. The accountancy sector in New Zealand is large and covers a wide spectrum of practitioners, from large multi-national accountancy firms to individual bookkeepers and the accountancy sector has several industry bodies. These bodies vary in their size and in the scope of the services they provide for their members. While industry bodies cover the majority of people providing accountancy services, not all people providing these services are registered with an industry body. While chartered accountants have to be members of Chartered Accountants Australia and New Zealand (CAANZ), it is not a requirement to be a member of an industry body.
122. The sector comprises approximately 2,000 'Approved Practice Entities'[12] (in various legal forms) and a further approximately 433 book-keepers and Certified Practising Accountants, giving a total of 2,433 businesses. Of these 2,433 businesses, approximately 2,220 reporting entities are expected to require compliance with the AML/CFT regime. The size distribution of businesses is approximately: 'Small': 1,782 (73%); 'Medium': 549 (23%); 'Large': 102 (4%).
123. There are also an estimated 500 members of the Accountants and Tax Agents Institute of New Zealand (ATAINZ), and many ATAINZ members are also members of CAANZ.

Products and services

124. Accountants regularly deal with large sums of money and set up and manage trusts and companies. The professional services provided by accountants are attractive to money launderers because they can give the impression of respectability, legitimacy or normality, especially in dealing with large transactions, which are common for accountants. They also create an additional step in the ML chain that can hinder detection and investigation, and obscure the beneficial ownership of the money.
125. The services provided by accountants can allow access to legitimate services and techniques that money launderers would not normally have access to, such as making introductions (opening accounts), or facilitating setting up of structures such as trusts or companies. The role of accountants in this activity may be complicit or unwitting.
126. Accountants can provide a broad range of products and services, many of which can be exploited to launder funds. This includes:
    - Acting as a formation agent of legal persons or arrangements (such as trusts)
    - Arranging for a person to act as a nominee shareholder or trustee or a nominee director in relation to legal persons or arrangements
    - Providing a registered office, a business address, a correspondence address, or an administrative address for a company, a partnership, or any other legal person or arrangement
    - Assist with purchasing of large assets or businesses
    - Managing client funds, accounts, securities or other assets
    - Preparing for, or carrying out, real estate transactions on behalf of a customer
    - Preparing for, or carrying out, transactions for customers related to creating, operating or managing companies
    - Bookkeeping – recording transactions, accounts receivable, banking funds, entering financial transactions into software, producing reports (balance sheets etc.)
    - Tax services (in association with tax evasion)
    - False accounting
    - Setting up and managing charities

[12] Chartered Accountants Australia and New Zealand

Methods of delivery

127. ML/TF risk is present if customers can access accountancy products and services through indirect methods. Anonymity risks occur when products and services are provided to customers via intermediaries and other methods where the reporting entity does not have face-to-face contact with the customer.

Customer types

128. Accountants need to know all their customers well and be aware of the ML/TF risks associated with them. Reporting entities should assess the ML/TF vulnerabilities associated with particular customer types (see Appendix 8: Key ML/TF vulnerabilities and high-risk factors). Access to accountancy services and activities by non-residents (see the "Country risk" section below) is also a factor that can increase the risk of ML/TF if there are no genuine reasons for operating in New Zealand. The use of accountancy services and activities by 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 invest and the ease of fund movement through New Zealand facilities.

Country risk

129. Country risk comes from dealing with persons or entities or in jurisdictions with poor or insufficient AML/CFT measures. Accountants should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, accountants should consider whether the country is a conflict zone or if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Accountants should consider not only higher-risk countries but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.
130. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme.
131. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[13]

Institutions

132. As gatekeepers, accountants will have exposure to a number of different institutions, including other gatekeepers. Accountants, depending on the services and advice they provide, should also consider reviewing the SRAs produced by the FMA[14] and RBNZ[15] for additional information on the ML/TF risks when dealing with the financial and banking sector.
133. Where multiple gatekeepers act as intermediaries in a chain for the same customer(s), activity or transaction, this is a significant ML/TF vulnerability.

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

[14] http://bit.ly/2jTH2Pg

[15] http://bit.ly/2hPOaIa

Part 9: Sector risks – real estate agents

Overall inherent risk: Medium-high
The use of real estate in ML/TF is well-known and demonstrable. FIU research indicates real estate is the ML asset of choice. In addition, this sector has low levels of AML/CFT awareness and sophistication. As such, this sector presents a medium-high inherent ML/TF risk.

134. Real estate agents will be covered by the Act from 1 January 2019. Further industry-specific guidance will provide more detail on the risks and vulnerabilities of this sector.

135. The real estate sector is a well-recognised avenue for ML/TF. Real estate is readily available in New Zealand and is a very active market. Purchasing both residential and commercial property is a reliable and profitable investment strategy. The FIU considers that the real estate sector is highly vulnerable to ML. It also considers that international exposure is significant, and there is a risk that New Zealand real estate is being abused by offshore criminals.

136. The medium-high rating is consistent with these characteristics and the sector's demonstrated involvement with ML, as evidenced by FIU data. It is also consistent with international experience and expectations given the real estate sector's exposure to ML/TF vulnerabilities. The consequences of such vulnerabilities can be wide ranging and result in significant financial, reputational and even political impact.

137. The professional services provided by the real estate sector are attractive to money launderers because:
    - They are widely available, and they can give the impression of respectability, legitimacy, or normality
    - Offenders can move large amounts of illicit funds in a single transaction without raising suspicion, and the duration of the relationship with a real estate agent is short-lived
    - They can create additional steps in the ML/TF chain that can hinder detection and investigation
    - They provide access to services and techniques that money launderers would not normally have access to or be comfortable doing, such as buying and selling property
    - The large number of agents means that offenders can seek out a suitable agent to target

138. The FIU reports that between the commencement of the FTRA and December 2015 it received 56 STRs from real estate agents. Inclusion into the Act will require this sector to fully embrace AML/CFT and the submission of SARs.

Nature, size and complexity

139. Real Estate Institute of New Zealand (REINZ) and Quotable Value New Zealand (QV) data indicates that around $60 billion of real estate is transacted per annum. There are approximately 15,000 licensed real estate agents operating in New Zealand, half of these are employees of franchises. Currently, there are 860 real estate companies with an active licence and a further 102 real estate companies that have a suspended licence (not currently trading). There are 148 agencies operating as sole traders.

140. Real estate agents or agencies need to be registered to carry out "real estate agency work" (see section 6 of the Real Estate Agents Act 2008). Real estate agents can operate as a company or a sole trader. Both can employ salespersons and may be a member of a franchise group.

141. Real estate agents operate from small towns to big cities, with widely different skill sets and experience. Most work for small companies, many are franchisees and some are sole traders. A very small amount act as agents for foreign purchasers.

142. The buoyant housing market in New Zealand, especially in the Auckland region, has likely increased the opportunities for exploitation of the real estate sector by transnational criminals. This has been observed in other comparable jurisdictions as well, such as the United Kingdom, United States, Canada and Australia.

Products and services

143. Real estate is an attractive option for money launderers because it can be used both in layering and integrating proceeds of crime by re-entering the legitimate economy. In particular, a scheme involving real estate may be appealing in the following ways:
    - It may be the ultimate purpose of the ML (i.e. to use proceeds as real estate to enjoy). This may send a sign to communities that crime pays and enhances the status of the offender
    - A sale of property can be used to explain a source of funds
    - Transactions are large, so large sums may be laundered through real estate vehicles.
    - Beneficial ownership may be hidden using gatekeepers – for example, legal structures such as trusts, nominees or companies These techniques may appear to be normal practice and may not attract heightened suspicion
    - Real estate is a speculative market where values may be difficult to assess, particularly in atypical properties. This may make under- or over-valuing possible to enable ML techniques
    - Real estate transactions provide access to various financial vehicles (such as mortgages) through which to launder funds
    - Property, such as commercial property, rental property or farms, may provide legitimate income with which to co-mingle illicit proceeds
144. Once real estate has been bought, it can be used as security for a loan, or resold, which "integrates" the proceeds of crime into the legitimate economy. Very large sums may be laundered through real estate vehicles

Methods of delivery

145. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Transactions made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.
146. This is particularly true when dealing with customers in higher-risk overseas jurisdictions. Transnational real estate services are low cost and are readily available online. Services can be provided anonymously, and these are being marketed to offshore clients. However, both the source of offshore funds and the beneficial owner can be difficult to validate, with money launderers taking advantage of cross-jurisdictional language, identity and legal complexity barriers.

Customer types

147. Real estate agents are more customer-facing than many other sectors, so they have better oversight of their customers and transactions to identify suspicious activity (see Appendix 8: Key ML/TF vulnerabilities and high-risk factors). For instance, they may have insight as to whether a customer is suspiciously under- or over-valuing properties (which may indicate tax evasion) or how long or short a period a customer is holding onto a property for (which may indicate property "flipping" to disguise the origin of the funds). They also may have oversight of a customer's property portfolio and their use of different lawyers or financial institutions (particularly when representing international investors), which would not be visible by any other reporting entity.
148. Some of the main customer risk categories identified by the FATF for real estate agents are:
    - Significant and unexplained geographic distance between the agent and the location of the customer
    - Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interest
    - Customers that are cash-intensive businesses
    - Customers who use intermediaries who are not subject to adequate AML/CFT laws and measures and who are not adequately supervised
    - Customers who are PEPs

149. Agents should be aware of the possibility of relationships between the sellers and buyers of a property who may be colluding to create a paper transaction for dishonest purposes.
150. It is not uncommon for a nominee to be used and the beneficial owner to be added to the sale and purchase agreement at the last minute. For example, a family may be deciding whether to place the purchase in the name of a trust. This presents challenges in identifying the true beneficial owner or effective controller of the customer.

Country risk

151. Access to real estate services and activities by non-residents is a factor that can increase the risk of ML/TF if there are not genuine reasons for operating in New Zealand. The buying and selling of real estate by PEPs also heightens ML/TF risk due to their potential exposure to fraud, bribery and corruption. Likewise, high net worth customers from overseas pose a higher-risk due to the larger amounts they have available to invest and the ease of fund movement through New Zealand real estate.
152. Country risk comes from dealing with persons or entities in jurisdictions with poor or insufficient AML/CFT measures. Real estate agents should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, real estate agents should consider whether the country is a conflict zone or if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. Real estate agents should consider not only higher-risk countries but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.
153. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme.
154. Reporting entities should refer to the *Countries Assessment Guideline*[16] produced by the AML/CFT supervisors.

Institutions

155. As a gatekeeper, real estate agents will have exposure to a number of different institutions, including other gatekeepers. Depending on the services and advice they provide, real estate agents should also consider reviewing the SRAs produced by the FMA[17] and RBNZ[18] for additional information on the ML/TF risks when dealing with the financial and banking sector.
156. Where multiple gatekeepers act as intermediaries in a chain for the same customer(s), activity or transaction, this is a significant ML/TF vulnerability.

[16] http://bit.ly/2hOTHPk
[17] http://bit.ly/2jTH2Pg
[18] http://bit.ly/2hPOaIa

Part 10: Sector risks – New Zealand Racing Board

Overall inherent risk: Medium-high

The overall **medium-high** risk rating for the NZRB sector reflects its size, ease of access and demographic spread coupled with its higher risk products and services. The gambling and betting sector is recognised as being vulnerable to a number of high-risk ML/TF activities and industry specific risk factors.

157. NZRB will be covered by the Act from 1 August 2019. Further industry-specific guidance will provide more detail on the risks and vulnerabilities of this sector.

158. The gambling and betting sector is a well-recognised avenue for ML/TF. Access to gambling services and products is easy and widespread. Gambling services are provided online, over the phone, on-course and across hundreds of retail outlets and touch points. Cash is still widely used, and betting accountants can be used to pool, move and disguise criminal proceeds.

159. The medium-high rating is consistent with these characteristics and with international experience and expectations, given the gambling sector's exposure to ML/TF vulnerabilities.

160. The products and services provided by the gambling sector are attractive to money launderers because:
- They are widely available, and they can give the impression of legitimacy, or normality
- Offenders can move large amounts of illicit funds in a single transaction without raising suspicion, and the duration of the business relationship is short-lived
- Gambling activity can create additional steps in the ML/TF chain that can hinder detection and investigation
- The large number of providers of gambling services and products means that offenders can seek out a suitable provider to target

161. NZRB has not previously been subject to AML/CFT supervision and obligations. Inclusion into the Act will require this sector to fully embrace AML/CFT and the submission of SARs.

162. NZRB is an independent statutory entity governed by the Racing Act 2003 and is subject to a range of public accountability and transparency requirements. It has broad statutory obligations and responsibilities to both the racing industry and the community.

163. All betting through TAB outlets, pubs, clubs and on racecourses is provided under contract. NZRB's operating model relies on contractors to operate TAB outlets, with NZRB remaining liable for actions carried out by TAB outlets.

Nature, size and complexity

164. NZRB provides betting services under contract through various TAB outlets (agencies, pubs, clubs, and on racecourses), which represent 95% of the retail network. The remaining 5% are part of the NZRB branch network, where staff are employed by NZRB.

165. NZRB reports that they provide racing and sports betting services to approximately 180,000 account-based customers online, over the phone, on-course and across 700 retail outlets and touch points (ranging from a standalone TAB store through to a self-service terminal in a pub). The TAB supports betting on more than 68,000 domestic and imported thoroughbred, harness and greyhound races each season, as well as on approximately 29,000 domestic and international sporting events. In addition, NZRB also exports over 10,200 New Zealand races a year. NZRB also has betting agreements with a number of national sports organisations allowing it to take betting on 33 sports.

166. The nature, size and complexity of NZRB's services and its methods of delivery present ML/TF risks. The operating model means that NZRB contractors have a high level of autonomy with limited oversight of their AML/CFT functions. However, in their branch networks, where all staff are employees of NZRB, there is much greater opportunity for AML/CFT obligations to be met.

Products and services

167. NZRB activities fall into four broad products/services, which are provided across a range of categories:
- Bet: Selling bets on racing or sports events to customers
- Voucher: Selling betting vouchers that can be redeemed for a bet, cash, or deposited into an account
- Account: Providing accounts to allow customers to bet online and over the phone
- Gaming: Providing Class 4 gaming machines in-store **(this is not covered by the Act)**

168. The products and services listed above can present ML/TF risk. For instance, there is potential to use illegally obtained funds to purchase and subsequently redeem high-value vouchers or to place large bets. Betting structures (such as syndicates or aggregating services) can be used to obscure the origin of funds, or pool illegitimate funds with legal funds.
169. Betting accounts present similar risks to banking accounts and may have the same red flags for ML/TF activity.
170. In regard to cash betting, this is a core part of the betting business both historically and operationally. NZRB reports that the channels that are dominated by cash (branches, agencies, pubs, clubs and on-course) are also dominated by customers betting on racing (as opposed to sport). Cash allows for a faster transaction than electronic funds transfer at point of sale (EFTPOS) and is still preferred by a large portion of customers. Cash plays a more significant role in some channels compared to others, with on-course betting being particularly cash-based.

Methods of delivery

171. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Bets and transactions made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF. NZRB provides several methods of delivery for gambling: retail, digital, on-course, telephony channels and channels dedicated to high-value customers.

Customer types

172. NZRB's customer-base across all channels is diverse. The majority of customers are domestic, small transaction bettors and many transactions and activities will be considered "occasional" for the purposes of the Act. In some circumstances (for instance, high-value customers) NZRB will form longer-term relationships with customers. For these customers, monitoring patterns of activity will be possible, including customer history of deposits and withdraws.
173. NZRB reports that customers place a premium on the speed at which they can sell a bet. NZRB data shows that most betting on a race occurs approximately two minutes before the race commences. This presents obvious challenges for effective CDD and transaction monitoring and poses corresponding ML/TF risk.

Country risk

174. Compared to other Phase 2 sectors, NZRB presents a higher domestic ML/TF risk – particularly with financially motivated crimes associated with organised crime groups, gangs, drug-related offending and acquisitive crime.
175. Country risk comes from dealing with persons or entities in jurisdictions with poor or insufficient AML/CFT measures. NZRB should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, NZRB should consider whether the country is a conflict zone or if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. NZRB should consider not only higher-risk countries but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.
176. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme.

177. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AMLCFT supervisors. [19]

Institutions

178. NZRB will have limited exposure to the ML/TF risk presented by other institutions.

Part 11: Sector risks – high-value dealers

Overall inherent risk: Medium-high

Given the size, nature and diversity of this sector and its previous and continued unregulated nature, it is difficult to get an accurate picture of the nature and extent of ML/TF. However, based on domestic and international evidence, HVDs are highly vulnerable to ML/TF. Coupled with low overall ML/TF awareness and lower levels of supervision and reporting obligations, the HVD sector presents a medium-high inherent risk of ML/TF.

179. HVDs will be covered by the Act from 1 August 2019. Further industry-specific guidance will provide more detail on the risks and vulnerabilities of this sector.

180. One of the most common and easiest methods of ML/TF is through the purchase and sale of high-value commodities. The use of high-value commodities for ML/TF purposes is prevalent where there is an illicit cash economy. The New Zealand methamphetamine and cannabis markets are largely cash-based. This makes people who buy and sell high-value commodities vulnerable to money launderers.

181. There is also a significant transnational element to New Zealand's drug market, including methamphetamine precursors and products flowing inwards from overseas jurisdictions. One way of paying others in the transnational supply chain is through trade in high-value commodities. With the banking and border cash systems being progressively tightened around the world, small, transportable high-value commodities are commonly transported across borders and traded or sold.

[19] http://bit.ly/2hOTHPk

182. The medium-high rating is consistent with these characteristics and the sector's demonstrated involvement with ML/TF, as evidenced by FIU data. It is also consistent with international experience and expectations.
183. HVDs are only subject to limited obligations of the Act (some mandatory, some voluntary) under specific circumstances. An HVD is only covered by the Act if they carry out activities defined in the Act and accept cash above the prescribed threshold (anticipated to be $15,000) or more in cash or make a series of related cash payments that total the prescribed threshold or more. For instance, HVDs may choose to submit SARs, but they must submit prescribed transaction reports (PTRs).
184. Given the anticipated $15,000 cash threshold, structuring of payments will be a significant ML/TF typology. Even though there are elements in the Act to report on structuring, it may be difficult to detect this activity, especially if spread over time, location and via different types of HVD.
185. DIA recognise that HVDs are not all the same and the activities they carry out are diverse. For the purposes of this SRA, some generalisations have been made.

Nature, size and complexity

186. Given the diversity of this sector and its unregulated nature, it is difficult to get an accurate picture of its size, nature or complexity. What is clear is this sector is highly vulnerable to criminal abuse, and AML/CFT measures and supervision are still underdeveloped. Note: Private sales are not covered by the Act.
187. High-value goods cover a wide range of items. Some HVDs, like bullion and gem dealers, are explicitly covered by FATF requirements. Other HVDs are included in the Act to ensure that displacement of ML/TF activity does not occur from one HVD to another. The scope of the broader HVD sector is large, covering auctioneers, brokers, bullion dealers, jewellers, precious metal and stone dealers, motor vehicle and boat dealers, and antiquities and fine art dealers. Some vehicle dealers provide finance to customers through on-site services, but these separate companies are already subject to AML/CFT obligations.

Products and services

188. High-value products share some commonalities. High-value cash transactions for such items can avoid interaction with the financial sector, and money launderers can target businesses that are unlikely to reject them. Precious metals, stones and jewellery can be easily hidden, transported domestically or internationally, and dispersed to third parties. They can also be easily converted back into cash, can hold or increase in value, and can be transferred from person to person.
189. High-value commodities are highly versatile for criminals. Once purchased they can be recapitalised through uncontrolled trading markets, they are easy to transport (both domestically and internationally), are easy to disguise and conceal, and maintain their value for long periods. High-value commodities are a practical option for ML/TF because there is no paper trail, transactions are quick and easy to undertake, they are facilitated with cash that is legal tender, and items can be easily hidden for safe keeping and transportation. ML/TF through the sale and purchase of high-value commodities enables the criminal to have direct control over the entire process.
190. There are also a wide range of unusual high-value commodities (such as art and antiquities, rare wildlife products, and casino chips) that can be associated with ML/TF.
191. Purchasing high-value commodities from an HVD improves the appearance of legitimacy, protects the offender from the added risk of trading with unknown members of the public, and provides ready access to a wide range of high-value commodities, with the possibility of making many transactions relatively quickly.
192. FIU research indicates that car, motorcycle and boat dealers are the most vulnerable HVDs in New Zealand to criminal misuse. These commodities are used as status symbols, are traded "in kind", hold value, and can be on-sold. Vehicles can be used for further criminal offending, including drugs transportation and financial dealing. Expensive boats and yachts can be moved across borders and around the country to avoid detection.
193. Given the cultural significance of gold and silver in many parts of the world, there is always a market for precious metals. This market can also intermingle with the legitimate financial market. The FATF Recommendations in relation to HVDs currently only cover gems and bullion. New Zealand has taken the step to cover a broader range of commodities to stop

displacement of ML/TF activity to other, non-regulated HVDs.

194. High-value commodities can also be transported overseas, helping to meet demand of a particular market in exchange for payment in a form capable of establishing a facade of legitimacy. Bullion and gems are known commodities in cross-border TF; however, antiquities, art and vehicles have all been reported as being used in international TF. For instance, the FIU reports that the shipment of cars to the Middle East and other forms of trade have been used by some terrorist organisations.

Methods of delivery

195. High-value commodity purchases represent an extremely low-risk for criminals, mainly associated with the point of retail or trade sale. Once purchased, commodities can be easily used to transfer wealth. Face-to-face contact with a customer offers some form of tangible business relationship and an opportunity to interact with the customer. Transactions made online, over the phone or via an intermediary reduce this exposure to the customer, decrease effective identification, and increase vulnerability to ML/TF.

196. New Zealand has a thriving trade in online markets that act as an interface between private sellers and buyers. It is not possible to regulate the private sales market.

197. In relation to "luxury firms", they may maintain control over their distribution channels to ensure exclusivity is not diluted and may have more developed customer business relationships to facilitate future sales and provide customer support.

Customer types

198. The target markets for customers are as diverse as the high-value goods that HVDs sell (see Appendix 8: Key ML/TF vulnerabilities and high-risk factors). Criminals not only use illegitimate or black-market dealers but also take advantage of unwitting legitimate dealers. Compared to other Phase 2 sectors, HVDs as ML/TF vehicles are likely more applicable in the domestic setting – particularly with financially motivated crimes seen in gangs and drug-related crimes.

199. Most HVDs do not have regular customers. Offenders are likely to conduct occasional transactions across a number of different HVDs, who each hold one part of the overall picture of suspicious activity. This means that HVDs can help investigations into ML/TF activities by collecting and reporting relevant information, including financial information and customer details. Cash and suspicious activity reporting provides important evidence for both investigations and prosecutions.

200. The more luxury-focused businesses of the HVD sector, where part of their business model is knowing their customer and cultivating relationships with them, are in an excellent position to carry out effective CDD on their customers.

Country risk

201. Compared to other Phase 2 sectors, HVDs present higher domestic ML/TF risk – particularly with financially motivated crimes associated with organised crime groups, gangs, drug-related offending and acquisitive crime. This is especially the case with high-value commodities such as vehicles and real estate. However, the movement of certain goods and the ease with which they can be transported makes for an easy method of ML/TF internationally.

202. Country risk comes from dealing with persons or entities in jurisdictions with poor or insufficient AML/CFT measures. HVDs should also consider the levels of bribery and corruption, tax evasion, capital flight and organised crime activity in a jurisdiction. In addition, HVDs should consider whether the country is a conflict zone or if the country is known for the presence of, or support of, terrorism and/or organised people trafficking. HVDs should consider not only higher-risk countries but also their neighbouring countries, as ML/TF often involves the movement of funds across borders.

203. Reporting entities can find information on higher-risk countries from a number of sources, including the FATF, Transparency International, the United Nations Office on Drugs and Crime (UNODC) and open source media. Reporting entities will need to gain their own level of comfort when assessing jurisdictional risk. Compliance officers will be expected to develop and maintain awareness around this topic and incorporate it into their AML/CFT programme.
204. Reporting entities should refer to the *Countries Assessment Guideline* produced by the AML/CFT supervisors.[20]

Institutions

205. The illicit high-value commodity market does not exist in isolation from other methods of ML/TF. It can be layered via misuse of professionals' services, real estate agents, casinos and financial institutions. Some HVDs may have a business relationship with finance companies to help customers pay for high-value commodities.

Part 12: Terrorism financing issues

206. The terrorist threat environment in New Zealand is assessed by the NRA 2017 as "benign" with a "low domestic terrorist threat". Despite this assessment, it is prudent for all DIA reporting entities to consider the vulnerabilities and risk factors associated with TF and the potential red flags that may indicate TF activity. Reporting entities should consider not only high-risk countries but also their neighbouring countries, as TF often involves the movement of funds across borders. Further information is included in Appendix 10 and in the NRA 2017.
207. TF 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. Reporting entities reporting TF activity must ensure it is accurate, timely and treated with urgency and sensitivity.**
208. The FIU has identified two main TF threats in the NRA 2017:
    - Radicalised individuals – These people may be inspired to contribute to overseas terror groups by travelling to conflict zones, which requires self or third-party funding. They may also contribute to terrorism by raising funds
    - Transnational laundering by terrorism financing networks – This may involve the movement of larger sums of money for terrorism, in particular for or by state-sponsored groups. This may occur through New Zealand vulnerabilities such as legal persons and alternative banking platforms

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

Nature of TF

209. 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 used to monitor ML can also be used for TF, as the movement of those funds often relies on similar methods to ML. Internationally the TF process is considered to typically involve three stages:
    - **Raising funds** (through donations, legitimate wages, selling items, criminal activity)
    - **Transferring funds** (to a terrorist network, to a neighbouring country for later pick up, to an organisational hub or cell)
    - **Using funds** (to purchase weapons or bomb-making equipment, for logistics, for compensation to families, for covering living expenses)
210. The risks associated with TF are highly dynamic. As such, reporting entities need to ensure that their CFT measures are current, regularly reviewed and flexible. It is important that reporting entities maintain CFT awareness and effective transaction monitoring systems that incorporate dynamic TF risks, as well as the more static risks associated with ML.
211. The value of funds moved through New Zealand connected to TF is likely to be much, much lower than other forms of illicit capital flows. However, if funds connected to TF were to be associated with New Zealand reporting entities, it would likely have a disproportionate effect on New Zealand's reputation. Outside of the obvious harm caused by TF, any New Zealand reporting entity associated with this activity could see their reputation severely damaged. If their CFT measures were found to be inadequate or ineffective, they could also face civil and even criminal charges.

New Zealand as a conduit for TF

212. One of the potential consequences of transnational ML is that channels may be established that may also be exploited by terrorism financiers. Overseas groups may seek to exploit New Zealand as a source or conduit for funds to capitalise on New Zealand's reputation as being low risk for TF. For instance, funds originating in or passing through New Zealand may be less likely to attract suspicion internationally.
213. TF through the Phase 2 sectors 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 New Zealand. It could also involve remittance agents sending funds overseas. More complex methods could see New Zealand businesses, professional services, non-profit organisations and charity accounts being used as fronts for sending funds offshore.

TF indicators and warnings

214. ML and TF share many indicators and warnings, or red flags. The following indicators and warnings may help reporting entities in the difficult task of drawing a link between unusual or suspicious activity and TF:
    - International funds transfers to and from high-risk jurisdictions, potentially at multiple branches of the same reporting entity
    - Multiple customers and/or occasional transactions by non-customers conducting international funds transfers to the same beneficiary located in a high-risk jurisdiction
    - A customer transferring funds to multiple beneficiaries in high-risk jurisdictions
    - A customer using incorrect spelling or providing variations on their name when conducting funds transfers to high-risk jurisdictions
    - Large cash deposits and withdrawals to and from non-profit organisation 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 the "Proliferation and dual-use items" section)
    - A sudden increase in business/accounts activity, inconsistent with customer profile
    - Multiple cash deposits into personal account described as "donations" or

"contributions to humanitarian aid" or similar terms
- Multiple customers using the same address/ telephone number to conduct business/ account activity
- Prescribed entities or entities suspected of terrorism using third-party accounts (e.g. a child's account or a family member's account) to conduct transfers, deposits or withdrawals
- Use of false identification to establish New Zealand companies
- Pre-loading credit cards, requesting multiple cards linked to common funds or purchasing cash passports/stored-value cards prior to travel
- Customers taking out loans 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
- Customers converting small-denomination bank notes into high-denomination notes (especially US dollars, euros or sterling)

Proliferation and dual-use items

215. Since the last DIA SRA, the FATF has revised its 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 reporting entities in New Zealand are involved in financing proliferation activities. However, included in "proliferation" are dual-use items or technologies, and New Zealand is not immune from abuse in this sector. Although the likelihood of occurrence is very low, the potential consequences, as with TF, could be catastrophic.

216. 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 New Zealand. Such items cannot be legally exported from New Zealand without an export licence and/or permission from the Secretary of Foreign Affairs and Trade. A list of strategic goods is available on the Ministry of Foreign Affairs and Trade website[21], and a booklet on the topic is available on the Security Intelligence Service website.[22] Appendix 10 contains a FATF-provided table of general dual-use items and proliferation risk factors that reporting entities may encounter.

[21] http://bit.ly/2A1piYg

[22] http://bit.ly/2Bhy8PL

Support Document for Phase 2 SRA: Appendices

December 2017

Appendix 1: SRA methodology

Concept of risk

217. The Phase 2 SRA works on two distinct levels: it provides an assessment of ML/TF risk, and it identifies key ML/TF vulnerabilities and high-risk factors and how they impact each sector. Where there are specific weaknesses or typologies of note, these are also highlighted.
218. This assessment follows the NRA 2017 and FATF guidance, which suggest that ML/TF risk should be assessed as a function of threat, vulnerability and consequence. This assessment uses a range of FATF guidance on risk assessment methodology and draws on specific international advice for assessing risk in the Phase 2 sectors. Threat combined with vulnerability was expressed as likelihood and aligns with existing DIA risk assessment models where risk is a function of likelihood and consequence.
219. The Phase 2 SRA is one of the decision-making tools DIA uses to plan and focus its AML/CFT supervisory activities on the reporting entities that may present the greatest risk, with the aim of carrying out DIA's statutory functions in an effective and efficient way. This reflects DIA's commitment to a risk-based approach to AML/CFT.

Methodology – assessment of risk

220. DIA assessed ML/TF risk for each sector using a simple model using the risk factors listed in section 58(2)(a)–(f) of the Act and in the *Risk Assessment Guideline*[23] to help reporting entities in using the Phase 2 SRA in their own risk assessment. The risk factors are:
    - Nature, size and complexity of business
    - Products/services
    - Methods of delivery of products/services
    - Customer types
    - Country risk
    - Institutions dealt with (if relevant)
221. DIA posed a number of ML/TF questions for each of these variables. The responses to these questions helped guide the assessment of **inherent** risk for each variable in combination with structured professional knowledge and domestic and international guidance.
222. The primary focus of the Enterprise Risk Management Tool in the Phase 2 SRA was likelihood. However, an explicit part of the risk rating process was to consider the consequences for each sector of ML/TF activity based on the potential for harm.
223. Determining consequence can be challenging and it was considered in the following context: nature and size of the sector, potential financial and reputational consequences, and wider criminal and social harms. These judgements were necessarily qualitative in nature due to the wide variance in ML/TF consequence across individual reporting entities.
224. Because DIA did not consider the adequacy or effectiveness of ML/TF controls in the risk rating process, DIA made no judgements as to whether the risks present in a sector are adequately managed or mitigated. Reporting entities may have systems and controls that address some or all the risks discussed in the risk assessment, but the Phase 2 SRA does not identify or comment on activities undertaken by individual entities within the sectors.
225. Taking all these variables into consideration, an overall assessment of **inherent** ML/TF risk was then assigned to each sector using ratings of low, medium, medium-high or high in line with DIA's Enterprise Risk Management Tool. DIA determined risk by cross-referencing the assessed likelihood of an event with its assessed consequence in the following matrix.

[23] http://bit.ly/2iL7Spp

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

226. For the purposes of the phase 2 SRA, weightings were assigned to the risk variables and each sector's risk rating was scored and aggregated to arrive at a final overall risk rating.

Methodology – identification of vulnerabilities and high-risk factors

227. As part of the Phase 2 SRA, DIA identified five key ML/TF vulnerabilities and five high-risk factors. The vulnerabilities/risk factors were selected during a series of DIA workshops using subject matter expertise, operational experience and both domestic and international guidance. They were chosen for their impact and commonality across the Phase 2 sectors and were deliberately kept few in number to help reporting entities understand the ML/TF environment in New Zealand. DIA assessed the vulnerabilities and high-risk factors (see Appendix 8 for details) using a Delphi process to ensure inter-rater reliability. DIA then identified key vulnerabilities and high-risk factors for each sector during consultation.

228. The Delphi technique is a quantitative exercise aimed at reaching a consensus. For the Phase 2 SRA DIA gathered opinions from DIA experts during workshops/consultation 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 Phase 2 SRA.

229. In future iterations of the Phase 2 SRA, this model will be combined with supervisory experience, structured professional judgement, annual reports and data from the DIA Entity Risk Model.

230. The vulnerabilities and high-risk factors are based on the knowledge and experience of DIA staff in conjunction with information from the NRA 2017, SRAs from the AML/CFT supervisors in New Zealand, and international guidance from the FATF, APG and comparable jurisdictions (e.g. AUSTRAC, Financial Crimes Enforcement Network, Financial Transactions and Reports Analysis Centre of Canada, Financial Conduct Authority) in addition to other open source media.

Entity Risk Model

231. The purpose of the Entity Risk Model is to assess AML/CFT risk across DIA's regulated sector. The Entity Risk Model is refreshed annually and the results will help inform future Phase 2 SRAs. The Act requires reporting entities to submit AML/CFT annual reports, and the Entity Risk Model uses this quantitative data, combined with insight and information from other partners, to assign **inherent** risk. The Entity Risk Model is one of the decision-making tools DIA uses to focus AML/CFT supervisory programmes on reporting entities that present the greatest risk.

Consultation with industry bodies

232. DIA consulted with reporting entities and representative bodies from the major Phase 2 sectors (lawyers, conveyancers, accountants and real estate agents) to further inform the Phase 2 SRA. DIA also sought feedback from an advisory group made up of members of these sectors during a series of workshops prior to publishing the Phase 2 SRA. DIA will be consulting with HVDs and NZRB for future iterations of this SRA.

Consultation with other AML/CFT sector supervisors

233. DIA, as one of the three AML/CFT supervisors, is in regular contact with RBNZ and the FMA. During the production of the Phase 2 SRA, DIA sought formal feedback and input from both these supervisors. This consultation was augmented by monthly National Coordination Committee meetings and fortnightly Supervisors Forum meetings.

Consultation with FIU

234. DIA consulted the FIU throughout the production of the Phase 2 SRA. Given the key nature of the NRA, communication, feedback, input and the exchange of information between DIA and FIU was comprehensive and robust. This SRA uses FIU research throughout its assessment of ML/TF risk.

Risk appetite and risk-based approach

235. Regardless of the assessed ML/TF risk and vulnerability ratings in the Phase 2 SRA, when reporting entities assess their own ML/TF risk, they should consider the level of risk they are willing to accept. A risk-based approach recognises that there can never be a zero-risk situation, and reporting entities must determine the level of ML/TF exposure they can tolerate. This is not a legislative requirement but may help reporting entities in their risk management.

Information sources

236. The Phase 2 SRA has drawn together information from a number of sources. A list of source documents is included in Appendix 9. DIA also considered other data sources available to the AML/CFT supervisors, including summary STR data and other information provided by the FIU (including the NRA 2017, Quarterly Typology Reports and associated research), as well as industry expertise, knowledge and experience from internal and external resources relevant to the sectors.

Qualitative and quantitative data

237. The Phase 2 SRA 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. Quantitative data included data from STRs (where relevant), the DIA Entity Risk Model (where relevant), Asset Recovery Unit data and criminal justice statistics. Data collection methods included expert assessments through structured questions, interviews, workshops and other assessment tools. This is in line with FATF, International Monetary Fund, World Bank, and Organization for Security and Co-operation in Europe (OSCE) methodologies.

Baseline monitoring – annual report data

238. Baseline monitoring via annual report data (still to be collected for Phase 2 sectors) will be able to demonstrate that DIA will be keeping track of issues across the Phase 2 sectors in an ongoing manner. DIA will use this data to inform targeted supervisory action in response to any identified risks. Baseline monitoring will also help measure the effectiveness of AML/CFT supervision by providing a clearer understanding of the levels of compliance within each reporting entity. This will help with decision-making on the appropriate frequency and intensity of AML/CFT supervision.

Limitations

239. The Phase 2 SRA process has the following limitations:
    - Information on ML/TF in the Phase 2 sectors is limited
    - It will take some time before annual report data gives us a clearer picture of the Phase 2 environment
    - A high degree of reliance on international typologies and guidance to identify risks
    - Phase 2 reporting entities have various degrees of understanding of AML/CFT legislation and procedures
    - Phase 2 reporting entities have various degrees of understanding of the ML/TF risks in their business, therefore the perception of ML/TF may not be fully developed in a reporting entity's AML/CFT risk assessment or programme
    - There is insufficient quality detailed data and information to inform some risk areas

Appendix 2: ML/TF inherent risk – lawyers

Variable	Assessed risk	Rationale
Nature, size and complexity of business	High	The legal sector environment lends itself to a high-risk of ML/TF because client relationships can be complex and the identity of beneficial owners may not be clear. The ease of access to the legal sector, its wide geographic spread, the gatekeeper role it plays in accessing the financial sector and the veneer of respectability it affords all compound ML/TF risk.
Products/services	High	Lawyers offer numerous products/services that can be used to facilitate ML/TF, including setting up and managing trusts, companies and other legal arrangements. Many of these products and services are internationally recognised as presenting a high-risk of ML/TF. Legal professional privilege adds another layer of complexity and potential concealment
Methods of delivery of products/services	Medium	Lawyers offer their products and services both via face-to-face and non-face-to-face means. Advances in the use of the internet also pose ML/TF risk.
Customer types	Medium-high	Lawyers' clients are generally lower-risk New Zealand-based individuals. However, lawyers need to consider ML/TF risk in relation to trusts, shell companies, PEPs and occasional transactions/activities, as well as exposure to criminals, organised crime groups and high-risk occupations.
Country risk	Medium	The legal sector is predominantly New Zealand-based and normally avoids higher-risk jurisdictions. However, increasing interaction with overseas clients and companies and a dynamic international ML/TF risk environment presents ML/TF vulnerabilities.
Institutions dealt with (if relevant)	Low	Lawyers have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Medium-high	Both domestic and international evidence and guidance indicate the ML/TF risks presented by the legal sector. The easy access and wide geographic spread of legal services, coupled with lawyers' gatekeeper role and use in every phase of ML/TF and in many different ML/TF typologies, means this sector presents a medium-high inherent risk of ML/TF.

Appendix 3: ML/TF inherent risk – conveyancers

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Low	There are a limited number of conveyancing firms in New Zealand offering a very specific range of services. While real estate transactions can be complex and of high-value, the specialised nature of this field reduces the exposure to ML/TF vulnerability.
Products/services	Medium	Conveyancers only offer a limited range of products/services with limited exposure to most high-risk products and services (e.g. cash-intensive activity). However, the role they play in real estate transactions is vulnerable to criminal misuse.
Methods of delivery of products/services	Medium	Conveyancers offer their products and services via both face-to-face and non-face-to-face means.
Customer types	Medium	Conveyancers' customers are generally low-risk New Zealand-based companies and associated individuals. However, conveyancers need to consider ML/TF risk in relation to trusts, shell companies and legal entities associated with PEPs, as well as businesses associated with organised crime groups and high-risk industries. Determining beneficial ownership and executive control of customers also needs attention, as do persons acting on their behalf.
Country risk	Low	Conveyancers primarily operate in New Zealand. However, global access of legal services and a dynamic international ML/TF risk environment associated with real estate does present some ML/TF vulnerability.
Institutions dealt with (if relevant)	Low	Conveyancers have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Low	The values and potential velocity of conveyancing activity and exposure to the high-risk real estate sector present ML/TF vulnerabilities. However, conveyancers' limited exposure to cash and other high-risk products/services, and their interaction with generally lower-risk customers and institutions, mean this sector presents a low inherent risk of ML/TF.

Appendix 4: ML/TF inherent risk – accountants

Variable	Assessed risk	Rationale
Nature, size and complexity of business	High	The accounting sector environment lends itself to a high-risk of ML/TF because client relationships can be complex and the identity of the beneficial owner may not clear. The ease of access to the accounting sector, its wide geographic spread, the gatekeeper role it plays, and the veneer of respectability it affords all compound this risk.
Products/services	High	The professional services provided by the accountancy sector are attractive to money launderers because they are widely available, and they can give the impression of respectability, legitimacy, or normality. In addition, high-value transactions are normal for accountants, who can create additional steps in the ML/TF chain that can hinder detection and investigation. They also provide access to services and techniques that money launderers would not normally have access to, such as setting up trusts and companies.
Methods of delivery of products/services	Medium	Accountants offer their products and services via both face-to-face and non-face-to-face means. Advances in the use of the internet also pose ML/TF risk.
Customer types	Medium	Accountants' customers are generally lower-risk New Zealand-based individuals. However, accountants need to consider ML/TF risk in relation to trusts, shell companies, PEPs and occasional transactions by non-customers, as well as exposure to criminals, organised crime groups and high-risk occupations.
Country risk	Medium	The accounting sector is predominantly New Zealand-based and normally avoids higher-risk jurisdictions. However, increasing interaction with overseas customers and companies and a dynamic international ML/TF risk environment does present ML/TF vulnerability.
Institutions dealt with (if relevant)	Low	Accountants have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Medium-high	The easy access and wide geographic spread of accounting services, coupled with accountants' gatekeeper role and use in every phase of ML/TF and in many different ML/TF typologies, means this sector presents a medium-high inherent risk of ML/TF.

Appendix 5: ML/TF inherent risk – real estate agents

Variable	Assessed risk	Rationale
Nature, size and complexity of business	High	The real estate sector is widely regarded as being highly vulnerable to ML/TF abuse, both domestically and internationally. Access to the real estate sector is easy and widely spread. The involvement of a real estate agent provides money launderers with the impression of respectability and normality, especially in large transactions, and is a further step in the ML/TF chain that frustrates detection and investigation.
Products/services	Medium-high	Real estate agents provide a more limited range of products and services than some other gatekeepers. However, real estate is a very high-value commodity that is attractive for both ML and the investment of criminal proceeds. Real estate agent involvement can obscure the identity of the person(s) behind the criminal dealings and effectively cleans illicit funds when the property investments are later realised.
Methods of delivery of products/services	Medium	Real estate agents offer their products and services via both face-to-face and non-face-to-face channels. Concealment of the identity of criminals enjoying beneficial ownership of real estate is common.
Customer types	Medium	Real estate agents' customers are generally low-risk New Zealand-based individuals. However, real estate agents need to consider ML/TF risk in relation to overseas buyers, trusts, shell companies and PEPs, as well as exposure to organised crime groups and high-risk occupations and industries.
Country risk	Medium-high	This sector has an overwhelmingly domestic customer base but does have significant and high-value business with overseas customers, some from high-risk jurisdictions.
Institutions dealt with (if relevant)	Low	Real estate agents have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Medium-high	The use of real estate in ML/TF is well-known and demonstrable. FIU research indicates real estate is the ML asset of choice. In addition, this sector has low levels of AML/CFT awareness and sophistication. As such, this sector presents a medium-high inherent ML/TF risk.

Appendix 6: ML/TF inherent risk – NZRB

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium-high	The gambling sector is widely regarded as being vulnerable to ML/TF abuse, both domestically and internationally. Access to the NZRB sector is easy and widely spread. Winnings from gambling enabled by NZRB provides money launderers with the impression of normality and can involve large amounts of funds, and is a further step in the ML/TF chain that frustrates detection and investigation.
Products/services	Medium	The gambling services provided by NZRB, though small in number, are attractive to money launderers because they are widely available, easily accessed, and can give the impression of legitimacy and normality. In addition, they can be used to facilitate high-value, high-volume and high-velocity transactions.
Methods of delivery of products/services	High	NZRB offer their products and services via both face-to-face and non-face-to-face channels. Access to gambling at trackside presents a number of CDD challenges, and determining beneficial ownership is very difficult. Concealment of the identity of criminals using gambling to launder funds is relatively straightforward in the absence of effective mitigation measures.
Customer types	Medium	NZRB's customers are generally lower risk New Zealand-based individuals. However, NZRB needs to consider its exposure to criminals, organised crime groups and high-risk occupations.
Country risk	Low	This sector has an overwhelmingly domestic customer-base but does have small amounts of business with overseas customers, some of whom may be from high-risk jurisdictions.
Institutions dealt with (if relevant)	Low	NZRB has limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Medium-high	Given the previous and continued unregulated nature of the NZRB, it is difficult to get an accurate picture of the nature and extent of ML/TF. The overall medium-high risk rating for the NZRB sector reflects the size and products and services covered by the Act. The gambling sector – widely spread and easy to access – is vulnerable to a number of high-risk ML/TF activities and industry-specific risk factors.

Appendix 7: ML/TF inherent risk – HVDs

Variable	Assessed risk	Rationale
Nature, size and complexity of business	Medium-high	HVDs are widely spread and easy to access. The nature of the industry lends itself to all stages of ML/TF. Many HVDs are small enterprises and may have less awareness of ML/TF and limited capability to meet AML/CFT obligations. In addition, anonymity and concealment of beneficial ownership has traditionally been associated with this sector. It will take several years to establish a culture of AML/CFT compliance.
Products/services	High	The products offered by HVDs are attractive for many reasons – they can be of high-value, easily transportable, easily converted into funds, and can be used to pay for goods/services in kind. In addition, HVD products can be used for the purposes of bribery and corruption.
Methods of delivery of products/services	Medium-high	HVDs offer their products and services via both face-to-face and non-face-to-face channels (including telephone or online auction). Concealment of the identity of criminals enjoying beneficial ownership of high-value commodities is common. Ability to source high-value commodities online or via intermediaries presents ML/TF risk.
Customer types	Medium	HVDs' customers are generally low-risk New Zealand-based individuals. However, HVDs need to consider ML/TF risk in relation to overseas buyers, high net worth individuals, trusts, shell companies and PEPs, as well as exposure to organised crime groups and high-risk occupations and industries.
Country risk	Medium	Globalisation has exposed the New Zealand HVD industry to international risks and vulnerability. While most business will be conducted in New Zealand with New Zealand-based customers, HVDs will need to consider their exposure to high-risk jurisdictions.
Institutions dealt with (if relevant)	Low	HVDs have limited exposure to dealing with institutions identified as presenting ML/TF risk.
Overall inherent risk	Medium-high	Given the size, nature and diversity of this sector and its previous and continued unregulated nature, it is difficult to get an accurate picture of the nature and extent of ML/TF. However, based on domestic and international evidence, HVDs are highly vulnerable to ML/TF. This, coupled with low overall ML/TF awareness and lower levels of supervision and reporting obligations, means this sector presents a medium-high inherent risk of ML/TF.

Appendix 8: Key ML/TF vulnerabilities and high-risk factors

Key vulnerabilities

Cash and liquidity

240. As noted in the NRA 2017, New Zealand is a relatively low-cash society. Citing Payment New Zealand analysis, the NRA 2017 reports an increased circulation of high denomination bank notes, concurrent with declining use of cash in retail, but increased use in the hidden economy. In addition, the FATF continues to highlight ML/TF through the physical transportation of cash as a key typology.
241. Crime such as drug dealing and converting stolen property generally generates proceeds in cash. Cash remains popular for ML/TF activity because 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 – between parties or geographical locations
242. 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.
243. Broadly, placement of cash criminal proceeds must occur either through deposits or co-mingling with legitimate cash, or transported offshore to where cash can be more easily placed through either deposits or co-mingling. The FIU highlighted this vulnerability in *Quarterly Typology Report Q4 2013–2014: Co-Mingling with Business Revenue*.[24]
244. The NRA 2017 reports multiple instances where individuals not involved in the predicate offending have been used to physically move cash (to act as cash couriers or money mules), particularly to transport cash internationally.
245. The use of cash-rich businesses is a well-known typology using all three stages of ML. They offer legitimacy and concealment of funds, easy methods of mixing criminal funds with legitimate income, and access to the financial sector. Cash-rich businesses include nail bars, takeaways and restaurants, bars, remitters, HVDs and short-term loan businesses.
246. The NRA 2017 reports that offending using cash is highly visible and transactions involving cash are highly represented in historical STR reporting. Many reporting entities report STRs exclusively, or near exclusively, in relation to cash transactions.
247. Criminals use cash to purchase assets, such as vehicles or real estate, and to conduct transactions through remittance channels (particularly international transactions).
248. For those HVDs with regular clients, they have a unique view of any transactions where cash is used to place illicit proceeds into their business, and they are well placed to identify such activity. These could include identifying unusual social or financial behaviours – for example, changes in the buying and selling patterns of clients, the purchase of high-value commodities in multiple transactions over a short period of time, and situations in which a customer has an occupation that is inconsistent with their financial profile or there is an unusual pattern and nature of transactions/activities.
249. Other ML/TF vulnerabilities presented by cash include:
    - Dispersing placement through multiple cash deposits (often called smurfing)
    - Refinement into higher-denomination notes or specific currencies
    - Being used in casinos and gambling/betting
    - Using anonymous deposit drop boxes or deposit-capable ATMs
250. Customers with foreign currency accounts may conceal illegitimate funds generated overseas by depositing cash into those accounts, which allows them to easily convert, transfer and access the funds.

[24] http://bit.ly/2hZZogQ

New payment technologies

251. New payment technologies (some more mainstream and established than others) can increase the opportunities for ML/TF, in particular where they allow criminals to exploit developments that break down the barriers posed by international borders, or facilitate new anonymous means of payments between individuals.
252. 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. 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.
253. Technology that can be accessed remotely anywhere in the world, that can move funds quickly, and that allows the quick reintegration of the proceeds of crime back into the financial system will be attractive to launderers and terrorism financiers.
254. 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.
255. Money launderers and terrorism financiers may be attracted by the speed and convenience of new payment technologies. Criminals can exploit the borderless nature of the internet whereby there are difficulties regulating financial services that operate online.
256. Some new payment technology vulnerabilities are:
    - Open-loop stored-value instruments that may be used overseas
    - Online payment facilities 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
257. Digital, virtual or crypto-currencies (e.g. Bitcoin) have not been observed in significant numbers in ML/TF cases, and where they have been used the value of funds has been relatively low. However, the products and methods of delivery associated with this typology present a dynamic ML/TF risk.
258. The FATF has produced guidance on this vulnerability – *Money Laundering Using New Payment Methods (2010)*[25] – though, by its nature, this topic is a dynamic risk environment and guidance will develop accordingly.

Real estate

259. Analysis of New Zealand Police Asset Recovery Unit cases shows that hiding the ownership of property is a common ML method, often by placing the property in the name of a trust set up by a lawyer. Another common method identified by the FIU was transferring the criminal proceeds to a lawyer or real estate agent by electronic transfer.
260. The FIU highlighted this vulnerability in *Quarterly Typology Report Q4 2014–2015: Real Estate*.[26]
261. In 2007 a FATF typology study on real estate identified the following areas of opportunity for money launderers:
    - Use of complex loans or credit finance
    - Use of gatekeeper professionals to access financial services, facilitate transactions through client trust accounts, or to act as intermediaries in transactions
    - Use of corporate vehicles, such as offshore 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
262. Use of nominees during a real estate transaction can disguise the true beneficial owner or effective controller of a customer and adds another level of complexity to transactions and activities.

[25] http://bit.ly/1ewq4rq

[26] http://bit.ly/2hMEjml

263. The NRA 2017 reports on the attractiveness of the real estate sector to 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
264. The use of real estate has also been highlighted as the preferred method of ML by numerous comparable jurisdictions and by Transparency International.
265. The buoyant housing market in New Zealand has likely increased the opportunities for transnational money launderers to exploit the real estate sector. This has been observed in other comparable jurisdictions as well, such as the UK, USA, Canada and Australia.
266. Some property transaction and financing red flags identified by the FATF include:
    - Speed of the transaction (transactions that are unduly expedited without a reasonable explanation may be higher risk)
    - Successive transactions, especially of the same property in a short period of time with unexplained changes in value
    - Introduction of unknown parties at a late stage of transactions
    - Third-party vehicles (i.e. trusts) used to obscure true ownership of the buyer
    - Under- or over-valued transactions
    - Property value that is not in the profile of the customer
    - Location of client's and/or customer's source of funds
    - Funds obtained from unknown individuals or unusual organisations
    - Funds from high-risk countries
    - Use of complex loans, or other obscure means of finance, versus loans from regulated financial institutions
    - Unexplained changes in financing arrangements
    - Type of property (residential or commercial, vacant land, investment, high-turnover properties, multi-unit properties for lettings/leases)
    - Purchase with large amounts of cash and cash deposits or money orders from unusual sources or high-risk countries

Anonymity and complexity

267. Anonymity and complexity can be considered as part of the broader obfuscation of beneficial ownership and/or executive control. Concealment and disguise are highly desirable for ML/TF purposes. Any products, services, business relationships or methods of delivery that facilitate anonymity or the disguising of identity or ownership represents a high ML/TF risk.
268. The broad range of professional services offered by gatekeepers enables money launderers to manage all their financial and business affairs in one place. Professionals can act on behalf of clients in respect of both financial and legal affairs, and changes to arrangements can be made quickly and frequently. Professionals can be used unwittingly to facilitate a range of illicit transfers, particularly when acting in a proxy role.
269. Typically, a money launderer arranges for a professional to set up a company or trust and then also act, or arrange for a third-party to act, in a proxy role, including acting as a trustee, nominee resident director, or nominee shareholder. With the fiduciary role appearing legitimate, the money launderer can conduct a range of criminal activity or asset transfers at arm's length from both regulatory and law enforcement agencies. Tracking and tracing the beneficial owner is time consuming and can be challenging because information on beneficial ownership may not be held by professionals.
270. Determining and verifying the identity of the individual customer (not legal person) is one of the most important AML/CFT measures that reporting entities must undertake. Shortfalls in this area represent the highest ML/TF risk and will receive significant supervisory attention.
271. The following items (not exhaustive in nature) all provide varying degrees of concealment and disguise. Reporting entities should carefully consider their use in the ordinary course of business and what AML/CFT measures should be deployed:
    - **Non-face-to-face methods of delivery –** A lack of direct contact between reporting entities and customers makes 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 –** New Zealand 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 the "Trusts, shell companies and other legal arrangements" section below).

- **Trusts –** New Zealand has a large number of trusts (including family trusts), which are a well-known method of providing anonymity (see the "Trusts, shell companies and other legal arrangements" section below).
- **Safety deposit boxes –** Though it is not a common typology in New Zealand, the use of deposit boxes has been linked in international reporting to organised crime and the hiding of the proceeds of crime.
- **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.
- **Drop boxes/Smart ATMs –** These services provide a high degree of anonymity and an easy method to place the proceeds of crime into the banking system. The use of smart ATMs that accept deposits anonymously present ML/TF risk.

272. The use of intermediaries, such as brokers, presents 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.
273. Use of intermediaries may also circumvent some of the CDD 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.
274. Where multiple gatekeepers act as intermediaries in a chain for the same customer(s), activity or transaction, this is a significant ML/TF vulnerability.
275. The FIU highlighted the risks presented by gatekeepers in the following reports:
    - *Quarterly Typology Report Q3 2013–2014: Money Laundering and Terrorist Financing through Professionals' Client Accounts* [27]
    - *Quarterly Typology Q2 2013–14: Money Laundering through Use of 3rd Party Intermediaries & Terrorism Financing (Intermediaries)*[28]

Lack of ML/TF awareness

276. While many reporting entities consider themselves at a low risk of ML/TF activity, their lack of awareness of the topic may make them more vulnerable to abuse by money launderers and terrorism financiers. The role of the compliance officer is key in preventing this, and DIA encourages them to explore and consider the ML/TF risk pertinent to their organisation in the ordinary course of business.
277. To increase awareness, there are a number of agencies and organisations that provide open source guidance and information. Those listed below are a good place to start:
    - National Risk Assessment and Sector Risk Assessment (New Zealand)
    - FIU Quarterly Typology Reports and SAR guidance (New Zealand)
    - Sector supervisor guidance material (New Zealand)
    - APG typology reports (international)
    - FATF guidance and best practice material (international)
    - AUSTRAC guidance material (Australia)
    - UNODC guidance documents (international)
278. Establishing and maintaining an AML/CFT culture from the top down is an important part of having an effective regime. Senior management involvement is required for parts of the Act, and regular AML/CFT reporting to senior management should be business as usual.

[27] http://bit.ly/2zijNkM

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

279. Developing, maintaining, demonstrating and evidencing situational awareness is a vital responsibility of the compliance officer and the reporting entity. Keeping aware of ML/TF-related current affairs, media, typologies and research is expected from compliance officers. For instance, attending AML/CFT conferences and seminars can provide a wide range of benefits and learning opportunities as well as invaluable networking with peers.

280. Some basic awareness-raising situations from the Act are listed below:

- **Reporting to Board and senior management –** The compliance officer is to act, where relevant, as a conduit between senior management and operational staff to ensure that AML/CFT is actioned and understood at all levels of an organisation.
- **Training –** This is a key requirement for an adequate and effective AML/CFT programme, especially for senior managers, compliance officers and customer-facing staff. Training should include the identification of industry-specific red flags and anticipation of new and emerging risks and vulnerabilities.
- **Audit –** Reporting entities must have their AML/CFT risk assessment and programme audited on a regular basis. This presents an excellent opportunity to re-visit previous assessments and to incorporate the findings of the audit into existing policies, procedures and controls.
- **Trigger events –** There is an expectation that reporting entities will develop processes and procedures that take into account dynamic risk factors, changes in legislation, advances in technology and new guidance material. These "trigger" events should prompt the reporting entity to re-visit its risk assessment and programme to ensure they are still fit-for-purpose.

Key high-risk factors

Trusts, shell companies and other legal arrangements

281. New Zealand company structures and trusts are attractive to money launderers because New Zealand's reputation as a well-regulated jurisdiction provides a veneer of legitimacy and credibility.

282. It is easy and inexpensive to register companies and set up trusts in New Zealand, and they are essentially disposable and cheaply replaceable. In addition, registration on the Financial Service Provider Register provides a veneer of legitimacy with no obligation to adhere to AML/CFT requirements.

283. 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. At the integration phase, trusts can be an effective means of dispersing assets while retaining effective control and enjoying the proceeds of criminal offending.

284. 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.

285. Using shell companies to conduct ML/TF transactions and activity helps criminals conceal the involvement of natural persons. The company conducts transactions while beneficial ownership or effective control of the company is hidden behind nominee directors and/or shareholders. The Act prohibits business relationships with shell banks.

286. Overseas money launderers may also use New Zealand's foreign trusts as a vehicle for international transactions, giving the appearance of a transaction involving New Zealand. This may make the transaction appear benign by trading on New Zealand's reputation, or may simply obscure the money trail by adding to the complexity of tracing money internationally.

287. Of note are New Zealand offshore finance companies, which present a very high-degree of ML/TF vulnerability, especially around tax evasion, and should be subject to close attention.

288. The NRA 2017 notes that New Zealand

companies, often acting as alternative banking platforms, have been implicated in numerous incidents of international offending. In addition, the NRA 2017 notes that trusts are used to hide and protect the ownership of property by offenders, and that bank accounts held for the trust receive criminal proceeds that are used to repay mortgages on the property. In the sample of Asset Recovery Unit cases analysed in the NRA 2017, 46% of cases, representing 50% of the value of restrained assets in the sample, involved trusts. Trusts were especially popular in drug cases and were most commonly abused by criminal entrepreneurs, although they were also used in several organised crime cases.

289. Given the above, shell companies and trusts, including family trusts, should be considered highly vulnerable to ML/TF activity. The FIU highlighted these vulnerabilities in the following reports:
    - *Quarterly Typology Report Q2 2014–2015: Abuse of Shell Companies*[29]
    - *Quarterly Typology Report Q1 2014–2015: Abuse of Trusts*[30]
290. Legal arrangements are versatile, as they can be sold or transferred to other people along with the assets or bank accounts established in the name of the legal entity. In addition, concealment of beneficial ownership is relatively easy using deeply nested, and complex, legal arrangements across multiple jurisdictions.
291. Trusts/companies can give the appearance of legitimate business transactions and can be used at all three stages of the ML process. Trusts/companies can hinder detection and investigation of ML/TF. Trusts/companies can also be used to create complex structures that hinder law enforcement investigations.
292. In the New Zealand context the FIU rates the vulnerability of ML through of trusts/companies as high. There have been several high-profile international cases where New Zealand shell companies have been exploited to launder money. Currently there is no central register of trusts, and trust transparency is low, making it difficult to detect the existence of a trust, the activity of a trust, or the involvement of an individual in a trust.
293. Company structures, including complex arrangements using shell companies, limited partnerships, trusts, and other vehicles to obscure beneficial ownership, are readily available in New Zealand. These may be attractive to money launderers because:
    - Company registration can be facilitated online in one day
    - The cost of establishing a New Zealand company is low
    - There is minimal CDD – only verification of identity is required of persons involved in a company structure assessed as high-risk
    - Third parties can be used as nominee shareholders and nominee directors
    - The beneficial owner of a company does not need to be declared
    - The physical location of the company does not need to be declared – the office of a lawyer, accountant, virtual office, or company formation agent can be used

International payments

294. International payments through the mainstream financial sector appear to be the primary means for money launderers and terrorism financiers to move illicit funds offshore. This movement of funds can constitute either layering or integration. In addition, it can constitute placement of cash proceeds of crime, especially in the case of remitters.
295. 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.
296. Wire transfers between jurisdictions can obscure the source of funds, particularly where information on the originator of the transaction is incomplete or absent. While international wire transfers are more likely to attract suspicion, domestic transfers are not free of risk.
297. Moving funds transnationally allows criminals to complicate investigations by creating a complex money trail and creates jurisdictional hurdles for law enforcement agencies. Criminals may structure their transactions, including occasional transactions, below reporting/identification thresholds to avoid detection.

[29] http://bit.ly/2BfP21c

[30] http://bit.ly/2A2XKC6

298. ML/TF via international payment may be easily combined with other ML/TF methods, such as the use of professional services, use of intermediaries and the use of trusts and companies.
299. Entities engaged in international payments can be involved in foreign currency exchange and may accept cash. Some entities that conduct international payments, such as brokers, may be perceived as prestigious and therefore low risk.
300. International payments may facilitate the use of "money mules" to create layers and obscure the money trail. For example, transnational payments could be made to a money mule's account, which is then followed by cash withdrawal and the remittance of that cash.
301. 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 terrorism financing schemes.
302. 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.
303. Transactions through New Zealand 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 criminals deleting or substituting information to circumvent ML/TF controls.
304. Money launderers may use New Zealand businesses to move funds to escape detection in their own jurisdiction. Third parties may be based in overseas locations with reduced or no AML/CFT requirements. Some countries also have secrecy laws or conventions that prevent the underlying beneficiary or source of funds being identified.
305. 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.
306. The FIU highlighted this vulnerability (wire transfers) in *Quarterly Typology Report Q1 2013–2014: Money Laundering Typology – Wire Transfers*.[31]

Client accounts

307. Client accounts (also called trust accounts) are provided by several Phase 2 reporting entities. Client accounts may be an attractive option for criminals to place funds, particularly if the criminal perceives that the respectability and legitimacy added by using a professional service is likely to result in less CDD than approaching a financial institution. Client accounts can be useful for layering purposes, especially where the criminal wishes to access services, or transactions, that would seem unusual for the individual involved. Client accounts can also be used to integrate proceeds into sectors such as real estate where the use of legal services is common practice.
308. The use of client accounts is attractive to criminals at all three stages of the ML process (placement, layering, and integration) as client accounts can:
    - Be used as part of the first step in converting proceeds of crime into other less-suspicious assets
    - Permit access to the financial system when the criminal may otherwise appear suspicious or undesirable to a financial institution
    - Serve to hide the true ownership of criminally derived funds or other assets
    - Be used as a link between different ML/TF techniques, such as purchasing real estate or setting up shell companies/trusts and transferring the proceeds of crime
309. Client accounts can pool funds, making it difficult to investigate or trace ML activity.
310. Red flags associated with client accounts include:
    - Use of a client account without underlying legal transactions or legal work
    - Requests for payments to third parties without substantiating reason or corresponding transaction
    - Funds sent to countries with high levels of secrecy
    - Transfers structured to avoid threshold reporting requirements
    - Unusual speed of transactions requested
    - Transactions aborted after receipt of funds and there is a request to send funds to a third-party

[31] http://bit.ly/2Asgb3N

High-risk customers and jurisdictions

311. Customers represent the primary source of ML/TF risk for reporting entities. Every effort should be made to ensure CDD is carried out in line with a risk-based approach and is both robust and proportionate. Given the importance of CDD, reporting entities need to be mindful of identify fraud and the use of uncertified or counterfeit identity documents.
312. 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, and casinos. In addition to the ML/TF opportunities, money launderers may be attracted to a business because its industry provides access to other facilitators of crime. FIU research indicates that transport businesses, pharmacies and bars may all be used to facilitate the trafficking and sale of illicit drugs.
313. 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 co-mingling cash proceeds with cash takings from a business to place funds in a financial institution establishes a legitimate origin for the cash, and reduces suspicion and detection by a financial institution.
314. Small, cash-intensive businesses are attractive to criminals as they may also be expected to have less sophisticated AML/CFT awareness.
315. At the layering stage, criminals may move funds through business accounts 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 can effectively obscure the involvement of beneficial criminal owners in a transaction.
316. Remitters and alternative remitters outside of the formal financial sector present well documented ML/TF risk. For the purposes of the Phase 2 SRA, this also covers foreign currency exchanges. **This high-risk factor concerns the use of remitters as a typology of ML/TF. It does not highlight the remittance industry as an ML/TF risk as a whole.**
317. The FATF has classified alternative remittance into three categories:
    - **Traditional hawala and similar service providers –** Providers may establish traditional services within emerging or existing ethnic communities
    - **Hybrid gatekeepers and alternative remittance providers –** Gatekeepers may expand their services to offer alternative remittance
    - **Criminal alternative remittance providers –** These are established or expanded to serve criminals and/or circumvent controls. They are by nature high risk and may be connected to complex specialised ML/TF networks managed by offshore international "controllers"
318. Currency exchange businesses are vulnerable to ML/TF. 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.
319. 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. There is no universally agreed definition of a high-risk country, but when undertaking a risk assessment, some variables to consider include countries that are:
    - Identified as lacking adequate AML/CFT systems/measures or controls
    - Identified as having supporters of terrorism or the financing of terrorism
    - Identified as having significant levels of corruption and/or organised crime
    - Identified by credible sources as being tax havens
    - Associated with production and/or transnational shipment of illicit drugs or people trafficking
    - Subject to sanctions, embargoes or similar measures
320. The Act does not prohibit business relationships or transactions with persons/organisations based in high-risk countries. However, reporting entities should make sure sufficient mitigation and control measures are in place. When dealing with a high-risk jurisdiction, the following ML/TF factors should be considered:

- Is the country a conflict zone or a jurisdiction associated with terrorism?
- Does the country have laws that make it illegal to launder money or finance terrorism?
- Does the country's legislative framework put obligations on financial institutions for CDD, account monitoring, SARs and record keeping similar to those set out in the Act?
- Does the country have an established and effective AML/CFT supervisory regime?
- Is the country a member of the FATF or a FATF-style regional body (e.g. the APG)?
- Has the country been subject to any recent independent assessment of its AML/CFT systems/measures (i.e. a FATF mutual evaluation)?
- Are there any public concerns raised about the country's AML/CFT systems/measures?
- Does the country have a high degree of organised crime, bribery and corruption, or people trafficking?

321. 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. As such, reporting entities may wish to consider "high-risk jurisdictions" to cover both high ML/TF risk countries and their neighbours.
322. For further guidance, refer to the sector supervisors' *Countries Assessment Guideline*[32].

PEPs and high net worth individuals

323. Reporting entities should establish whether the customer is a politically exposed person (PEP) or a relative/close associate (RCA) of a PEP. If they are, then enhanced CDD (most commonly known as "EDD") will be required. However, not all PEPs carry the same risks depending on the country the PEP is from, where they are located (see the "High-risk customers and jurisdictions" section above) and the position of power or funds the person holds or controls.
324. For very high-risk PEPs, extra AML/CFT measures will be needed.
325. Senior management authorisation is required by the Act to establish a business relationship with a PEP. The reporting entity must also obtain information about the source of wealth or source of funds of the PEP.
326. Foreign PEPs may use banking facilities in other countries to launder funds away from scrutiny in their home jurisdiction using the New Zealand financial 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.
327. Facilities provided to higher net worth customers and heads of international organisations (HIOs), particularly those with dedicated customer representative relationships, can be misused for ML/TF. This is especially the case if transactions are rarely questioned because of the high-value of the business to the reporting entity.
328. High net worth individuals/HIOs may have patterns of financial activity that can be exploited to mask ML/TF. Value, volume and velocity red flags that would apply to other customers may be ignored for presumed legitimate activity.
329. PEPs and high net worth individuals/HIOs have been linked to corruption and bribery. To fight corruption and ML/TF, the FATF 40 Recommendations provide preventative measures relating to CDD, PEPs, record keeping, the transparent movement of funds through wire transfers or physical transportations of cash, and the transparency of the beneficial ownership of legal persons and arrangements.
330. The sources for the funds that a PEP/HIO may try to launder are not only bribes, illegal kickbacks and other directly corruption-related proceeds but also embezzlement, tax fraud, and theft of State assets or funds from political parties and unions. PEPs/HIOs that come from countries or regions where corruption is endemic, organised and systemic present the greatest risk. However, it should be noted that corrupt or dishonest PEPs/HIOs can be found in almost any country.
331. Transparency is an issue that goes beyond the fight against corruption and ML/TF. It also impacts tax evasion, corporate governance, and the fight against all types of criminal activity.
332. The FATF has produced several papers on this topic, including *Specific Risk Factors in Laundering the Proceeds of Corruption: Assistance to Reporting Institutions (2012)*.[33]

[32] http://bit.ly/2hOTHPk

[33] http://bit.ly/1M0fkGo

Appendix 9: Suggested reading and source documents

333. All the following are open source documents used in the production of the Phase 2 SRA. They can be accessed via a simple internet search. Some documents are 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 – *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 Combating 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
- FATF Report – *Proliferation Financing Report* – June 2008
- FATF Report – *Money Laundering and Terrorist Financing through the Real Estate Sector* – June 2007
- APG – *APG Yearly Typologies Report 2016*
- APG – *APG Yearly Typologies Report 2015*
- APG – *APG Yearly Typologies Report 2014*
- APG – *Trade Based Money Laundering Typologies* – July 2012
- APG – *New Zealand Mutual Evaluation Report (MER)* – 2010
- UNODC – *Risk of Money Laundering through Financial Instruments – 2nd Edition* – 2013
- European Supervisory Authorities (ESA) – *Final Guidelines – Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849: Risk Factor Guidelines* – June 2017
- 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
- Basel Institute on Governance – *AML Index* – August 2014
- Transparency International – *Doors Wide Open: Corruption and Real Estate in Four Key Markets* – 2017
- Transparency International – *Tainted Treasures: Money Laundering Risks in Luxury Markets* – April 2017
- 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 Combating Money Laundering and Terrorist Financing* – May 2015
- FINTRAC – *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada* – July 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 – *Insights from Compliance Assessments* – December 2016
- AUSTRAC – *Methodologies Brief 01 – Building a Profile: Financial Characteristics Associated with Known Foreign Terrorist Fighters and Supporters* – December 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
- AUSTRAC – *Insights from Compliance Assessments* – December 2016

- 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)
- International Bar Association, American Bar Association and Council of Bars and Law Societies – *A Lawyer's Guide to Detecting and Preventing Money Laundering* – October 2014
- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2017*
- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2010*
- FIU – *National Risk Assessment of Money Laundering and Terrorist Financing 2010 – Support Document*
- FIU – Quarterly Typology Reports (multiple and ongoing)
- FIU – Guidelines relating to reporting of suspicious transactions – 2013
- FIU – Terrorism Suppression Act 2002 Advisory – 2013
- FIU – Financial Action Task Force (FATF) statements and advisories (ongoing)
- FIU – PTR: Understanding the Regulations – 2017
- FIU – PTR: Reporting (Obligation) Guidance – 2017
- DIA – AML/CFT Sector Risk Assessment Guides (multiple) – April 2014
- DIA – *Internal Affairs AML/CFT Sector Risk Assessment* – March 2011
- FMA (then Securities Commission) – *Anti-Money Laundering and Countering the Financing of Terrorism Sector Risk Assessment* – March 2011
- FMA – *Anti-Money Laundering and Countering Financing of Terrorism Sector Risk Assessment* – 2017
- RBNZ, DIA and FMA – *Beneficial Ownership Guideline* – December 2012
- RBNZ, DIA and FMA – *Countries Assessment Guideline* – July 2012
- RBNZ, DIA and FMA – A*ML/CFT Programme Guideline* – December 2011
- RBNZ, DIA and FMA – *Risk Assessment Guideline* – June 2011
- RBNZ – *Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers* – March 2011
- RBNZ – *Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers* – February 2017

Appendix 10: Terrorism financing and dual-use items and proliferation risk factors

This appendix should be read in conjunction with Part 12 of the Phase 2 SRA.

Remitters and alternative remitters (remitters)

334. Remitters are recognised internationally as presenting a high-risk of TF, and reporting entities should be aware of the risks associated with them. To some extent remitters offer a degree of anonymity (variable levels of CDD) 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 remitters and AML/CFT responses to the risks they present should be proportionate and reflect a risk-based approach.

Non-profit organisations and charities

335. The use of non-profit organisations and charities is an internationally recognised TF typology. They 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. Non-profit organisations 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.

336. The FATF reports that the non-profit organisations most at risk of abuse are those engaged in "service" activities that are operating near 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 non-profit organisations. 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.

337. However, it is important to consider this TF vulnerability in the context of the lower-risk New Zealand environment, and that this will not apply to the vast majority of New Zealand charities and non-profit organisations.

Cash couriers

338. TF risk associated with cash couriers is assessed internationally as high. This method of TF may be undertaken by multiple individuals and may involve smuggling cash across porous borders to high-risk TF jurisdictions. Bulk cash smuggling can also be used. 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). The 500-euro note was removed from sale in the UK due to its overwhelming use in organised crime.

New Zealand shell companies

339. FIU research indicates that overseas groups have demonstrated a desire to use New Zealand shell companies for activities similar to TF (see examples below). As such, reporting entities should not immediately discount New Zealand companies from suspicion of TF as a matter of course.
    - 2009 – New Zealand 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 clients.
    - 2014 – A New Zealand postal hosting service was apparently abused to establish a website associated with the Islamic State. The persons responsible for the website were successful in using the New Zealand address for activities that could facilitate financing.

FATF and TF

340. TF continues to be a priority issue for the FATF. They have published numerous papers on the topic, including *Terrorist Financing Typologies Report* (2008)[34] , *Terrorist Financing in West Africa* (2013)[35] , *Risk of Terrorist Abuse in Non-Profit Organisations* (2014)[36] and *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* (2015)[37]. This attention reflects global concern in relation to TF and signals the need for reporting entities to give TF due consideration in their AML/CFT risk assessment.

TF indicators and warnings (red flags)

341. Given the difficulty of detecting TF, reporting entities' transaction monitoring systems and procedures will play a key role, especially given PTR obligations. Furthermore, the Phase 2 sectors' knowledge of their customers and their customers' established and expected transactions and activity is vital in determining if TF activity is potentially taking place.

342. ML and TF share many indicators and warnings, or red flags. The following indicators and warnings may help reporting entities in the difficult task of drawing a link between unusual or suspicious activity and TF. The list is not exhaustive, and DIA encourage reporting entities to identify indicators and warnings that may occur in their ordinary course of business as part of their risk assessment. Red flags that may occur across all DIA sectors include:
    - International funds transfers to and from high-risk jurisdictions, potentially at multiple branches of the same reporting entity
    - Multiple customers and/or occasional transactions by non-customers conducting international funds transfers to the same beneficiary located in a high-risk jurisdiction
    - A customer conducting funds 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
    - Large cash deposits and withdrawals to and from non-profit organisation 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 the "Proliferation and dual-use items" section below)
    - A sudden increase in business/account activity, inconsistent with customer profile
    - Multiple cash deposits into personal account described as "donations" or "contributions to humanitarian aid" or similar terms
    - Multiple customers using the same address/ telephone number to conduct business/ account activity
    - Prescribed entities or entities suspected of terrorism using third-party accounts (e.g. a child's account or a family member's account) to conduct transfers, deposits or withdrawals
    - Use of false identification to establish New Zealand 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 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
    - Customers converting small-denomination bank notes into high-denomination notes (especially US dollars, euros or sterling)

Emerging TF risk

343. The FATF has highlighted the need for forward-looking analysis in relation to TF given the dynamic risk environment. Areas of potential risk are:
    - Foreign terrorist fighters and foreign terrorist supporters
    - Fundraising through social media
    - New payment products and services
    - Exploitation of natural resources

344. The extent to which these avenues have been exploited for TF purposes is unclear and,

[34] http://bit.ly/2xfrtXB

[35] http://bit.ly/1GyZayn

[36] http://bit.ly/2A1Bp7M

[37] http://bit.ly/1AOrZIw

although these activities may not have an immediate association with reporting entities, their potential impact on TF should be noted.

345. The dynamic nature of the TF environment necessitates that reporting entities should make sure their compliance officers maintain situational awareness in relation to this topic. Reporting entities should also make sure that in the face of evolving TF their AML/CFT measures are both adequate and effective.

346. This should be reflected in relevant AML/CFT documentation and be evidenced by regular testing and validation. While the likelihood of TF in New Zealand may be low compared to other jurisdictions, the consequences are potentially catastrophic.

Proliferation and dual-use items

347. These items are taken from the FATF *Proliferation Financing Report* (2008)[38].

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/Coolers	Presses	Isostatic presses
Pulse generators	Connectors	Pumps	Composites
X-ray flash apparatus	Heat exchanges	Spray dryers	Maraging steel
Pressure gauges	Precursors	Tanks	Homing devices
Ignition	Pumps	Growth media	Oxidants
Vacuum pumps	Reactors		Machine tools

[38] http://bit.ly/2zBY0Yd

348. The FATF *Proliferation Financing Report* (2008) identified the following general risk factors:
    - Weak AML/CFT controls and/or weak regulation of the financial sector. A weak or non-existent export control regime and/or weak enforcement of the 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.
    - The presence of industry that produces weapon of mass destruction components or dual-use goods.
    - A relatively well-developed financial system or an open economy. A jurisdiction that has secondary markets for technology. The nature of the jurisdiction's export trade.
    - 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.

Appendix 11: AML/CFT abbreviations and acronyms

349. This table contains abbreviations and acronyms used in this document and in the wider AML/CFT environment. It is included for reference purposes.

1LOD, 2LOD etc.	first line of defence, second line of defence…
AML	anti-money laundering
AML/CFT compliance officer	compliance officer
APG	Asia Pacific Group
ATAINZ	Auditors and Tax Agents New Zealand
AUSTRAC	Australian Transaction Reports and Analysis Centre
BCR	border cash report
BO	beneficial owner
CAANZ	Chartered Accountants Australia and New Zealand
CBR	correspondent banking relationship
CDD	customer due diligence
CFT	countering financing of terrorism
CPRA	Criminal Proceeds (Recovery) Act 2009
CTR	cash transaction report (part of prescribed reporting)
DBG	designated business group
DIA	Department of Internal Affairs
DNFBP	designated non-financial business or profession/gatekeeper
EDD	enhanced customer due diligence
Egmont	Egmont group of international FIUs
FATF	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)
FMA	Financial Markets Authority
FSRB	FATF style regional body (APG is an FSRB)
FTRA	Financial Transaction Reporting Act 1996
goAML	FIU reporting system for STRs/SARs
HIO	head of international organisation (e.g. a company president or CEO)
HVD	high-value dealer
I&W	indicators and warnings (of ML/TF)
IFT	international fund transfer (part of prescribed reporting)
IFTI	international fund transfer instruction (part of prescribed reporting)
IVCOP/IDVCOP	Identity Verification Code of Practice

LCT	large cash transaction (part of prescribed reporting)
LPP	legal professional privilege
MER	mutual evaluation report
ML	money laundering
MSB	money service business
N&P	nature and purpose
NBDT	non-bank deposit taking entity
NBNDT	non-bank non-deposit taking entity
NCC	National Coordination Committee
NRA	National Risk Assessment
NZRB	New Zealand Racing Board
PAOBO	person acting on behalf of
PEP	politically exposed person
Phase 2	Phase 2 of the AML/CFT Act
POWBATIC	person on whose behalf a transaction is carried out
PPCs	procedures, policies and controls
PTR	prescribed transaction report
QA	quality assurance
RA	risk assessment
RBNZ	Reserve Bank of New Zealand
RCA	relative/close associate (of PEP)
RE	reporting entity
Regs	AML/CFT Regulations
SAR	suspicious activity report
SPR	suspicious property report (Terrorism Suppression Act 2002)
SRA	sector risk assessment
STR	suspicious transaction report
SVI	stored value instruments
TBML	trade-based money laundering
TCSP	trust and company service provider
TF	terrorism financing
TM	transaction monitoring
TSA	Terrorism Suppression Act 2002
UNODC	United Nations Office on Drugs and Crime