Anti-money laundering and counter-terrorist financing measures

New Zealand

Mutual Evaluation Report

April 2021

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org.**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This assessment was adopted by the FATF at its February 2021 Plenary meeting.

Citing reference:

FATF (2021), *Anti-money laundering and counter-terrorist financing measures – New Zealand,* Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-new-zealand-2021.html

Photo Credit - Cover: © Miles Holden

Table of Contents

Executive Summary

1. This report summarises the AML/CFT measures in place in New Zealand as at the date of the on-site visit from 26 February to 15 March 2020. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of New Zealand's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

a) New Zealand has a robust understanding of its money laundering and terrorist financing (ML/TF) risks. It has established a comprehensive multi-tiered risk assessment process, with its national risk assessment (NRA) undergoing two full cycles. National AML/CFT policies and activities address identified ML/TF risks to a substantial extent. Authorities have taken action to respond to emerging TF risks in the context of a lower overall risk profile. Domestic co-ordination and co-operation are strengths of New Zealand's AML/CFT system.

b) New Zealand's law enforcement agencies (LEAs) regularly use financial intelligence. The New Zealand Police Financial Intelligence Unit (FIU) produces and disseminates a wide range of financial intelligence products, which generally support the operational needs of competent authorities. However, New Zealand authorities could benefit from better exploiting the potential of financial intelligence to detect criminal activity by persons not already known to law enforcement.

c) New Zealand identifies and pursues parallel money laundering investigations alongside investigations of significant proceeds-generating. Its authorities are adequately skilled and trained to conduct financial investigations with a wide range of investigative tools are available to them. Financial investigations are increasingly being used to support prosecution on money laundering charges and the number of prosecutions into ML have increased since 2018.

d) New Zealand Police has a strong focus on confiscation of proceeds of crime, backed by a top-level target for the volume of criminal assets to be restrained (NZD 500 million by 2021). The skilled Asset Recovery Unit (ARU) works in co-operation with investigative authorities to initiate parallel restraint and forfeiture proceedings in response to identified crime and financial intelligence. New Zealand has pursued international asset recovery cases that involve significant volumes of inbound and outbound proceeds.

e) There is sound co-operation and co-ordination between New Zealand Police's National Security Group (NSG), Financial Crime Group (FCG) (including the NZPFIU) and other relevant agencies on monitoring possible Terrorist Financing. Following the 2019 Christchurch attacks, New Zealand demonstrated its capacity and effectiveness in undertaking and supporting terrorism financing investigations. New Zealand has not prosecuted any terrorism financing cases, which is consistent with its generally low TF risk profile.

f) There is a strong legislative framework for the implementation of targeted financial sanctions (TFS) without delay. However, reporting entities have a variable understanding of TFS, due to limited guidance and outreach by relevant authorities, as well as the lack of a mandate for supervisors to undertake supervision of TFS implementation. No assets have been frozen in New Zealand pursuant to TFS regimes. While this may be consistent with New Zealand's risk profile, it could also reflect the limited TFS guidance, and the lack of outreach and supervision on TFS. New Zealand authorities have prosecuted a contravention of export restrictions under UNSC DPRK sanctions.

g) New Zealand covers financial institutions (FIs), designated non-financial businesses and professions (DNFBPs) and most virtual asset service providers (VASPs) as reporting entities under the *Anti-Money Laundering and Countering the Financing of Terrorism Act 2009* (AML/CFT Act). There remain some gaps in the AML/CFT Act, which impact New Zealand's overall effectiveness. Reporting entities' understanding and implementation of their AML/CFT obligations is mixed, with a better understanding and implementation in larger and more sophisticated reporting entities.

h) New Zealand's three AML/CFT supervisors have a good understanding of the inherent ML/TF risk profiles of their respective sectors. The scope and depth of supervision for each financial sector are broadly commensurate with their respective risk levels, except for the banking sector, where the scope and depth of inspections does not adequately reflect the risk and complexity of the banks inspected. There is scope to improve the range of sanction powers available to the supervisors and for the supervisors to impose sanctions that are more effective, proportionate and dissuasive.

i) Most DNFBPs were only brought within the scope of AML/CFT regulation in 2018 as part of New Zealand's 'Phase 2'. The newly supervised Phase 2 reporting entities and VASPs are still developing their understanding of their ML/TF risks and how AML/CFT obligations apply to their business. The level of suspicious transaction report (STR) and suspicious activity report (SAR) reporting by some DNFBPs remains low. AML/CFT supervision for Phase 2 sectors is at an early stage but the rollout of new obligations has been conducted in an effective and well-managed way so far.

j) New Zealand's legal system provides for a wide range of legal persons and arrangements, and authorities have a comprehensive understanding of the ML/TF risks associated with them. In recent years, New Zealand has implemented measures to mitigate the ML/TF risks of misuse of legal persons and arrangements, including the creation of a register of New Zealand Foreign Trusts, and residency requirements for company directors. However substantial gaps remain in relation to ensuring the availability of adequate, accurate and current beneficial ownership information, and in relation to nominee directors and shareholders.

k) Authorities actively respond to formal and informal international co-operation requests. New Zealand has a sound legal basis to provide and seek MLA and extradition. Several different competent authorities are involved in handling extradition requests and there is no clear authority with primary responsibility. New Zealand has received positive feedback from counterparts concerning the quality and timeliness of assistance provided. LEAs and supervisors also engage in various forms of international co-operation with counterparts.

Risks and General Situation

2. New Zealand faces ML threats from proceeds of crime generated both domestically and internationally, particularly through its financial, legal, property and cash-intensive sectors. While New Zealand is a high integrity jurisdiction with comparatively low crime rates, it has a very open economy, with free flow of capital and people and substantial ease of access to legal persons and arrangements. The major domestic proceeds-generating crimes are drugs, fraud, and tax offending. Transnational organised crime groups seek to move funds through New Zealand, its financial system, and its legal structures. Several sectors in New Zealand have also been identified as significant in terms of their scale, role, or vulnerability. These include the banking, money or value transfer services (MVTS), real estate and professional services sectors.

3. New Zealand companies and limited partnerships are vulnerable to abuse for ML/TF purposes due to the low cost with which they can be established, as well as New Zealand's reputation as a well-regulated jurisdiction. Nominees are able to provide resident director or trustee services for oversees customers. Law enforcement have

noted the abuse of New Zealand shell companies for both transnational and domestic laundering. Domestically, trusts are widely used in New Zealand and there are comparatively fewer measures to enable law enforcement to detect the abuse of trusts for ML/TF purposes.

4. For TF, the greatest risk to New Zealand for large-scale financing of terrorism remains in relation to overseas-based groups, within an overall low TF risk. However, the potential consequences of small-scale domestic TF could be very high. In particular, funds may be used within, or sent to, New Zealand to finance terrorism activity by lone actors or small cells. Following the Christchurch attacks on 15 March 2019, New Zealand's national threat level was raised to 'high' and sat at 'medium' as of March 2020. New Zealand authorities remain alert to the possibility that funds may be raised, moved or used for terrorist purposes in New Zealand.

Overall Level of Compliance and Effectiveness

5. New Zealand has implemented an AML/CFT system that is effective in many respects. Particularly strong results are being achieved in relation to the confiscation of proceeds of crime. New Zealand also has a good understanding of its ML/TF risks, uses financial intelligence and investigates and prosecutes ML/TF activity effectively, and co-operates with its international partners well. However, major improvements are needed to strengthen supervision and implementation of preventive measures, to improve the transparency of legal persons and arrangements, and to ensure that TFS are being effectively implemented.

6. In terms of technical compliance, New Zealand fundamentally overhauled its AML/CFT regime with the introduction of the AML/CFT Act 2009. This was extended in 2018 to cover all DNFBP sectors. The Act also covers most VASPs as a type of financial institution. While this is significant progress, further work is needed to fully embed AML/CFT measures among DNFBPs, and a number of preventive measures need reform to meet the FATF Standards. New Zealand also needs to improve its technical framework in relation to TFS, beneficial ownership of legal persons and arrangements and the powers and responsibilities of supervisors.

Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7. New Zealand has a robust understanding of its ML/TF risks and has established a comprehensive multi-tiered risk assessment process. This includes their NRA and four sectoral risk assessments (SRAs). The NRA is comprehensive and systematic in its identification of New Zealand's ML/TF risks and has been refined over successive updates, though there is scope for further minor improvements. New Zealand authorities share a sound understanding of their risks, with the results of the NRA and SRAs communicated to all stakeholders, including the private sector.

8. National AML/CFT policies and activities address the identified ML/TF risks to a large extent, although New Zealand's policy response has not completely addressed the risks associated with beneficial ownership, and New Zealand should undertake further supervisory activity against unregistered MVTS providers. The objectives and activities of the supervisors and LEAs to prevent, detect and respond to ML/TF are informed by the risk assessments. Authorities have also taken action to respond to emerging TF risks, in the context of New Zealand's overall lower risk profile for TF. New Zealand has introduced enhanced measures in certain circumstances and allows

for simplified measures in specific justified circumstances. New Zealand has granted a large number of exemptions from AML/CFT requirements but is not clear that some historical and transitional exemptions granted are based on proven low ML/TF risks or applied in strictly limited and justified circumstances.

9. Domestic co-ordination and co-operation are strengths of New Zealand's AML/CFT system. Competent authorities have a strong tradition of co-ordination and collaboration, and continually work to improve the flow of information between authorities.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

10. New Zealand's law enforcement agencies routinely conduct parallel financial investigations and regularly use financial intelligence to support investigations, trace assets, enforce forfeiture orders and identify risks. LEAs obtain financial information both from the FIU, via direct access to the FIU's database, and through requests to financial institutions and DNFBPs.

11. The Police FIU is well-situated to understand law enforcement priorities and strategic objectives, and is its collaborative relationship with LEAs is a key strength. The FIU produces and disseminates a wide range of financial intelligence products, which generally support the operational needs of competent authorities.

12. The FIU's approach to prioritisation and targeting relies on feedback from police units, in response to strategic intelligence and raw financial intelligence, to refine the FIU's priorities for deeper analysis. New Zealand authorities could nevertheless upgrade their analytical tools to better exploit the potential of financial intelligence to detect criminal activity by persons who are not already of interest to law enforcement, and to take advantage of reports on international funds transfers and large cash transactions.

13. Most SARs and PTRs are received from banks and MVTS, with a limited number received from DNFBPs and TCSPs. In relation to criminal activity, the financial intelligence that the FIU receives is generally in line with New Zealand's risk profile.

14. New Zealand authorities use various multi-agency groups to co-operate and exchange information and financial intelligence. This includes a public-private partnership with financial institutions used by Police and Customs to conduct joint operations at both the tactical and strategic level.

15. New Zealand identifies and pursues parallel money laundering investigations alongside investigations of significant proceeds-generating its authorities are adequately skilled and trained to conduct financial investigations with a wide range of investigative tools are available to them. Operational agencies actively co-operate and share information and resources.

16. Financial investigations are increasingly being used to support prosecution on money laundering charges and the number of prosecutions into money laundering have increased since 2018. This is a result of policy and operational measures put in place to address the stronger focus on asset recovery as compared to prosecution of money laundering offences.

17. The operating strategy of New Zealand's Police reflects a strong and committed focus on confiscation of the proceeds of crime. National strategy documents identify a target volume of criminal assets to be restrained (NZD 500 million by 2021), and the

Criminal Proceeds (Recovery) Act 2009 (CPRA) provides a civil confiscation framework to detect and trace the widest range of criminal proceeds and benefits of crime. New Zealand Police has established a skilled Asset Recovery Unit (ARU), which works in co-operation with domestic and foreign investigative authorities to initiate parallel restraint and forfeiture proceedings in response to identified crime and financial intelligence. New Zealand also pursues asset sharing or repatriation transnationally and has pursued international asset recovery cases that involve significant volumes of inbound and outbound proceeds. This is supported by a sophisticated and effective asset management system managed by the Official Assignee that works to maintain the value of assets seized.

18. New Zealand Customs Service conducts operations, investigations and pursues intelligence to detect non-declared cash, but only a small portion of this is confiscated and the penalties applied are not sufficiently dissuasive.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

19. New Zealand has dedicated units with responsibility for monitoring possible terrorism financing within the FIU and in the National Security Group (NSG) of the New Zealand Police. There is strong co-operation and co-ordination between the NSG and the Police's Financial Crime Group (FCG, which includes the FIU) and other relevant agencies, and the NSG draws on financial investigation expertise from within the FCG as required. New Zealand Police have established standard operating procedures for managing terrorism financing investigations. Authorities demonstrated their capacity and effectiveness in undertaking and supporting terrorism financing investigations following the Christchurch attacks.

20. New Zealand has not prosecuted any terrorism financing cases to date, which is consistent with its risk profile, as articulated in the NRA (investigation of the 2019 Christchurch attack did not find a TF case to prosecute). New Zealand has taken steps to understand its TF risk exposure following the emergence of the foreign terrorist fighter threat, and took steps commensurate with these risks, including to improve co-ordination among relevant agencies.

21. There is a sound legislative framework for the implementation of TFS without delay, which gives immediate and automatic effect to UN Security Council designations under New Zealand law. New Zealand has also made active use of designations by the Prime Minister pursuant to its implementation of UNSCR 1373 in the Terrorism Suppression Act 2002 in relation to global and regional terrorist organisations.

22. Currently no competent authority has a mandate to undertake supervision of financial institutions or DNFBPs for compliance with their TFS obligations. The level of understanding of TFS obligations among reporting entities is variable, due to the absence of supervision and the limited guidance and outreach by relevant authorities. At the time of the on-site visit, a proportion of reporting entities, mainly DNFBPs, did not receive notification of updates to counter-terrorism TFS lists, nor was there a process in place to notify reporting entities of updates to Iran and DPRK TFS lists. Together with the lack of supervision, this lessened the impact of measures applied in response to older cases of proliferation connected to New Zealand.

23. No assets have been frozen in New Zealand pursuant to any TFS regimes. While this may be consistent with New Zealand's risk profile, it could also reflect the limited guidance and the lack of outreach to and supervision of reporting entities for TFS. New

Zealand authorities have prosecuted a contravention of export restrictions under UNSC DPRK sanctions.

Preventive measures (Chapter 5; IO.4; R.9–23)

24. New Zealand covers FIs, DNFBPs and most VASPs under the AML/CFT Act as reporting entities. However there are moderate shortcomings in the AML/CFT Act, particularly in relation to political exposed persons (PEPs), MVTS, wire transfers, internal controls, higher-risk countries, AML/CFT obligations for dealers in precious metals and stones (DPMS), the definition of trust and company service providers (TCSP), and real estate customer due diligence (CDD) obligations, which impact New Zealand's overall compliance and effectiveness.

25. Reporting entities' overall understanding and implementation of their AML/CFT obligations is mixed. Larger and more sophisticated reporting entities have a better understanding of their ML/TF risks and AML/CFT obligations, while newly supervised DNFBPs (Phase 2 reporting entities) and VASPs are largely still developing their understanding of their ML/TF risks and their awareness of obligations.

26. The implementation of AML/CFT controls by banks and other large FIs is generally of a good standard. However, there are areas that could be enhanced, including PEPs and sanctions screening, CDD on existing customers, and group-wide risk management. The level of implementation of AML/CFT rules in the MVTS sector is variable. The AML/CFT controls implemented by Phase 2 reporting entities are less sophisticated than those of sectors where AML/CFT rules are longer-established and are still developing. The implementation of AML/CFT controls by casinos and TCSPs could also be enhanced further.

27. The level of STR and SAR reporting by DNFBPs remains low, particularly by TCSPs, law firms, accounting practices and real estate agents. The challenges faced by reporting entities in the registration and filing process with the FIU portal presents a barrier to effective reporting.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

28. New Zealand has three supervisors (the Reserve Bank of New Zealand (RBNZ), the Financial Markets Authority (FMA) and the Department of Internal Affairs (DIA)) which oversee compliance with AML/CFT obligations. However, no agency has a mandate to supervise the implementation of TFS obligations.

29. New Zealand authorities generally apply effective licensing and registration measures for FIs and VASPs, although some technical deficiencies were identified. Licensing bodies for DNFBP sectors apply licensing and screening measures to a varying degree, and TCSPs, high-value dealers, and some accounting practices are not subject to licensing or registration requirements.

30. The AML/CFT supervisors maintain an overall good understanding of the inherent ML/TF risk profiles of their respective sectors. The scope and depth of supervision for each financial sector is broadly commensurate with their respective risk levels, except for the banking sector, where the scope and depth of inspections does not adequately reflect the risk and complexity of the banks inspected, due in part to a lack of adequate resources available to conduct AML/CFT inspections in RBNZ. AML/CFT supervision for Phase 2 sectors has been conducted in an effective and well-managed way so far but remains at an early stage and has not yet progressed from outreach and awareness-raising to inspection and enforcement.

31. Supervisors generally apply remedial actions in an effective manner. However, the range of sanctions powers available to the supervisors under the AML/CFT Act is inadequate, particularly the low range of pecuniary penalties available and the lack of administrative penalties, and the sanctions that have been applied in practice do not appear to have been fully effective, proportionate and dissuasive. Reporting entities generally have good communication and working relationships with the AML/CFT supervisors.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

32. Basic information on legal persons is publicly available on a number of registers held by the Ministry of Business, Innovation and Employment (MBIE). Some types of trusts are also registered with various agencies, though New Zealand does not have a register of all domestic trusts.

33. New Zealand has a comprehensive understanding of the ML/TF risks of legal persons and legal arrangements. In recent years, New Zealand has implemented specific additional measures to mitigate the risks of misuse of legal persons and arrangements that it has identified, including creation of the register of New Zealand Foreign Trusts, the creation of an Integrity and Enforcement Team, responsible for ensuring the integrity of corporate registries, and introduction of residency requirements for company directors. New Zealand has also established an Integrity and Enforcement Team within MBIE, responsible for assuring the integrity of information held in registries. However, major gaps remain in New Zealand's framework: there are insufficient measures to mitigate the risks posed by nominee directors and shareholders; insufficient mechanisms for authorities to obtain adequate, accurate and current beneficial ownership information for legal persons and insufficient measures for adequate, accurate and current information on trusts, which are very common in New Zealand.

34. A range of sanctions are available for failures to comply with information requirements. New Zealand has effectively used its ability to deregister companies to promote compliance. However, there are insufficient sanctions applied to individuals and to breaches of information requirements for other types of structures (e.g. partnerships, trusts),

International co-operation (Chapter 8; IO.2; R.36–40)

35. New Zealand has a sound legal basis to provide and to seek MLA and extradition in relation to ML/TF and associated predicate offences. New Zealand authorities actively respond to formal and informal international co-operation requests. They have received positive feedback from counterparts on the quality and timeliness of assistance provided.

36. The central authority for MLA, the Crown Law Office, has mechanisms in place to prioritise MLA requests and ensure timely responses, although these mechanisms are relatively informal. Several competent authorities are involved in handling extradition requests and there is no clear authority with primary responsibility.

37. New Zealand authorities make MLA requests to the extent needed to build cases and are willing to pursue proceeds of crime located offshore. The number of outgoing requests has been increasing in recent years. LEAs in New Zealand actively engage in various forms of international co-operation with counterparts. The AML/CFT supervisors engage in close international co-operation with foreign regulators. New Zealand also shares basic and beneficial ownership with international counterparts.

Priority Actions

a) Improve the availability of accurate and up-to-date beneficial ownership information on legal persons, particularly limited liability companies and partnerships, and domestic trusts, and take steps to mitigate the ML/TF risks of nominee shareholders and directors.

b) Ensure that supervisors have a sufficient range of proportionate and dissuasive sanctions available, and that RBNZ has adequate resources to apply the appropriate scope and depth of supervision to banks.

c) Give clear powers and mandates to appropriate agencies to supervise and enforce TFS obligations, supported by outreach to reporting entities, a point of contact for TFS-related queries, and enhanced dissemination of updates to sanctions lists.

d) Consolidate implementation of Phase 2 of the AML/CFT Act, including by further developing DNFBPs' understanding of their risks and obligations; ensuring that they are registered with the FIU reporting system and submit reports; and progressing towards a mature supervision regime for these sectors.

e) Improve the FIU's tools for prioritisation, database integration and analysis of financial intelligence to enhance its ability to directly identify new targets and trends. Conduct outreach to enable LEAs to make more use of FIU proactive financial intelligence products to launch investigations into new targets.

f) Update New Zealand's laws and regulations to address gaps and vulnerabilities including: shortcomings relating to licensing and registration of FIs and DNFBPs; gaps in preventive measures (particularly for MVTS); and the authorisation of essential human needs for sanctioned individuals.

g) Take steps to sustain the recent increase in money laundering prosecutions, by monitoring trends and outcomes through better data and statistics and considering development of ML prosecution guidelines.

Effectiveness & Technical Compliance Ratings

Table 1. Effectiveness Ratings

IO.1 - Risk, policy and co-ordination	IO.2 International co-operation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Substantial	**High**	**Moderate**	**Moderate**	**Moderate**	**Substantial**
IO.7 - ML investigation & prosecution	**IO.8 - Confiscation**	**IO.9 - TF investigation & prosecution**	**IO.10 - TF preventive measures & financial sanctions**	**IO.11 - PF financial sanctions**	
Substantial	**High**	**Substantial**	**Moderate**	**Moderate**	

Note: Effectiveness ratings can be either a High – HE, Substantial – SE, Moderate – ME, or Low – LE, level of effectiveness.

Table 2. Technical Compliance Ratings

R.1 - assessing risk & applying risk-based approach	**R.2** - national co-operation and co-ordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	**C**	**C**	**C**	**LC**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
PC	**LC**	**C**	**LC**	**LC**	**PC**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
LC	**PC**	**LC**	**PC**	**LC**	**PC**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
PC	**C**	**C**	**PC**	**PC**	**PC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
PC	**PC**	**LC**	**PC**	**C**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
LC	**LC**	**LC**	**LC**	**LC**	**LC**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international co-operation		
LC	**LC**	**LC**	**LC**		

Note: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 26 February to 15 March 2020.

The evaluation was conducted by an assessment team consisting of:

- Ms Alexandra Bobylkova, Rosfinmonitoring, (FIU of Russian Federation) (FIU expert)
- Mr Gavin Cheung, Hong Kong Monetary Authority (financial expert)
- Mr Evan Gallagher, Australia Transaction Reports and Analysis Centre (AUSTRAC), (FIU and AML/CFT supervisor of Australia) (legal expert)
- Ms Maryam Salman, Central Bank of Bahrain (financial expert), and
- Mr Arvind Saran, India Revenue Service (law enforcement expert).

With the support of

- Mr Tom Neylan, Ms Ravneet Kaur and Mr Ken Menz, FATF Secretariat, and
- Mr Mustafa Akbar and Ms Suzie White, APG Secretariat.

The report was reviewed by Ms Cheryl McCarthy, Financial Supervisory Commission of the Cook Islands; Ms Mun Chooi Wan, Central Bank of Malaysia; and Ms Rebekah Sittner, United States Department of Justice.

New Zealand previously underwent a FATF/APG Mutual Evaluation in 2009, conducted according to the 2004 FATF Methodology. The 2009 evaluation and 2013 follow-up report have been published and are available at: www.fatf-gafi.org/countries/#New%20Zealand.

That Mutual Evaluation concluded that the country was: compliant with eight Recommendations; largely compliant with 17; partially compliant with 6; and noncompliant with 18. New Zealand was rated compliant or largely compliant with 13 of the 16 Core and Key Recommendations. New Zealand was placed on the regular follow-up process immediately after the adoption of its 3rd round mutual evaluation report. In October 2013, New Zealand exited the follow-up process on the basis that it had reached a satisfactory level of compliance with all Core and Key Recommendations.

Chapter 1. ML/TF RISKS AND CONTEXT

38. New Zealand comprises two main narrow and mountainous islands approximately 2 000 kilometres southeast of Australia, the North Island and the South Island, separated by the Cook Strait and a number of smaller islands. The population of New Zealand is 4.9 million of which approximately 1.66 million live in Auckland. The currency is the New Zealand Dollar (NZD).

39. New Zealand is the largest state in the Realm of New Zealand, a collection of states that share the monarch of New Zealand as head of state, located in Oceania. This includes Niue, and the Cook Islands, which are self-governing territories. They have their own APG membership and have their compliance with the FATF Standards assessed separately. The total land area of New Zealand is approximately 268 000 square kilometres. At the date of the on-site, NZD 1 was equivalent to EUR 0.564

40. New Zealand is a constitutional monarchy with a Westminster-style parliamentary democracy. New Zealand does not have a codified constitution. Instead, the constitution is located in a range of legal and extra-legal documents including key statutes, judicial decisions and constitutional conventions. As such, New Zealand adheres to the doctrine of parliamentary supremacy with the executive Government formed from and responsible to the single chamber parliament (the House of Representatives). The constitution increasingly reflects the Treaty of Waitangi as the founding document in New Zealand.[1]

41. New Zealand's legal system is like other common law legal systems in the Commonwealth of Nations. In New Zealand, the courts' role is based on the constitutional principle that the judiciary is independent of the policy makers (the executive) and from the legislature (Parliament). Judges make decisions by interpreting the laws which are passed by Parliament. Parliament passes laws representing the policy decisions which reflect the intention or interests of citizens collectively. The legislature, executive and judiciary operate independently from one another.

42. Parliament consists of the Sovereign (represented by the Governor-General) and the House of Representatives, which has 120 seats. Each parliament has a term of three years, unless dissolved earlier. The Governor-General has the power to summon, prorogue and dissolve parliament. A bill passed by the House becomes law when the Sovereign or Governor-General assents to it. The Executive consists of Ministers, who

1 The Treaty of Waitangi is New Zealand's founding document. The Treaty is an agreement, in Māori and English, made between the British Crown and about 540 Māori chiefs on 6 February 1840. While there are important differences between the Māori and English versions of the Treaty that have been the subject of debate, broadly the Treaty provided for the following:

- Chiefs gave the Crown governance or government over the land;
- The Crown guaranteed the chiefs exercise of chieftainship over their lands, villages and 'all treasured things'. Māori agreed to give the Crown a right to deal with them over land transactions; and
- The Crown gave an assurance that Māori would have the queen's protection and all rights accorded British subjects.

1

are drawn from the House of Representatives, and Government departments. The role of the Executive is to decide policy, propose laws (which must be approved by the legislature) and administer the law. There are 32 central government departments in New Zealand.

43. The court structure consists of (in order of precedence) the Supreme Court, the Court of Appeal, the High Court and the District Court. Decisions of higher courts on issues of law are generally binding on lower courts.

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

44. New Zealand faces ML threats from proceeds of crime generated both domestically and internationally, particularly through its financial, legal, property and retail sectors. New Zealand is a high integrity jurisdiction with comparatively low crime rates. It has a very open economy, with free flow of capital and people and substantial ease of access to legal persons and arrangements.

45. As noted in the 2019 NRA, the major domestic proceeds-generating crimes are drugs, fraud and tax offending. New Zealand is a destination country for methamphetamine and other narcotic substances due to the high retail value of the illegal narcotics. The proceeds generated are laundered through cash deposits, cash purchases of property and high value commodities, remittances and through co-mingling with legitimate business earnings.

46. Compared to drugs, the tax and fraud threat is more likely to comprise of individualistic, smaller value offenders who engage in self-laundering. However, the NRA notes that fraud offenders may have access to more sophisticated methods of ML. The NRA particularly noted the use of electronic transactions, abuse of professional services and companies, business and trust structures in ML related to fraud and tax offending. The NZPFIU estimates that NZD 1.35 billion is generated annually for ML, primarily from drug and fraud offending. This figure excludes ML of proceeds generated overseas and the proceeds of domestic tax offending. The value of transnational ML is likely to be significantly more than this figure.

47. Transnational organised crime groups, including those linked to New Zealand and those not linked to New Zealand, seek to move funds through New Zealand and/or its financial system and/or its legal structures. Transnational networks may seek to exploit New Zealand as a conduit for funds to capitalise on the country's reputation for high integrity and stability. New Zealand has also seen a rise in the presence of gang members establishing themselves from regional jurisdictions. This has provided a setting for a range of organised criminal activities. ML techniques observed by the NZPFIU include the use of wire transfers, the use of shell companies, investment in real estate, and trade-based ML.

48. Several sectors in New Zealand have also been identified as significant in terms of their scale, role, or vulnerability. These include the banking, MVTS, real estate and professional services sectors, as well as the misuse of legal persons and arrangements. There are 27 registered banks in New Zealand. Four banks, which are subsidiaries of the largest Australian banks, hold 82% of the banking sector's total assets. Banks are focused on lending to the domestic private sector, particularly to the real estate market and farms. New Zealand banks also offer other retail services. Many of these are vulnerable to ML, such as international payments.

49. New Zealand also plays a pivotal role as a remittance hub for the Pacific region. The MVTS sector in New Zealand facilitates international payments to over 200 countries. The 2019 NRA identifies alternative remittance as being high risk, with the size and activities of the sector being largely unknown to the authorities. The providers that have been identified appear to be small-scale operations that pool transactions to make consolidated payments.

50. New Zealand has noted that various professional sectors, including law firms, conveyancers, accounting practices, TCSPs and estate agents, are used by money launderers due to their reputation of trustworthiness and professional skills. Police cases routinely involve professional facilitators, including complicit involvement. There have also been low levels of SAR/STR reporting by professionals and the AML/CFT obligations for these sectors (except for TCSPs) remain relatively new. Observed ML methods include laundering funds through trust accounts, the creation and management of trusts and companies, the management of client affairs and the transfer of ownership of assets to third parties. The 2019 NRA also finds that real estate is an asset of choice for laundering in New Zealand, with high numbers of real estate assets restrained and forfeited in New Zealand annually.

51. New Zealand companies and limited partnerships are seen as attractive for illicit finance due to the low cost with which they can be established, as well as New Zealand's reputation as a well-regulated jurisdiction. Nominees are able to provide resident director or trustee services for oversees customers. Law enforcement have noted the abuse of New Zealand shell companies for both transnational and domestic laundering. Domestically, trusts are widely used in New Zealand and there are comparatively fewer measures to enable law enforcement to detect the abuse of trusts for ML/TF purposes. New Zealand also does not tax trusts with overseas settlors, which has created a market for New Zealand Foreign Trusts to be used as asset protection vehicles.

52. New Zealand's 2019 NRA assessed that the greatest risk to New Zealand for large-scale TF remains in relation to overseas-based groups. However, the potential consequences of small-scale domestic TF could be very high. In particular, financing may be used within, or sent to, New Zealand to fund terrorism activity by lone actors or small cells. Following the Christchurch attacks on 15 March 2019, New Zealand's national threat level was raised to 'high' and sat at 'medium' as of March 2020. A marked increase in STR/SAR reporting relating to TF is attributed to the heightened awareness and vigilance on the part of reporting entities and the NZPFIU following the Christchurch attacks. New Zealand authorities did not see this as indicative of a change in the nature of the TF threat, but in line with global trends. However, New Zealand authorities remain alert to the possibility that funds may be raised, moved or used for terrorist purposes in New Zealand.

Country's Risk Assessment & Scoping of Higher Risk Issues

53. New Zealand assesses its ML/TF risks formally through its NRA process. The process of developing the NRA is led by NZPFIU and co-ordinated by the working groups of the National Co-ordination Committee (NCC). Relevant government agencies and certain reporting entities also contributed in this process. Sector Risk Assessments (SRAs) are conducted by the relevant supervisor (the Reserve Bank of New Zealand (RBNZ), the Department of Internal Affairs (DIA) and the Financial Markets Authority (FMA)). There are four SRAs in place across the three supervisors. The SRAs are informed by the findings of the NRA.

54. Both the NRA and the SRAs have been through two full generations and can be updated and amended between iterations in response to significant events or developments. The NRA assess threats, vulnerable channels, and the risks arising from these. The 2019 NRA identifies 18 priority areas and proposes steps at the national policy and agency level to address these risks.

55. In deciding what issues to prioritise for increased focus, the assessors reviewed material provided by New Zealand on their national ML/TF risks (as outlined above), and information from reliable third-party sources (e.g. reports of other international organisations). The assessors focused on the following priority issues, which are broadly consistent with the issues identified in New Zealand's NRA and SRAs.

a. **Banking sector and supervision:** Aside from looking generally at banking sector supervision, the adequacy of compliance and remediation in New Zealand's banking sector, in light of major AML/CFT compliance issues identified in the Australian parent banks by Australian supervisors was reviewed. This includes the response of the New Zealand authorities and the actions taken and the effectiveness of New Zealand banks' internal controls and group-wide compliance programs. Due to the risk of infiltration of foreign criminal proceeds, the effectiveness of controls applied to high-risk customer classes, including PEPs and international retail transactions, was also a focus.

b. **Companies, trusts, and associated gatekeepers (including law firms, accounting practices and TCSPs)**, including the extent to which the relative ease of company formation in New Zealand and the perceived credibility of companies and legal arrangements set up in New Zealand poses ML/TF risks. This involved reviewing the effectiveness of New Zealand's controls and transparency measures for legal persons and arrangements, including timely access to basic and beneficial ownership information, nominee arrangements and resident director or trustee services; the level of supervision and compliance of these sectors and whether it is proportionate to the risks and vulnerabilities. The emergence of transnational professional ML facilitators using such mechanisms, and authorities' efforts to investigate and prosecute this activity was also a focus.

c. **MVTS and the alternative remittance sector**, including how effectively customer due diligence (CDD), transaction monitoring and other controls are applied within the sector, the actions taken by authorities to identify and shut down unlicensed providers and the extent to which alternative payment methods and emerging or new technology are used in this area and how the risks are mitigated.

d. **ML through the real estate sector**, focusing on the regulation of gatekeepers such as real estate agents, law firms and conveyancers. The assessment team reviewed the effectiveness of the preventive measures in place to mitigate the ML/TF risks, supervision in the associated gatekeeper professions and the authorities' effectiveness in investigating and prosecuting ML through the real estate sector and recovering proceeds of crime used to purchase real estate.

e. **Cash deposits and cash-intensive businesses:** Cash and cash deposits are primary vehicles to launder the proceeds of domestic drug and economic crimes, including through cash-intensive businesses and casinos. The effectiveness of the preventative and monitoring measures in place, and the

extent to which these have been effective in minimising cash businesses from being used for ML/TF purposes was reviewed.

f. **New Zealand's approach to TF and PF**, including how New Zealand's CTF measures were used in the response to the 2019 Christchurch attacks, and how authorities are responding to any lessons learned from those events. Assessors also explored whether CTF legislation would adequately support investigation and prosecution of TF in the event of a case arising. Implementation of CTF and CPF TFS was also a focus given that these measures are not subject to supervision.

g. **VASPs:** The NRA 2019 noted that VASPs pose high inherent ML risks and that virtual assets have now become widely available in New Zealand. Between January 2015 and September 2018, the NZPFIU received 380 SARs relating to virtual assets, detailing transactions totalling approximately NZD 150 million. The assessors considered the extent to which New Zealand's AML/CFT framework is sufficiently updated and complies with the FATF Standards for this sector.

56. The main area identified as lower-risk and not warranting significant focus during the course of the assessment is **insurance**. The insurance products most at risk of exploitation for ML are not sold in New Zealand, mitigating many of the associated ML/TF risks.

Materiality

57. New Zealand has a small open economy and is heavily dependent on international trade. New Zealand's 2019 GDP of USD 206 billion places it 53rd in global nominal rankings and 68th in purchasing power parity rankings. Services industries are the largest sector, followed by goods-producing industries. Primary industries dominate the exports sector. Economic activity is highly concentrated in the North Island, and in particular in Auckland.

58. New Zealand's economy is very open and known for its business-friendly environment. It ranks first on the World Bank ease of doing business index, which notes New Zealand has the lowest number of procedures necessary to start a business and the shortest time in which to start a business.

59. New Zealand's financial system is comparatively simple by advanced economy standards and is dominated by the banks. There are 27 registered banks in New Zealand with the four largest banks being Australian owned and accounting for 82 percent of total bank assets (NZD 556 billion in March 2020). New Zealand's net external liabilities are high relative to most other developed economies. Offshore bank funding accounts for almost two-thirds of New Zealand's net external liabilities.

60. Other sectors of the financial system are much smaller. Financial firms that offer deposit products, but are not registered banks, must obtain a non-bank deposit taker (NBDT) license from the RBNZ. There are 20 licensed NBDTs in New Zealand, with total assets of NZD 2.5 billion that account for approximately 2 percent of the financial sector assets. New Zealand's insurance sector has around NZD 70 billion in total assets, equivalent to 25 percent of the GDP.

61. Although not a major financial centre, New Zealand is an important regional remittance centre for the South Pacific. There are strong remittance networks between New Zealand and Pacific nations. New Zealand estimates that remittance flows to the

Pacific Islands from New Zealand constitute around a quarter of the total amount remitted to the region.

Structural Elements

62. New Zealand has all of the key structural elements required for an effective AML/CFT system including political and institutional stability, governmental accountability, rule of law, and a professional and independent bar and judiciary.

Background and Other Contextual Factors

63. New Zealand introduced its current AML/CFT regime in 2009 with the *Anti-Money Laundering and Countering the Financing of Terrorism Act 2009* (AML/CFT Act) largely replacing the former *Financial Transaction Reports Act 1996* (FTR Act). The AML/CFT Act originally applied to financial institutions and casinos, with TCSPs added in 2013 (Phase 1 reporting entities). New Zealand then amended the AML/CFT Act in 2018 to apply it to all remaining DNFBPs (law firms, accountants, conveyancers, estate agents and high-value dealers (HVDs)) (Phase 2 reporting entities) in a staggered approach (see Table 1.1). HVDs, which include dealers in precious metals and stones (DPMS), do not have the full range of AML/CFT obligations. The Phase 2 reforms also extended AML/CFT requirements to the Racing Industry Transition Agency (RITA),[2] which provides sports betting services in New Zealand. VASPs are largely captured under the AML/CFT Act as FIs depending on what services they offer.

Table 1.1. Effective dates for FIs and DNFBPs under AML/CFT Act

Effective date	Reporting entities under AML/CFT Act
Phase 1	
30 June 2013	FIs: registered banks; life insurers; non-bank deposit-takers; derivatives issuers; brokers and custodians; equity crowd-funding platforms; financial advisers; managed investment scheme managers; peer to peer lending providers; discretionary investment management services providers; licensed supervisors; issuers of securities; providers of money remittance; currency exchange, payment; non-bank non-deposit taking lending; non-bank credit card; stored value instruments; financial leasing; tax pooling; factoring; payroll remittance; debt collection; cash transport; and safe deposit boxes DNFBPs: casinos and TCSPs
Phase 2	
1 July 2018	DNFBPs: law firms and conveyancers
1 October 2018	DNFBPs: accounting practices
1 January 2019	DNFBPs: real estate agents
1 August 2019	DNFBPs: HVDs and RITA

64. New Zealand is considered to be one of the least corrupt countries in the world. Transparency International found that New Zealand was perceived to be the least corrupt country in the world in 2019.

AML/CFT strategy

65. The Ministry of Justice (MOJ) leads the development of AML/CFT strategy for New Zealand. Since its first NRA in 2010, New Zealand's national AML/CFT strategy was spread across several strategies, initiatives and legislative programmes. In 2020, the Ministry turned this policy framework into a unified overarching strategy with the development of a National AML/CFT Strategy, which responded to the outcomes of the

2 After the onsite, RITA was renamed TAB New Zealand.

2019 NRA. The Ministry also created an implementation and action plan for the National Strategy for the period 2020 to 2022.

66. The National Strategy brings together strategic priorities across areas of national interest including, national security, counter-terrorism, transnational organised crime, organised crime, cyber-crime and corruption. Overall, the National Strategy aims to guide the strategic direction for AML/CFT system and help further co-ordinate actions and guide prioritisation.

67. The National Strategy is considered an evolving process, which will change and adapt as New Zealand's AML/CFT system matures. The National Strategy will also feed into the third generation NRA and statutory reviews expected to take place in 2021 and 2022, which will also consider the results from this mutual evaluation.

68. In parallel with the AML/CFT Strategy, New Zealand adopted a national Counter-Terrorism Strategy in September 2019. This notes the importance of combating TF to reducing the threat of terrorism in New Zealand.

Legal & institutional framework

69. New Zealand supervises and regulates FIs, DNFBPs and VASPs (called 'reporting entities') under the AML/CFT Act and its associated Regulations and ministerial exemptions. Other key measures are set out in the *Reserve Bank of New Zealand Act 1989* (RBNZ Act)*, Financial Markets Conduct Act 2013* (FMC Act) and the *Financial Services Providers (Registration and Dispute Resolution) Act 2008* (FSPR Act). Key criminal justice legislation includes the AML/CFT Act and the *Criminal Proceeds (Recovery) Act 2009.* Measures on transparency of legal persons and arrangements are set out in common law and key acts such as the *Companies Act 1993, Limited Partnerships Act 2008* and *Trusts Act 1956.*[3]

70. The institutional framework for AML/CFT is broad, involving a range of authorities. The **Ministry of Justice** (MOJ) is responsible for the administration of the AML/CFT Act and the development of criminal justice policy and leads the development of New Zealand's AML/CFT strategy. It is supported by:

a. the **Ministry of Business, Innovation and Employment** (MBIE), which is responsible for financial markets and company legislation and policy, and

b. the **Ministry for Foreign Affairs and Trade** (MFAT), which is responsible for New Zealand's foreign and trade policy, co-administers the *Terrorism Suppression Act 2002* (TSA) with the MOJ, and administers the *United Nations Act 1946* (UN Act).

71. The AML/CFT Act establishes a **National Co-ordination Committee** (NCC) to ensure the necessary connections to ensure there is consistent, effective, and efficient operation of the AML/CFT regulatory system. MOJ chairs the committee, which includes representatives from law enforcement, supervisors and central government. The NCC is supported by the Oversight Committee (OC), which provides strategic oversight of the operation and effectiveness of the AML/CFT regime. Membership of the OC comprises senior managers from law enforcement, supervisors and central government.

3 New Zealand has passed new legislation (Trusts Act 2019) to replace the Trusts Act 1956, however the new Act did not commence operation until January 2021.

72. **New Zealand Police** (NZ Police) is the main LEA for investigating ML/TF and most predicate offences. It investigates both serious and organised crime, and low-level offending. While it is a unified police service, it is split into twelve geographical policing districts and has several specialist national groups. Major units within NZ Police include:

a. The **Financial Crime Group** (FCG), which encompasses the NZPFIU, the Asset Recovery Units (ARUs) and a dedicated team focused on criminal ML investigations.

   1) The **FIU** is part of New Zealand Police and is responsible for receiving, analysing and disseminating STRs/SARs, border cash reports, large cash transaction reports and international wire reports. The FIU provides typologies and reporting guidance to reporting entities and is the lead for the NRA. The FIU is also the lead for the Police's public-private partnership with reporting entities, the **Financial Crime Prevention Network** (FCPN), which was formally established in October 2018.

   2) The **ARUs** have responsibility for the restraint and forfeiture of proceeds of crime and property used during the commission of crime. ARUs also assist with the financial aspect of investigations, such as those involving illicit drugs, property and vehicle crime, as well as assisting other law enforcement investigations.

   3) The **Money Laundering Team** (MLT) was established in April 2017 and undertakes complex ML investigations.

b. The **National Organised Crime Group** (NOCG) investigates nationally significant organised crime enterprises with an emphasis on cross-agency response. The NOCG undertakes ML investigations that are associated with organised crime.

c. The **National Security and Counter-Terrorism Group** (NSCTG) is responsible for TF investigations, supported by the specialist capability of the FCG.

d. The **National Intelligence Centre** (NIC) provides national law enforcement intelligence, including on organised crime, ML and TF. Strategic, operational and tactical support is provided by the NIC in collaboration with the NZPFIU and NOCG intelligence.

e. At a district level, the **Criminal Investigation Branch** undertakes criminal investigations of predicate offences and ML. These may be supported by and/or support National Operations.

73. Other LEAs who have responsibilities associated with AML/CFT in New Zealand are:

a. The **New Zealand Customs Service** (Customs) which investigates the importation of drugs and other prohibited goods into New Zealand, and is involved in commercial fraud investigations. Customs also enforces New Zealand's cross-border cash requirements.

b. **Inland Revenue** (IR) investigates and prosecutes for tax evasion and related ML.

c. The **Serious Fraud Office** (SFO) investigates and prosecutes serious or complex fraud. It has the national investigative lead for corruption matters.

d. The **Solicitor-General** is the head of the **Crown Law Office (CLO)**. The CLO commission Crown Solicitors for each District. The Crown Solicitors are then private law firms who prosecute the most serious offences on behalf of the Crown. The Commissioner of Police is also responsible for bringing proceedings for restraint and forfeiture of criminal proceeds and he engages Crown Solicitors to represent him in these proceedings. The CLO is also New Zealand's central authority for MLA.

e. The **Official Assignee** is responsible for the management of criminal and terrorist assets until they are released or disposed of.

f. Additional intelligence collection and analysis is conducted through New Zealand's national security agencies, primarily the **New Zealand Security Intelligence Service** (NZSIS) and the **Government Communications Security Bureau** (GCSB).

74. New Zealand has three **AML/CFT supervisors (RBNZ, FMA and DIA**). Registration and licensing of FIs, DNFBPs and VASPs is undertaken by a range of bodies including RBNZ, FMA, MBIE, **Gambling Commission, New Zealand Law Society (NZLS), New Zealand Society of Conveyancers (NZSC), Chartered Accountants Australia New Zealand (CAANZ)** and the **Real Estate Authority (REA**).

75. The **MBIE** maintains various registries with respect to different legal entities operating in New Zealand. Its Integrity and Enforcement Team undertakes compliance and enforcement functions in relation to entities.

76. The **Charities Services**, which is part of DIA, is responsible for registering and monitoring charities.

Financial sector, DNFBPs and VASPs

77. This section gives general information on the size and make-up of the financial, DNFBP and VASP sectors in New Zealand. Not all of the sectors are of equal importance, given the specific risks and context of the New Zealand system. The level and types of ML/TF risks affecting individual reporting entities vary greatly, as do the ML/TF risks facing particular sectors.

78. The assessors ranked the sectors based on their relative importance in New Zealand's context given their respective materiality and level of ML/TF risks. The assessors used these rankings to inform their conclusions throughout this report, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report but is most evident in Chapter 6 on IO.3 and Chapter 5 on IO.4.

a. The **banking sector** is weighted the most heavily as being the most important sector, based on its materiality and risk in New Zealand. The banking sector plays a predominant role in New Zealand and is, therefore, materially significant. RBNZ's 2017 SRA found the banking sector to have an overall inherent risk rating of high due to its relative size, the large number of customers, high number and value of transactions, ease of access and connection to international financial systems.

79. MVTS, accounting practices, law firms, real estate agents and TCSPs are heavily weighted based on their materiality and risk:

a. **MVTS:** There are 121 non-bank reporting entities providing MVTS services, although there may be more unregistered operators. The volume/value of transactions are dominated by China, Hong Kong, China and India. DIA considered them, in their 2018 SRA to have high ML/TF risk, due to the sector's high-risk services/products combined with ease of access, wide geographic spread, high-risk customers and the ability to move funds overseas.

b. **Accounting practices:** There are 2 779 accounting practices listed as reporting entities in New Zealand. DIA considered them, in their 2019 SRA, to have a medium-high ML/TF risk due to their easy access and wide geographic spread of services, coupled with their gatekeeper role and use in every phase of ML/TF and in many different ML/TF typologies.

c. **Law firms:** Lawyers (solicitors and barristers) in New Zealand provide a full suite of legal services. The reporting entities in the sector comprise 1 397 law firms, 304 sole barristers, and 167 barrister and solicitor firms (1 868 reporting entities in total). Similar to accounting practices, DIA considered them, in their 2019 SRA, to have a medium-high ML/TF risk due to their 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. Law firms may also carry out TCSP services.

d. **Real estate agents:** There are 924 real estate companies with an active licence and 148 agencies operating as sole traders, representing 15 000 licensed real estate agents. DIA considered them, in their 2019 SRA, to have a medium-high ML/TF risk due to real estate being the ML asset of choice and the sector's low levels of AML/CFT awareness and sophistication.

e. **TCSPs:** There are 450 TCSPs registered in New Zealand, which is a well-known centre for TCSP services. The TCSPs provide a number of services including company and trust formation, nominee director, shareholder and trustee services, and virtual office services. DIA considered them in their 2017 SRA to have high ML/TF risk due to the sector's high-risk services/products, combined with ease of access, wide geographic spread, high-risk customers and the ability to disguise and conceal beneficial ownership.

80. Brokers and custodians, currency exchange, derivative issuers, NBDTs, payment providers, casinos, conveyancers, HVDs and VASPs are weighted as being moderately important based on their materiality and risk:

a. **Brokers and custodians of managed investment schemes:** There are 66 brokers and custodians in New Zealand, which have over 450 000 customers and conduct NZD 523 billion in transactions each year. FMA's 2017 SRA found that this sector was medium-high risk because of the liquidity of the products, the anonymity of non-face-to-face onboarding, the high concentration of trust and other legal arrangements, and non-resident customers.

b. **Currency exchange:** DIA identifies 74 non-bank reporting entities as providers of currency exchange service. Some currency exchanges may also offer remittance and lending services which further increases the ML/TF risk presented by the sector. DIA considered them, in their 2019 SRA, to have a medium-high ML/TF risk due to the services and products of this sector, the ease of access, global spread and the ability to process large cash transactions.

c. **Derivatives issuers:** There are 25 derivatives issuers in New Zealand, which have over 52 000 customers and conduct over NZD 15.7 billion in transactions each year. FMA's 2017 SRA, found that this sector was high risk because of the sector's high liquidity, ease of opening accounts, limited face-to-face on-boarding and the large number of non-resident customers in higher risk jurisdictions. Of the 25 issuers, only 10 trade derivatives for speculative purposes and are considered to be exposed to greater ML/TF risk.

d. **NBDTs:** These are entities that make regulated offers of debt securities and who carry on the business of borrowing and lending money or providing financial services, or both. Many NBDTs operate in a similar nature to registered banks by providing a range of financial services including accepting deposits and lending funds. There are 20 registered NBDTs. This includes New Zealand building societies, deposit-taking finance companies, and credit unions. RBNZ, in its 2017 SRA, considered NBDTs to have a medium rating, reflecting the relatively smaller size and complexity compared to the banking sub-sector even though NBDTs have some similar products and services.

e. **Payment providers:** There are 63 payment providers in New Zealand. The sector is broad and includes mobile and internet-based payment systems, digital wallets, electronic money and alternative banking platforms. DIA considered them, in their 2019 SRA, to have a medium-high ML/TF risk due to the services and products of this sector, the ease of access, lack of regulation, global reach, international transfer of funds and the ability to process large numbers of high value transactions.

f. **Casinos:** New Zealand has three casino operators with six casinos. New casino licences are prohibited but existing licenses may be renewed. Online casinos are illegal. DIA's 2019 SRA found the sector to be medium-high risk due to the ease of access to casinos, coupled with high risk services/products and their use in every phase of ML/TF and in many different typologies.

g. **Conveyancers**: Conveyancing is often carried out by lawyers. However, a person may register as a conveyancing practitioner without also practising as a lawyer. DIA supervises 15 such conveyancing practitioners. However, unlike lawyers, DIA's 2019 SRA found them to have a medium overall inherent ML/TF risk due to their more limited exposure to high-risk products/services, and their interaction with generally lower-risk customers and institutions.

h. **HVDs:** New Zealand regulates DPMS as a type of HVD, although some DPMS are exempt. DIA considered HVDs, in their 2017 SRA, to have a medium-high ML/TF risk due to the sector's vulnerabilities to ML/TF and low levels of AML/CFT awareness and sophistication. DIA supervises 93 HVDs. New Zealand estimates approximately 12% of HVDs are DPMS.

i. **VASPs:** New Zealand incorporates most VASPs as FIs under the pre-existing AML/CFT Act. Depending on what service they offer, they may be classified as a money remitter, payment provider or a broker or custodian. DIA's 2019 SRA assigned an overall high ML/TF risk rating to the sector due to vulnerabilities of the sector, including ease of access, anonymity and beneficial ownership issues, exposure to cross-border payments and prior association with organised crime. However, due to their limited materiality in New Zealand's economy, they are given moderate importance. DIA supervises 22 VASPs and FMA supervises one VASP.

81. The insurance sector and other financial institutions are weighted as being of relatively low importance:

a. **Insurance**: There are 87 licensed insurers in New Zealand. The market is concentrated, with the largest insurer accounting for over half of the non-life insurance market. The Government also provides coverage of particular risks (such as earthquakes). In its 2017 SRA, RBNZ considered life insurance to have a low risk rating due to the little evidence of ML, small size and simple products.

b. **Other financial institutions**: Other FIs include a range of businesses supervised by FMA, such as equity crowd funding platforms, financial advisors, managed investment scheme managers, peer-to-peer lending providers, discretionary investment managers, licensed supervisors and issuers of securities. It also includes FIs supervised by DIA, including safe deposit boxes, cash transport, non-bank credit cards, factoring, debt collection, payroll remittance, tax pooling, non-bank non-deposit taking lenders, financial leasing and stored value instruments issuers. FMA and DIA's 2017 and 2019 SRAs found these to have, in general, a medium to low ML/TF risk.

Preventive measures

82. New Zealand's preventive measures are set out in the AML/CFT Act and its associated Regulations. Since the Act came into force in 2009, New Zealand has amended the Act several times. Most notably this includes substantial amendments in 2017 to extend the application of the Act to the full range of DNFBPs, as well as amending the requirements applicable to CDD, STRs, AML/CFT programmes and wire transfers. The preventive measures however do not fully meet the FATF Standards, with notable gaps relating to domestic PEPs, MVTS, wire transfers, financial groups and higher-risk countries. HVDs, such as DPMS, also have limited obligations under the Act.

83. The Act also exempts a number of activities and businesses from the full range of preventive measures through ministerial exemption under the *AML/CFT (Exemptions) Regulations 2011* and *AML/CFT (Definitions) Regulations 2011*. New Zealand has not sufficiently demonstrated that all of these exemptions were undertaken on the basis of demonstrated low risk (see IO.1).

Legal persons and arrangements

84. New Zealand recognises a wide range of legal persons and arrangements, with limited liability companies, limited partnerships and trusts considered to be the structures most likely to be abused for ML/TF purposes.

85. Legal persons include companies, partnerships, incorporated charitable trusts, incorporated societies, building societies, credit unions and industrial and provident societies. Companies may be limited liability, co-operative or unlimited liability and are incorporated under the *Companies Act 1993*. Partnerships are most common in certain professions such as law, accounting and farming and are usually established with a partnership agreement. Limited Partnerships are formed under the *Limited Partnership Act 2008*. Membership based organisations, known collectively as 'mutuals', include incorporated societies, credit unions, building societies, friendly societies and industrial and provident societies.

Table 1.2. Types of legal persons in New Zealand

Legal person	Number (at March 2020)	Description
Building societies	9	A building society is a society of at least 20 members that provides member services. Generally, building societies raise funds by the issue of shares to members, who usually pay for them by subscription over time.
Credit unions	10	A credit union is a member-owned co-operative financial organisation that has been set up to provide its members with savings and loan facilities. A credit union cannot carry on business without being incorporated.
Friendly societies	109	A friendly society is an organisation established to provide for, by voluntary subscriptions of the members, with or without donations, the relief or maintenance of members and their families during poor health, old age or widowhood. Registration as a friendly society does not confer incorporation status. However, both corporate and unincorporated bodies can apply for registration.
Incorporated society	23 835	An incorporated society is a society of at least 15 members, formed for any lawful purpose other than pecuniary gain, which has been registered (and incorporated).
Industrial and provident societies	81	An industrial and provident society is a society of at least seven members formed in relation to the carrying on of any industry, business, or trade (except banking).
Incorporated charitable trusts	26 117	The trustees of charitable trusts, and charitable unincorporated associations, can choose to incorporate as a charitable trust board. A New Zealand charitable trust board has legal personality and its members have limited liability.
Limited partnerships	2 818	Limited partnerships are a form of partnership involving general partners, who are liable for all the debts and liabilities of the partnership, and limited partners, who are liable to the extent of their capital contribution to the partnership.
Limited liability companies	649 217	A limited liability company is a company of at least one or more director, one or more shareholder, and has one or more shares. Shareholders have limited liability for the obligations of the company.
Co-operative companies	128	Co-operative companies are limited liability companies that are owned and controlled by their members. The principal activity of co-operative companies is, and is stated in its constitution as being, a co-operative activity and in which not less than 60% of the voting rights are held by transacting shareholders.
Unlimited liability companies	385	Unlimited liability companies are companies where shareholders have ultimate liability for the debts of the company, meaning they must pay any debts that the company cannot pay. This liability is included in the company's constitution. Unlimited companies are used to meet very particular, often foreign, legal requirements.
Totals	699 891	

86. Trusts are very common in New Zealand. They are used for a range of purposes in particular as holding vehicles for family assets (such as the family home). Trusts are governed by the common law and particular statutory provisions including those in the *Trustee Act 1956*.[4] Trusts that have exclusively charitable purposes are known as charitable trusts and these may choose to register with Charities Services. Charitable trusts may also choose to incorporate as a charitable trust board, which has a legal personality. There are 26 117 incorporated charitable trusts in addition to the 25 709 charitable trusts registered with the Charities Register. The Māori Land Court also has the jurisdiction to constitute trusts over Māori land and general land owned by Māori. Since most trusts are not required to register, it is not known how many trusts there are in New Zealand. New Zealand estimates there are between 300 000 to 500 000.

87. New Zealand Foreign Trusts are trusts that are established by a non-resident settlor but have a trustee resident in New Zealand. These are considered particularly vulnerable to ML/TF and tax evasion. To mitigate these risks, New Zealand introduced new requirements in 2016 for New Zealand Foreign Trusts to register with the IR and

4 The *Trustee Act 1956* has been replaced by the *Trusts Act 2019*. This Act was not in force however at the time of the onsite.

provide certain information. At March 2020, there were 2 807 New Zealand Foreign Trusts registered. This represents a 75% decline over the preceding three years.

Table 1.3. Types of legal arrangements in New Zealand

Legal person	Number (at March 2020)
Express trusts (including family trusts)	300 000 – 500 000
Charitable trusts registered with Charities Services	25 709
Māori Land Trusts	20 795
New Zealand Foreign Trusts	2 807

Supervisory arrangements

88. There are three AML/CFT supervisors in New Zealand, supervising all reporting entities. The basic powers and responsibilities of these supervisors are set out in the AML/CFT Act:

a. **RBNZ** is New Zealand's central bank and is responsible for prudential regulation of financial institutions. The RBNZ is the AML/CFT supervisor for banks, life insurers and non-bank deposit takers.

b. **FMA** is responsible for conduct regulation of financial institutions. The FMA is the AML/CFT supervisor for issuers of securities, licensed supervisors, derivatives issuers, managed investment scheme managers, brokers and custodians, certain financial advisers, equity crowdfunding platforms, peer-to-peer lending providers, discretionary managed investment service providers and a small number of VASPs.

c. **DIA** is a government department responsible for AML/CFT supervision of some financial institutions, including non-deposit taking lenders, money changers, MVTS, payroll remitters, debt collectors, factors, financial lessors, safe deposit box vaults, non-bank credit card providers, stored value card providers, cash transporters and most VASPs. The DIA is also the AML/CFT supervisor for all DNFBPs and RITA.

89. Registration and licensing of reporting entities is not required under the AML/CFT Act. Instead, it is undertaken through other legislation by a range of bodies including, RBNZ, the FMA, Gambling Commission, MBIE, NZLS, NZSC, CAANZ and REA. Some DNFBPs do not have registration or licensing obligations (e.g. TCSPs and HVDs).

Table 1.4. New Zealand supervisors and their supervisory population

Supervisor	Supervisory population
RBNZ	27 registered banks 20 NBDTs 8 life insurers
FMA	16 Derivative Issuers 66 Brokers/custodians 386 Financial advisers 139 Managed Investment Schemes 6 Equity Crowd Funding 7 Peer-to-Peer 53 DIMS 18 Issuers 6 Supervisors 1 VASP 66 Other [5]
DIA	DIA supervises 10 353 reporting entities, with the following breakdown. DIA supervises the following FIs: 121 remittance providers 74 foreign exchange providers (including in-hotel) 76 non-bank non-deposit taking lenders 63 payment providers 12 NBDTs 6 non-bank credit card providers 4 stored value card providers 195 other FIs (debt collection, factoring, financial leasing, foreign exchange, payroll, safe deposits, tax pooling, cash transport) 63 payment providers DIA supervises the following DNFBPs: 2 779 accounting practices 1 397 law firms 924 real estate agency firms 450 TCSPs 304 sole barristers 167 barrister and solicitor firms 93 HVDs 55 bookkeepers 15 conveyancing firms 3 casino operators 2 auction houses RITA DIA supervises 22 VASPs. DIA also supervises 422 firms listed as 'other'.

90. **MBIE** maintains various registers with respect to different legal entities operating in New Zealand. In addition, most financial institutions must be registered on the Financial Services Providers Register (FSPR). MBIE maintains the FSPR and carries out the registration process. At March 2020, 14 080 financial services providers were registered on the FSPR.

International co-operation

91. Due to its open economy, New Zealand is exposed to transnational ML/TF risks. While not a major financial centre, it is an important regional remittance centre for the South Pacific, where New Zealand has strong economic and cultural ties. New Zealand

5 REs associated with parent companies and are part of a Designated Business Group

co-operates with many jurisdictions, particularly Australia, which is its major partner for law enforcement and supervisory co-operation.

92. The Attorney-General is designated by the *Mutual Assistance in Criminal Matters Act 1992* (MACMA) as the central authority for MLA in New Zealand and the Attorney-General's powers under MACMA are largely delegated to the Solicitor-General. The Office of the Solicitor-General, i.e. the CLO, undertakes the legal work required for transmission and execution of MLA requests.

93. New Zealand's extradition procedures are laid out in the *Extradition Act 1999*, which governs the extradition of persons to and from New Zealand. The Extradition Act does not designate any central authority. MFAT is generally the contact point for all extradition inquiries, except for extradition requests from Australia and the United Kingdom which follow the "backed-warrant" procedure. Under the standard procedures, extradition requests arising through diplomatic channels are directed to the Minister of Justice and dealt with by the CLO. Backed-warrant extradition requests are handled by New Zealand Police.

94. New Zealand also engages actively in all areas of informal international co-operation. Competent authorities regularly seek forms of international co-operation. Competent authorities also participate actively in various international AML/CFT fora and networks.

Chapter 2. NATIONAL AML/CFT POLICIES AND CO-ORDINATION

Key Findings and Recommended Actions

Key findings

a) New Zealand has a robust understanding of its ML/TF risks and has established a comprehensive multi-tiered risk assessment process through their NRA and SRAs. The NRA is comprehensive and systematic in its identification of New Zealand's ML/TF risks and has been refined over successive updates. Nonetheless, there is scope for some minor improvements, including making the results of the sectoral risk rankings in the SRAs more comparable at a national level. New Zealand authorities share a sound understanding of their risks, with the results of the NRA and SRAs communicated to all stakeholders in a systemic manner.

b) National AML/CFT policies and activities address identified ML/TF risks to a large extent. New Zealand has introduced measures to address a number of identified risks. Authorities have taken action to respond to emerging TF risks in the context of a lower overall risk profile, including in response to New Zealand's limited exposure to the foreign terrorist fighter phenomenon and in the aftermath of the 2019 Christchurch terrorist attacks. However, there is scope for increased focus on ensuring a shared understanding across all relevant agencies of the TF elements of New Zealand's CT efforts. The objectives and activities of the supervisors and LEAs to prevent, detect and respond to ML/TF are informed by the risk assessments.

c) Domestic co-ordination and co-operation are strengths of New Zealand's AML/CFT system. Competent authorities have a strong tradition of co-ordination and collaboration, and continually work to improve the flow of information between authorities. New Zealand re-established the Counter-Proliferation Forum in 2019 as a mechanism for policy co-ordination and development on counter-proliferation issues. It has considered proliferation financing risk at a high level as part of broader proliferation risk.

d) New Zealand has granted a large number of exemptions and allows for simplified measures in specific, justified circumstances. It is not clear that all the exemptions granted were in cases of proven low ML/TF risks in strictly limited and justified circumstances (certain limited and historical exemptions in relation to certain special remittance facilities, providers of some family trusts

and pawnbrokers). In line with its risk understanding, New Zealand also requires enhanced measures in certain circumstances.

e) Authorities have conducted considerable outreach to ensure that the private sector is aware of New Zealand's ML/TF risks.

Recommended Actions

a) New Zealand should continue its efforts to ensure its national policies and activities address the ML/TF risks posed by beneficial ownership of legal persons and arrangements (see IO.5) and unregistered MVTS providers (see IO.4). New Zealand should update its National Strategy in response to the third NRA and its forthcoming statutory review of the AML/CFT Act and improve its maintenance of relevant national statistics to enable it to better understand the effectiveness of its AML/CFT regime.

b) New Zealand should continue its work to understand its ML/TF risks, including new and emerging risks, by completing its planned third NRA. The third NRA should allow for the direct comparison between the different SRAs to give a clearer national picture of sectoral risk.

c) Authorities should continue to work through the CTCC, the NCC and other co-ordination mechanisms to ensure that New Zealand's TF policy continues to respond to new and emerging TF threats. This could be enhanced by work to foster a shared understanding among all relevant agencies of the TF elements of New Zealand's broader CT efforts. The CTCC should include input from supervisors as appropriate.

d) The Counter-Proliferation Forum should progress work on co-ordination and development of policies to counter proliferation financing (within the context of broader counter-proliferation efforts), including supporting New Zealand's counter-proliferation financing risk assessment.

e) New Zealand should review its exemption regime, particularly historical and transitional exemptions granted when the AML/CFT Act was introduced, to ensure that the exemptions take place strictly on the basis of proven low risk of ML/TF.

95. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34, and elements of R.15.

96. The assessment team's findings on IO.1 are based on its review of key documents, such as the NRAs, SRAs and other risk and threat assessments; and key policy documents such as the National AML/CFT Strategy. The team reviewed the

decision notices for all of the ministerial exemptions and the supporting documents for a selection of regulatory exemptions. The assessment team also met with New Zealand government authorities, LEAs, the AML/CFT supervisors and select reporting entities.

Immediate Outcome 1 (Risk, Policy and Co-ordination)

Country's understanding of its ML/TF risks

97. New Zealand has a robust understanding of its ML/TF risks. It has a three-tiered risk assessment system to identify and assess its ML/TF risks, comprising the NRA, the SRAs and reporting entities' risk assessments. The NRA assesses risk as a function of threats, vulnerabilities and consequences and describes the scale and nature of the ML/TF risks faced by New Zealand at the national level. The development of the NRA is led by the NZPFIU and co-ordinated by the working groups of the NCC. Relevant government agencies and certain reporting entities contribute to this process. At the second tier, the supervisors (RBNZ, FMA and DIA) produce more specific assessments of the risks faced by the sector they each supervise (SRAs). The SRAs are informed by the findings of the NRA. At the bottom tier, reporting entities are required by the AML/CFT Act to produce their own risk assessments.

98. Both the NRA and the SRAs have been through two full iterations, with amendments and updates in response to significant events or developments. The two iterations of the NRA were conducted in 2010 and 2013-15 with updates made to the second NRA in 2016, 2017 and 2019. A public version of the NRA was published in 2018 and updated in 2019. The AML/CFT supervisors first published SRAs in 2011. During 2017-2018, each of the supervisors published new SRAs for their supervised sectors. DIA also published a further SRA for the newly captured Phase 2 sectors in 2017. In this respect, there are a total of four current SRAs across the three supervisors.

99. The methodology of the NRA is sound, producing a multi-dimensional assessment of domestic and international threats, vulnerabilities and the potential impact of these on the objectives of the AML/CFT Act. The NRA methodology has been enhanced since the first iteration of the NRA in 2010. In 2010, the NRA process commenced with a very small group of agencies using the Delphi Survey methodology. In the later iterations, the NRA used a wider threat and vulnerability analysis based on FATF guidance. The SRAs have been based predominantly on surveys and other information from select reporting entities. These assessments were developed using a modified version of the joint model developed by the World Bank and APG and considered structural risk areas. New Zealand's SRAs are shifting from a purely inherent risk rating model for assessing individual reporting entities to a more residual risk or overall ML/TF risk rating. The risk ratings between the supervisors' SRAs are not directly comparable. This inhibits a clear understanding of which sectors are high, medium and low risk at a national level.

100. The NRA uses quantitative and qualitative data from a range of public and non-public sources to identify and analyse the major domestic and international ML/TF risks. The NRA process uses case studies, international studies, intelligence, and information from the NZPFIU, LEAs and the supervisors and input from reporting entities to identify major domestic and international ML/TF risks.

101. New Zealand's identification of ML risks in the NRA is comprehensive and reasonable in New Zealand's context. Broadly speaking, New Zealand is perceived as a safe jurisdiction, with a reputation for integrity and stability and with comparatively low risks from crime and terrorism. Domestic proceeds of crime arise mostly from drug

offending and fraud, as well as tax evasion. New Zealand is also exposed to ML threats from transnational organised crime, particularly from South East and East Asia, Australia, North America and Eastern Europe. Australian-based organised crime and tax evasion also pose a significant threat, with offenders known to conduct illicit transactions in New Zealand and/or use New Zealand as a conduit to layer illicit proceeds.

102. The NRA provides comprehensive analysis on the risk of abuse of its vulnerabilities and assesses the resulting impact. New Zealand's sectoral risks are concentrated in banks, with the MVTS sector (especially alternative remittance) and gatekeeper professionals remaining of particular concern. New Zealand's identified vulnerabilities also include the real estate sector, international wire transfers, businesses dealing in high-value goods, casinos and new payment technologies.

103. The NRA considers that the international and domestic TF threat from lone actors, small cells, terrorist networks, Islamist and right-wing extremism. The national terrorism threat was raised following the 15 March 2019 Christchurch attacks and was assessed as 'medium' at the time of the onsite (see IO.9). Authorities cited the increased likelihood of terrorist attacks by copy-cats or in retaliation to the Christchurch attacks as the reason for the change in rating. Within the context of an overall lower TF risk, New Zealand has assessed that its domestic risks relate primarily to lone actors for which self-funding is assessed as the likeliest means of finance. International risks include the risk of radicalised individuals in New Zealand providing support to overseas groups and the risk of traditional laundering by established networks through New Zealand's financial system and legal structures.

104. New Zealand demonstrated a good understanding of the risk of TF associated with foreign terrorist fighters. A small number of people with New Zealand passports and with limited ongoing connections to New Zealand were known to have travelled to conflict zones. Officials demonstrated to the assessment teams that the associated TF risks were well understood, including through New Zealand's active participation in a number of international forums focused responding to global threats associated with foreign terrorist fighters and the emergence of ISIL, and the publication of indicators related to ISIL financing for reporting entities. Since the Christchurch attacks, which led to the largest criminal investigation in the country's history, authorities have also devoted resources to increasing understanding and monitoring of ethnically or racially motivated terrorism.

105. Ultimately, through the various iterations of its NRA and SRAs, New Zealand's authorities have a sound and detailed understanding of its ML/TF risks and are able to respond appropriately. This national approach will be maintained into the next generation of the NRA and SRAs, provided that New Zealand continues the same level of commitment towards understanding its ML/TF risks.

National policies to address identified ML/TF risks

106. New Zealand's national AML/CFT policies and activities address identified ML/TF risks to a large extent. New Zealand has introduced measures to address a number of identified risks, but some risks (e.g. in relation to beneficial ownership and unregistered MVTS providers) remain insufficiently addressed by New Zealand's policies or activities.

107. The MOJ leads the development of national AML/CFT policy, which is co-ordinated across all agencies through the NCC and its supporting Oversight Committee. Policy leads for related policy settings, such as MBIE for Companies Law, MFAT for TFS,

and IR for tax policy, co-ordinate efforts with AML/CFT through the NCC. The Ministry develops and updates policy in response to the findings of each iteration of the NRA and other major events. This seems a generally effective process, with all relevant agencies involved.

108. Following the first NRA in 2010, New Zealand's national AML/CFT strategy was spread across several strategies, initiatives and legislative programmes that flowed from the NRA process. The 2010 NRA noted the need to further develop the NRA and conduct SRAs, build the profile of AML/CFT in the context of organised crime and the forthcoming Phase 2 reforms. Following this, the supervisors conducted their first set of SRAs in 2011. The MOJ also led the development of an All of Government Response to Organised Crime in 2011. This recommended that New Zealand extend its AML/CFT regime to all DNFBP sectors in its Phase 2 reforms, improve information sharing, review New Zealand's ML offence, and establish a reporting regime to track and trace funds transfers. The AML/CFT Act also became fully operational for Phase 1 entities (FIs and casinos) in 2013. TCSPs were also included in scope of the regime to address the particular ML/TF risks relating to company formation arising from the SP Trading case (see IO.11).

109. New Zealand's 2015 NRA re-iterated these priorities and led to a range of legislative, policy and resourcing reforms to target the identified risks in the NRA. This included the extension of New Zealand's AML/CFT regime to cover all DNFBP sectors (the Phase 2 reforms), ensuring LEAs have access to tax information to target ML and the implementation of the prescribed transaction reports (PTRs) regime. Amendments were also made to the ML offence and several policing initiatives were implemented (e.g., funding was secured for dedicated ML investigation teams and ML training was expanded). New Zealand also developed an enhanced regulatory regime for New Zealand Foreign Trusts.

110. Following the 2019 update to the NRA, New Zealand developed an over-arching AML/CFT National Strategy to help set the strategic direction for the AML/CFT regime. Led by the MOJ, it includes four priorities to better understand New Zealand's AML/CFT regime, working together to combat ML/TF, preventing ML/TF and responding to ML/TF. It includes an action plan with a series of actions to be completed between 2020 and 2021. This includes conducting the third full NRA in 2021 and undertaking other risk assessments, undertaking a statutory review of the AML/CFT Act by 2022, expanding guidance on SARs for TF and improving the cross-border cash reporting regime. The improved collection and maintenance of relevant national AML/CFT statistics would assist New Zealand in understanding the effectiveness of its AML/CFT regime and the impact of its policies on its ML/TF risks.

111. In parallel with the AML/CFT Strategy, in September 2019, New Zealand adopted a national Counter-Terrorism Strategy, which notes the contribution of combating TF to reducing the threat of terrorism in New Zealand. The CT Strategy includes a work programme focused on 'reduction', 'readiness', 'response' and 'recovery'. TF is included as an element of 'reduction'. There were no specific action items on TF associated with the Counter-Terrorism Strategy at the time of the on-site visit and only one TF action item in the National Strategy. New Zealand authorities explained that this represented a point in time and followed on from earlier action taken in response to priorities identified through the 2015 NRA, including better information sharing between law enforcement and security agencies on TF risk, as well as the responses to the emergence of ISIL and the foreign terrorist fighter phenomenon outlined above. Further action items on TF may be identified as the result of the Royal

Commission of Inquiry into the Terrorist Attack on Christchurch Mosques and a New Zealand Government Review of the TS Act. Governance arrangements are in place to ensure that future priorities are implemented (see National Co-ordination and Co-operation below).

112. The above policy process has addressed some of New Zealand's identified ML/TF risks. For example, the NRAs recognise the risk that cash deposits and cash-intensive businesses pose. In response, New Zealand has gone further than the FATF Standard and extended AML/CFT regulation to all HVDs[6] and introduced a significant cash reporting regime (the PTR regime). The PTR regime also extends to the reporting of international transfers, which will improve visibility of international wire transfers. While this regime is still in the process of becoming operational, it demonstrates how New Zealand's national AML/CFT policies are addressing identified ML/TF risks. New Zealand also demonstrated its ability to respond to new and emerging risks, such as through its incorporation of most VASPs into its AML/CFT regime.

113. New Zealand's policies and activities address the identified ML/TF risks, but there are gaps in the implementation and some work remains ongoing. On beneficial ownership risks, New Zealand has taken actions, particularly through accelerating inclusion of TCSPs in the AML/CFT regime, creation of a register of New Zealand Foreign Trusts, the creation of a dedicated Integrity and Enforcement Team responsible for ensuring the integrity of corporate registries, and amendments to the Companies Act in 2014 to require that companies have a resident director (although these residency requirements can be avoided through nominee arrangements (see IO5)). New Zealand also undertook a consultation on beneficial ownership reforms in relation to companies and partnerships in 2018, although no decision has yet been made on whether reforms would be pursued. As such, these reforms are incomplete, and in the absence of a policy decision, corresponding actions have yet to be included in the AML/CFT National Strategy action plan. In relation to domestic legal arrangements, New Zealand has introduced policy measures, including LEA access to tax information, mandating enhanced due diligence (EDD) for trusts and reforms of the Trust Act.[7] However, New Zealand is yet to conduct a policy process focused specifically on addressing gaps in access to BO of trusts information (see IO5). New Zealand has also identified the MVTS sector as a major risk, particularly alternative remittance providers. While the DIA and New Zealand Police have taken enforcement action against MVTS providers for breaching their compliance obligations, there is insufficient activity by the relevant administrative authorities to identify unregistered MVTS providers in New Zealand and a lack of clarity as to which agency(ies) are responsible (see R.14). Authorities should enhance their national strategy to take a joined-up approach to these important risks.

114. The resources of LEAs and supervisory bodies are largely aligned to the risk areas identified in the NRA. New Zealand Police, including the NZPFIU, and other authorities have seen an increase in specialised resourcing for ML/TF investigations and prosecutions. New Zealand demonstrated that resources are allocated in accordance with these risks. For example, in recent years New Zealand has created new ML investigative teams and developed an integrity and enforcement team within MBIE

6 HVDs do not have however the full suite of AML/CFT obligations that other reporting entities have (see IO4).

7 In 2019, New Zealand introduced new legislation regarding trusts (*Trusts Act 2019*), however the new Act did not commence operation until January 2021 (see R.25).

to ensure the integrity of its corporate registers. The supervisors also adopted a risk-based approach in their supervisory frameworks.

Exemptions, enhanced and simplified measures

115. New Zealand allows for regulatory and ministerial exemptions to modify the requirements of the AML/CFT Act in certain circumstances. Under the regulatory exemption, classes of reporting entities can be exempted from all or some of their AML/CFT obligations. Under the ministerial exemption, individual reporting entities can be exempted from all, or some, obligations. The exemptions process is managed by the MOJ who consults with the supervisors and the NZPFIU. At March 2020, the Minister for Justice had granted approximately 120 individual exemptions and one class exemption covering 12 classes of reporting entities. These exemptions expire after five years. For the regulatory exemptions, the AML/CFT (Exemptions) Regulation 2011 provides exemptions for seven classes of transactions and 14 classes of services. The AML/CFT (Definitions) Regulations 2011 exempts 11 types of businesses from the definition of reporting entity. There is not a defined time period in which these exemptions are reviewed, but New Zealand has a programme of review underway.

116. Exemptions are granted or declined after taking into account multiple factors. ML/TF risk is a primary criterion with other factors also taken into consideration (for example regulatory burden). While the MOJ conducts a comprehensive assessment to demonstrate the basis for the exemption and considers the risk of ML/TF, there is not an explicit requirement that there be proven low risk of ML/TF before granting an exemption. While proven low ML/TF risk appears to be present in most exemptions, this was not demonstrated in all exemptions granted, particularly in relation to limited and historical exemptions granted at the time the AML/CFT Act was introduced in 2011 (exemptions in relation to certain special remittance facilities, providers of some family trusts and pawnbrokers). While these exemptions practically have limited impact, New Zealand should review its exemption regime, particularly historical and transitional exemptions granted when the AML/CFT Act was introduced, to ensure that exemptions take place strictly on the basis of proven low risk of ML/TF.

117. Simplified measures have also been permitted for certain sectors/entities. For example, simplified CDD is allowed for a range of lower risk customers, such as government owned businesses and publicly listed companies. These are consistent with the findings and conclusions of New Zealand's risk assessments.

118. There are certain circumstances outlined in the AML/CFT Act where EDD is required. These were included in the AML/CFT Act based on the risk assessments conducted in the 2009 legislative process. Specifically, these relate to circumstances where a customer is a trust, or similar arrangement, a person is from a higher risk jurisdiction, a company with nominee shareholders or bearer shares or a PEP (foreign only). While recognising the overall risks, some reporting entities considered that the requirement to conduct EDD on all trusts was disproportionate particularly in light of how common trusts are in New Zealand. New Zealand authorities may wish to consider whether there is a more nuanced approach to mitigating the risks posed by trusts (see IO.5). EDD measures also apply to certain transactions such as wire transfers, those involving emerging technology that favours anonymity and transactions which are complex, unusually large or have an unusual pattern.

Objectives and activities of competent authorities

119. LEAs take a preventative approach to serious crime, which is applied to the systemic risks identified within the NRA. LEAs' approach to the recovery of proceeds

of crime, the investigation and prosecution of ML/TF and predicate offending aim to maximise preventative outcomes. All LEAs demonstrated sound understanding of risk, consistent with the NRA and were aware of both evolving risks and new and emerging threats.

120. In particular, New Zealand has embraced a robust policy in respect of asset confiscation. New Zealand Police in its 'Our Business' strategy of 2018, has a target of restraining NZD 500 million in criminal proceeds by 2021. The pursuit and confiscation of criminal assets is an integral part of New Zealand's response to ML activity and forms part of the Police's strategic objectives. The ARU is an effective and well-resourced function of the Police with specialist investigators, analysts and accountants. The ARU has achieved impressive results in line with its ambitious objective, with approximately NZD 440 million of assets restrained between 2015 and 2020.

121. In comparison, New Zealand has historically not sufficiently prioritised ML investigations and prosecutions in line with its identified risks. New Zealand has however taken actions to ensure that LEAs place greater focus placed on ML. In particular, in 2018 the New Zealand Police set ML investigations that resulted in prosecution as one of its performance measures. Since 2018, New Zealand has seen an increase in the number of ML investigations and prosecutions (see IO.7). Accordingly, New Zealand's LEAs demonstrated the key role which ML investigations play in their strategy and policy objective to disrupt criminal activity through the pursuit of criminal assets.

122. Supervisors' objectives and activities are broadly consistent with national AML/CFT policies and identified risks. The risk-based approach is one of the guiding principles set out in the supervisor's joint supervisory framework. Supervisors use the NRA and their respective SRAs to inform their understanding of risk. All of the supervisors' activities to mitigate the ML/TF risk are aligned to that of the NRA and supervisors generally apply more focus and resources to the areas of highest risk.

123. TF is appropriately investigated given New Zealand's lower risk profile. In particular, the New Zealand Police have standard operating procedures for investigation of TF, including reaching out to other agencies as appropriate. These procedures were used effectively during the investigation of the Christchurch terrorist attacks. Other competent authorities' activities are guided by broader CT efforts directed at reducing the drivers for TF.

National co-ordination and co-operation

124. Domestic co-ordination and co-operation are strengths of New Zealand's AML/CFT system. Competent authorities have a strong tradition of co-ordination and collaboration, and continually work to improve the flow of information between them. Authorities use a variety of mechanisms and fora to share information, co-ordinate efforts, and collaborate with partner agencies and the private sector.

125. The NCC, established by the AML/CFT Act, is the central mechanism for co-ordinating AML/CFT policy and activity. The NCC consists of a representative of the MOJ, Customs, the supervisors, the Commissioner of Police and other invited agencies, including the IR, SFO, MBIE and MFAT. The NCC works closely with the Organised Crime Senior Manager's Forum, the CTCC and Sector Supervisors' Forum.

126. New Zealand has an established and comprehensive counter-terrorism governance framework. It takes a collaborative all-of-Government approach to identifying and managing its national security threats, including terrorism and violent

extremism. It has a whole-of-government National Security System (NSS), to identify, govern, and respond to identified national security risks. On the response side, the NSS comprises relevant ministers, agency chief executives comprising the Officials' Committee for Domestic and External Co-ordination (ODESC), and officials-level committees and working groups. The Combined Threat Assessment Group (CTAG) provides the assessments of the threat level when the NSS is activated in response to a terrorist threat. The CTAG currently consists of seven agencies, including the NZSIS, the GCSB, and Police. On the governance side, the CTCC is the primary forum for overseeing co-ordination of TF policy within the context of broader CT policy. The CTCC is chaired by the Department of Prime Minister and Cabinet and includes the Government Communications Security Bureau, MBIE, the Ministry of Defence, MFAT, Customs, NZ Defence Force, NZ Police and the NZ Security Intelligence Service. The CTCC, in turn, reports to the senior executive-level Security & Intelligence Board.

127. New Zealand has demonstrated that the operational co-operation and co-ordination by authorities on CFT is strong, flexible, and responsive to cases that emerge, and it has worked, including through informal co-ordination within New Zealand's highly inter-connected public sector. However, while individual agencies were effective in responding to TF risks they identify, the assessment team considered that, based on discussions during the on-site visit, not all agencies were clear about the TF elements of New Zealand's broader CT efforts. Further work could be done to foster a common understanding across all relevant agencies, particularly in relation to new and emerging risks.

128. All agencies working on counter-proliferation issues, including proliferation finance, are represented on a working level forum, the Counter-Proliferation Forum, under ODESC which facilitates information sharing and co-ordination. MOJ and the NZPFIU are members of the NCC participate in the Counter-Proliferation Forum. However, as the Forum was only re-established in 2019, counter-proliferation co-operation is at a nascent stage. In 2019, the Forum assessed New Zealand's overall proliferation risk as low, and this assessment included input from relevant agencies on proliferation financing risks. A separate risk assessment focused on proliferation financing is planned but has not yet been discussed in the Forum.

129. For the supervisors, co-ordination takes place through the joint supervisory framework, which establishes shared supervisory objectives and principles. The supervisors hold a fortnightly forum, which considers a variety of issues such as operational policy and emerging risks, consistency issues raised by reporting entities and development of AML/CFT guidance. The forum also co-ordinates supervisors' relationships with other parts of government and international partners, joint supervision, joint on-site inspections, training, outreach and technical assistance. DIA, RBNZ, FMA, the NZPFIU, Police and MOJ attend the forum.

130. Law enforcement co-operation occurs primarily through the free flow of information between agencies. The *Privacy Act 1993* and related legislation enables lawful information sharing and access for ML/TF and associated predicate offences. The assessment team observed that that there is a very high degree of formal and informal co-operation among the LEAs. This permissive environment has enabled LEA to co-operate effectively against high risk criminal targets.

Private sector's awareness of risks

131. New Zealand authorities have undertaken substantial outreach to ensure that reporting entities are aware of the results of the NRA and SRAs. The NZPFIU engaged

private sector entities in the NRA process through the FCPN, industry groups and representative bodies. For the SRAs, the supervisors used information sourced from reporting entities (e.g. annual report data, reporting entities' risk assessments and AML/CFT programmes and onsite inspections). DIA and FMA also engaged directly with the private sector in the development of their SRAs, whereas RBNZ did not.

132. The results of the NRA and SRAs are made available to reporting entities. The SRAs are available on the respective supervisor's webpage, along with other guidance. The NZPFIU uses its secure message board system to advise registered reporting entities of updates and changes to any risk assessments. The NZPFIU published a public version of the NRA on its website in 2018, which was updated in 2019. Most reporting entities met with by the team demonstrated familiarity with the NRA and their relevant SRA.

133. New Zealand authorities have also conducted considerable outreach to ensure that the private sector is aware of ML/TF risks and receive training on ML/TF risk management. Sector supervisors and the NZPFIU also conduct frequent outreach and training on ML/TF risk and compliance. For example, the NZPFIU in partnership with ACAMS conducts annual FIU/ACAMS.

134. The FCPN is also an effective co-operation and co-ordination mechanism between the public and private sector and is a feature of New Zealand's ongoing ML/TF risk assessment process. The FCPN consists of the NZPFIU, five major banks in New Zealand, Customs and RBNZ.

Overall Conclusions on IO.1

135. New Zealand has a robust understanding of its ML/TF risks and has established a comprehensive and updated multi-tiered risk assessment process. The methodology of the NRA and the SRAs is sound, with scope for some minor improvements.

136. New Zealand's national AML/CFT policies and activities largely address the identified ML/TF risks, however some remain insufficiently addressed. Authorities demonstrated a good understanding of the TF risks faced by New Zealand and an established framework is in place to ensure appropriate oversight of implementation of policies to address new and emerging risks.

137. All relevant New Zealand authorities share a sound understanding of their risks, and the risk assessments inform their policies, objectives, and activities. The results of the NRA are communicated to all the stakeholders in a systemic manner. Co-ordination, collaboration and information sharing among competent authorities is a strength of New Zealand's AML/CFT system. New Zealand should however ensure that its historical and transitional exemptions have been granted strictly based on proven low risk of ML/TF.

New Zealand has achieved a substantial level of effectiveness for IO.1.

Chapter 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

a) LEAs routinely conduct parallel financial investigations and financial intelligence is regularly used to support investigations, trace assets, enforce forfeiture orders and identify risks. LEAs obtain financial information from the FIU, via direct access to the goAML database and through requests to financial institutions and DNFBPs.

b) The FIU is well situated to understand law enforcement priorities and strategic objectives, and its collaborative relationships with LEAs is a key strength. The FIU produces and disseminates a wide range of financial intelligence products which generally support the operational needs of competent authorities. A high volume of raw financial intelligence is shared with LEAs in support of their ongoing criminal investigations and to refine the FIU's prioritisation of targets for deeper analysis based on feedback from LEAs.

c) The FIU does not fully exploit the potential of financial intelligence to detect criminal activity by persons not already known to law enforcement, and this is reflected in the relatively smaller number of investigations initiated on the basis of FIU reports alone. However, this also reflects the FIU's approach to prioritisation and targeting, which relies on feedback from LEAs, in response to strategic intelligence and raw financial intelligence, to refine the FIU's priorities for deeper analysis.

d) Most SARs and PTRs are received from banks and remitters, with a limited number from DNFBPs and TCSPs. At the time of the on-site visit, about 2 700 reporting entities (mostly DNFBPs) had yet to register with the STR reporting system, however taking into account the materiality of this sector and mitigating measures, this shortcoming does not have a significant impact on the FIU's access to financial intelligence. In relation to criminal activity, the financial intelligence that the FIU receives is generally in line with New Zealand's risk profile.

e) The FIU does not collect specific comprehensive statistics on the use of disseminated financial intelligence products by LEAs in

criminal investigations and asset recovery cases. Nevertheless, numerous cases were provided demonstrating successful investigations and asset recovery supported by the FIU's products.

f) New Zealand authorities participate in various multi-agency groups to co-operate and exchange information and financial intelligence. This includes a public-private partnership with Customs, Police and financial institutions used to conduct joint operations at both the tactical and strategic level.

Immediate Outcome 7

a) New Zealand identifies and pursues parallel money laundering investigations alongside investigations of significant proceeds-generating crimes as a matter of policy, and conducts stand-alone investigations into money laundering on the basis of financial intelligence. The authorities are adequately skilled and trained to conduct financial investigations and utilise a wide range of investigative tools that are available to them. Operational agencies actively co-operate and share information and resources.

b) New Zealand investigates money laundering particularly in relation to the predicate offences that generate the most significant proceeds of crime. Prior to 2014 authorities prioritised the recovery of assets alongside prosecution of predicate offence. However, low rates of ML prosecution were identified as a concern in the NRA and New Zealand authorities introduced policy measures to address this, including legislative amendments, and dedicated training in financial investigations and ML prosecutions. Specialist police Money Laundering Teams were established in 2017; and, a target for money laundering prosecution as a high-level performance indicator for the police was set in 2018-19. These developments have begun to show a change in the trend since 2018, and money laundering prosecution is now considered an important tool in response to serious crime.

c) The number of prosecutions for ML has increased since 2018, including prosecutions of third-party money laundering, and is consistent with the national ML risk profile. There remain few cases of prosecution for ML in relation to foreign predicate offences (although those cases involve significant proceeds). Despite the significant improvements, it is not clear whether Crown Prosecutors' decisions on whether to prefer ML charges fully reflect the role of ML in enabling serious crimes, or the police objective to pursue ML offences.

Immediate Outcome 8

a) Confiscation is an element of the New Zealand Police's "Prevention First" operating strategy reflecting a strong and committed focus on confiscation of proceeds and instrumentalities of crime. Strategic documents behind this strategy identify a target volume of criminal assets to be restrained (NZD 500million by 2021).

b) This policy objective is operationalised by all Police and in particular the specialised Asset Recovery Unit (ARU), which works in co-operation with domestic and foreign investigative authorities, to initiate parallel restraint and forfeiture proceedings in response to identified crime and financial intelligence.

c) The ARU is effective in the use of the Criminal Proceeds (Recovery) Act 2009 (CPRA), with the delivery of forfeiture policy objectives. The CPRA provides a civil confiscation framework to detect and trace the widest range of criminal proceeds and benefits of crime. Both statistics and case studies reflect the ARUs are highly skilled in the investigation and confiscation of proceeds and instrumentalities of crime.

d) New Zealand is willing to pursue asset sharing or repatriation transnationally, and have pursued a number of asset recovery cases that involve significant volumes of proceeds of foreign predicates or domestic proceeds moved abroad.

e) New Zealand has a sophisticated and effective asset management system managed by the Official Assignee that works well to maintain the value of assets seized.

f) Customs conduct operations, investigations and pursues intelligence to detect non-declared cash, but only a small portion of this is confiscated and the penalties applied are not dissuasive.

Recommended Actions

Immediate Outcome 6

a) The FIU should implement sophisticated tools for prioritisation, database integration and analysis of financial intelligence. This would significantly enhance the FIU's ability to identify new targets and trends. Such tools would enable the FIU analysts to work more efficiently and increase the output of value-added intelligence products.

b) The FIU should continue its guidance and outreach activities to ensure that reporting entities (including those DNFBPs that are

not yet registered with the FIU reporting system) understand their reporting obligations, are able to quickly and seamlessly report SARs to the FIU, and have access to information on typologies and indicators.

c) New Zealand should encourage and provide guidance to LEAs on using FIU proactive financial intelligence products to launch financial investigations into new targets with an objective to increase the number of such cases. Relevant LEAs should receive training on the use of financial intelligence. The FIU is encouraged to establish ways for government agencies to directly access financial intelligence information from its databases. This would allow the FIU to reallocate resources away from responding to queries, and towards developing more detailed value-added intelligence products.

d) The FIU should incorporate a tracking/feedback mechanism into its case management which tracks the use of FIU products and financial intelligence directly accessed by LEAs.

e) The FIU should maintain and leverage its strong relationships with LEAs and the financial sector (including via the FCPN) to continue to maximise its support of LEA activities and investigation outcomes.

Immediate Outcome 7

a) Authorities should sustain the recent increase in money laundering investigation and prosecution, including maintaining and monitoring targets for ML investigation and prosecution, articulating the role of ML in strategies to disrupt serious and organised crime, and collecting more up-to-date and comprehensive statistics in order to monitor performance at all stages.

b) The Crown Law Office should consider developing prosecution guidelines for money laundering, to promote a consistent and effective approach to the prosecution of money laundering offences.

Immediate Outcome 8

a) New Zealand authorities should continue their focus on detection, seizure and confiscation of cross-border criminal assets.

b) New Zealand should ensure that effective, proportionate and dissuasive sanctions are applied for non-declared transportation of cash.

138. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32 and elements of R.2, 8, 9, 15, 30, 31, 34, 37, 38, 39 and 40.

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

139. Financial intelligence is regularly used by a wide range of New Zealand competent authorities to support investigations into ML/TF and related predicate offences, trace assets, enforce forfeiture orders and identify risks. Given a strong focus by New Zealand authorities on confiscation of criminal proceeds and instrumentalities of crime, LEAs routinely conduct financial investigations in parallel with criminal investigations. As a part of the police, the FIU is well situated to understand law enforcement priorities and strategic objectives and able to identify detect and share financial information that can support law enforcement work.

140. LEAs obtain a range of financial information both from the FIU (in response to requests for information and in financial intelligence products spontaneously disseminated by the FIU), via direct access to the FIU database, and through direct requests to financial institutions and DNFBPs. Since 2015, the FIU has received 3750 requests for information including 3369 requests from domestic agencies.

141. Authorised users in the Police have direct access to the FIU's database. The main users include the Organised Crime Group, Asset Recovery Units, Child Protection Teams; District Policing; Money Laundering Team; Evidence Based Policing; National Intelligence Centre; and Police Liaison Officers (international). An increase in authorised users has led to a more than six-fold increase in the use of direct access data by non-FIU users over the last five years, with 13 834 person lookups conducted in 2019 (compared to average of 37 000 person lookups by FIU staff per annum). For Police employees who do not have authorised access to goAML, the FIU has a generic inbox whereby they can send a request for information.

142. Several other authorities (including Customs and sector supervisors) find goAML to be a valuable source of intelligence for financial investigations and have expressed interest in having direct access to the system. There are plans to provide direct access to a range of Government agencies including the DIA, FMA, RBNZ, Customs, MBIE, MPI, and the OIO. This will enable these authorities to identify risks across the sectors, and prioritise their activities accordingly, as well as reduce the burden on the FIU to manually respond to routine requests for information.

143. LEAs generally have the necessary resources and skills to utilise financial intelligence. In some cases, the FIU assigns an analyst to support a financial investigation. There are no statistics tracking the number of SARs that were used in financial investigations, nevertheless, based on analysis of case studies, financial intelligence is used to conduct investigations, detect criminal networks, identify beneficial owners, and detect property and other assets subject to further restraint and confiscation (e.g. see Operation Nova). Financial intelligence is used to support all asset recovery cases.

144. The cases reviewed show that financial intelligence is used across a spectrum of investigations relating to different types of predicate offence, including drug trafficking, fraud and tax crime, aligning with New Zealand's risk profile. Financial intelligence is also used in the investigations of other criminal offences such as bribery and illegal disclosure of information. It is used both in relation to domestic offences and where funds flow across jurisdictions. Financial intelligence was used to support investigations into serious offences such as terrorism financing, terrorism and labour

exploitation cases. In 2016-2019, the FIU supported 291 ML investigations and 1 482 investigations into other offences.

145. The FIU's output is utilised less by New Zealand's geographically-based district police units than it is in the more specialised national police units, which largely reflects the different nature of the crimes they investigate. However, there is a steady increase in access to the goAML database by district police staff, and the FIU is encouraged to continue to increase awareness of how financial intelligence can support district-led investigations.

146. The FIU also disseminates a significant amount of financial intelligence to LEAs (including SARs related to targets of their investigations) across Government (See Table 3.1) which is actively used by authorities, as set out in the table below.

Table 3.1. SARs Disseminated to the Competent Authorities

Agency	2017		2018		2019		Total no of SARs	Total no of Reports
	No of SARs	No of Reports	No of SARs	No of Reports	No of SARs	No of Reports		
Charity Services (DIA)	-	-	-	-	39	2	39	2
DIA	761	35	688	53	3 494	49	4 943	137
District Policing	737	234	1 465	393	886	323	3 088	950
FCG	89	50	224	81	555	151	868	282
IR	2 566	103	1 879	115	667	90	5 112	308
MBIE	282	78	341	81	252	49	875	208
MSD	400	154	332	97	64	7	796	258
National Policing	402	121	1 279	180	1 0351	226	1 2032	527
National Security	83	22	323	61	98	58	504	141
NZCS	255	39	282	35	639	43	1 176	117
Other	11	7	175	31	92	67	278	105
Other gov't agencies	53	14	64	21	185	20	302	55
Other police duties	83	26	185	55	131	24	399	105
RBNZ	-	-	1	1	67	3	68	4
SFO	50	18	36	17	55	7	142	41
Total	5 772	901	7 274	1 221	17 575	1 119	30 622	3 240

Box 3.1. Financial investigations into high-risk crime

Operation Nova (drugs, 3rd party ML by a gatekeeper profession)

From 2018 to 2019, the FIU assisted NOCG's investigation into an Outlaw Motorcycle Group operating across Australia and New Zealand, engaged in large scale illicit drug supply and ML. The FIU provided financial analysis of the targets' bank accounts; liaised with REs through the Financial Crime Prevention Network (FCPN) to inform targeted SAR

reporting; and analysed SAR information to identify financial facilitators, key associates and ML typologies.

During the investigation the FIU disseminated 83 distinct reports to the investigation team, relating to approximately 100 SARs. The FIU identified the trusts from financial reporting and obtained beneficial ownership information through trust deeds obtained from the banks. The operation resulting in the seizure of NZD 3.7 million worth of assets and the arrest of eight individuals for several charges including ML. These individuals included an accountant and a lawyer who were assisting gang members launder their criminal proceeds.

Operation Whitehorn (customs duties evasion)

The investigation was initiated following information that an individual was selling cigarettes from the boot of his vehicle. Investigations revealed that between 2015 and 2018, the offenders imported over one million cigarettes.

The financial component of the investigation included conducting a financial analysis using bank account data, loan files, property registries, information from Inland Revenue, through co-operation amongst Customs, Police (including the FIU and ARU), Inland Revenue, Sky City Casino and various financial institutions. The FIU provided ARU with financial intelligence. The volume of duties evaded was NZD 18 22 million and the amount of assets restrained under the CPRA included three properties, two cars, six bank accounts (NZD 184 500) and cash (NZD 4 182 000).

Operation Gandolf (proceeds of crime moved abroad, FIU triggered):

In May 2014 the FIU observed a pattern of remittances by New Zealand based criminals to Thailand. Network analysis determined that structured payments were being sent to a small number of individuals in that country who were known to be involved in the drug trade. As an understanding of the typology developed, the FIU liaised with reporting entities to provide tactical and typology information which prompted further SAR reporting. Over the course of the operation a total of 69 SARs were submitted by reporting entities.

In addition, the FIU produced subject-profiles and liaised with the Police Liaison Officer in Bangkok to provide further corroborating intelligence.

A covert operation by NOCG in September 2014 determined that an international drug syndicate had been importing methamphetamine to New Zealand for two years. As the operation progressed, the FIU worked closely with NOCG to provide them financial intelligence and an understanding of the network and methodology.

The ringleader based in Thailand was arrested in February 2016 by the Thai authorities. The syndicate members were prosecuted with the ring leader sentenced to 13 years' imprisonment.

Between 2015 and 2016 there were three subsequent Operations (Ops Broken, General, and Cossack) that targeted the successors to this

international drug syndicate who stepped in to fill the void by imprisoned members of the syndicate. These operations were run by district organised crime units and a network analysis of 28 SARs was undertaken by the FIU to identify entities. Prosecutions for drug dealing and ML arising out of these operations resulted in long terms of imprisonment (from 8 to 15 years). The ARU restrained assets across all four operations.

SARs received and requested by competent authorities

147. The FIU receives SARs and PTRs mostly from banks and money remitters, and to a much more limited extent from DNFBPs (which aligns with expectations, given the maturity of AML/CFT obligations for the DNFBP sectors). More recently, there has been increased reporting by VASPs and TCSPs.

Table 3.2. SARs/STRs by Type of Reporting Entity[8]

	2016	2017	2018	2019	Total
Banks	5 471	5 556	7 295	7 893	26 215
MVTS	2 905	2 727	2 892	3 578	12 102
Other FIs	505	498	719	1021	2 743
Casinos	81	83	88	73	325
Other DNFBPs	20	49	128	358	550
Total	8 982	8 914	11 129	12 941	41 966

148. The FIU uses goAML as the online reporting facility for submission, storage and analysis of PTRs, SARs, and for secure communication between the FIU and reporting entities. The goAML message board is used to post information associated with guidance, online training modules, etc. To register for goAML, reporting entities send a request to the FIU, with most reporting entities registering proactively. DNFBPs were introduced as reporting entities progressively between 2018 and 2019 and the FIU has invested a significant amount of time conducting outreach and training (both in form of webinars to industry groups and goAML training for individual registered users) to these sectors.

149. At the time of the onsite visit, about 2 700 reporting entities were not registered with the goAML. Almost all of these unregistered reporting entities are DNFBPs such as non-bank non-deposit taking lenders (low risk sector), accountants (medium-high risk), lawyers (medium-high risk), real estate agents (medium-high risk), TCSPs (high risk). This represents approximately 40% of DNFBPs or 25% of all reporting entities. The analysis of the number of employees and value of transactions of these reporting entities show that the entities not registered in goAML are materially smaller than those registered. There remains a concern that these entities will not be able to report promptly which may lead to a gap in the financial intelligence available to the FIU. However, there are mitigating measures undertaken by the FIU and sector supervisors, including provisions to report SARs orally/via email. These are followed up with registration with goAML and electronic re-submission of SARs, as well as intensive

8 See Table 5.1 for a fuller breakdown of reporting by reporting entity type.

outreach and training for these reporting entities. Taking into account the materiality and mitigating measures, this shortcoming does not have a significant impact on the FIU's access to financial intelligence. However, the FIU should continue its guidance and outreach activities to ensure the widest possible coverage of reporting entities.

150. Statistics indicate that the financial intelligence the FIU receives is generally in line with New Zealand's risk profile: ML (20%), tax evasion (20%), fraud (18%) and drug offending (9%) are the basis for most suspicious activity reporting. Some SARs are related to PEPs (0.5%), terrorism/terrorism financing (2.5%) and misuse of legal persons and arrangements (4%).

151. SARs are submitted in the form of a structured file with a textual description of suspicious activity that contains valuable details, including personal data, technical and geo-location information, as well as key words that indicate the type of crime the financial activity might relate to. SARs often contain attachments, such as individual wire transfers, geolocation information or files from video-surveillance systems. In addition, reporting entities have a range of indicators they can select from when reporting SARs, which assist with subsequent prioritisation and analysis. To maintain data quality, prior to 2018 the reports were manually checked before they were analysed. New Zealand authorities indicate that the quality of reports has improved over the years.

152. The FIU can access a wide range of other resources, such as criminal, administrative and ownership data. This includes access to the National Intelligence Application (NIA, criminal intelligence, criminal records, Land Transport New Zealand records, Immigration records, passport records, and Births, Deaths, and Marriages records), the Police's Investigation Search Tool (which searches across documents of all serious criminal investigations), Voicebox (application used by the Crime Monitoring Centre for the recording of intercepted communications); credit history checks, vehicle registers, telephone subscriber records, real estate registers, the WorldCheck database, NZ Companies Register, and the Foreign Trusts Register. The FIU can obtain information from other agencies' systems including Inland Revenue, Customs, MSD and Department of Corrections, through existing inter-agency agreements.

153. New Zealand amended the AML/CFT Act in November 2017 to require reporting entities to report PTRs based on a statutory threshold. These were introduced to address the high risk posed by international wire transfers and cash payments, as identified in the NRA. The FIU has received almost 9 million PTRs between 2018 and 2019, most of which are international wire transfers.

154. PTRs are used to give New Zealand competent authorities a broader intelligence picture, and to inform FIU risk assessments of persons who are the subjects of incoming SAR reports. This supports the FIU's tasking and deployment decisions for further analysis. The FIU also draws on PTRs to assist with network analysis in relation to persons connected to SAR reports (i.e. to identify third parties with whom the subjects of SARs may be transacting, but who are not directly identified in SAR reporting). The FIU routinely uses PTRs to develop insights into 'known unknowns', i.e. to identify associates and networks linked to known targets.

155. Current technology limits the ability of FIU analysts to proactively harness PTR reporting. To overcome this hurdle, data analysts scan for 'unknown unknowns' (i.e. to identify illicit activity through structural indications) using SAS Data Analytics. Products such as the FIU's Cash Based Scorecard (which is part of the PFT) and the

Country Profiles are examples of this. The FIU's technology also does not currently allow PTRs to be taken into account in the early part of the STR prioritisation process. The FIU is currently looking for the relevant software solutions as a part of its Service Delivery Transformation Project, which would allow it to fully exploit this information.

156. All Border Cash Reports (BCRs) collected by Customs officers at airports and other ports of entry/departure (on transportation of cash/BNIs in a value of more than NZD 10 000) are forwarded to the FIU in a physical form and must then be manually introduced into the FIU's database. In 2016-2019, more than 15 000 BCRs were completed.

SARs prioritisation and analysis process

157. The FIU's SAR/STR prioritisation process for tactical AML leads is called Proactive Financial Targeting (PFT) and it starts with the data quality control mechanism. SARs which are prioritised are subject to further, more detailed analysis.

158. Prior to 2018, SARs were scrutinised manually and prioritised based on a matrix. This process was unsustainable due to the increasing number of reports and the resources required. The current process is semi-automated, and is based on keywords and matches with the Police intelligence database. Since the introduction of this system in 2018, there has been limited manual review of individual SARs. Nevertheless, some manual oversight has been retained in order to allow SARs carrying certain risk factors to be subsequently prioritised by the automated process even if not triggered by the keyword system.

159. The current process for prioritisation automatically cross-checks SARs against a list of 199 keywords (including combinations of keywords and phrases), and also software cross-checks all of the SARs against the Police database. Approximately 20% (142) of reported SARs are prioritised by these tools and escalated for further review by an analyst. The remaining 80% of reports are not individually reviewed, though they do form part of the FIU database, and therefore are available to be analysed and disseminated in response to LEAs' request for SAR information (usually without added value from analysts), as well as included in STR spreadsheets, and used for strategic analysis purposes. 41% (58) of escalated SARs are sent in support of active investigations. 11% (16) are used in the PFT document which is sent out to LEAs every month and to CFT leads every week, and evolves according to operational needs. It can also be expanded based on strategic intelligence and discussion of specific typologies with LEAs (e.g. as set out in Box 3.2 on Operation Tyche). The key words list for CFT is more comprehensive and it continually evolves to support ongoing operational needs. On average, the PFT identifies 34 (24% of the isolated SARs) new investigation leads every month.

160. While the prioritisation process is an improvement on the previous manual review, and is efficient at identifying financial activity associated with known targets of LEAs, it does not fully exploit the intelligence and information available to the FIU, which has greater potential to identify suspicious activity by otherwise unknown persons. Notably, information already contained in the FIU database, including PTRs and BCRs, as well as correlations with past SARs, are not used during the prioritisation phase (although this information is used during subsequent analysis of SARs which are prioritised).

161. The FIU currently has 33 staff members, organised in four groups including intelligence functions, investigators to support development of financial intelligence,

and a training, liaison and compliance team. There are 14 analytical staff, (including two dedicated to TF), two investigators and two data analysts.

162. The FIU analysts have access to analytical tools such as IBM i2 for charting, Microsoft Excel & goAML profile queries to conduct financial analysis, and SAP Business Objects to match goAML data with other police systems. Data analysts are using SQL Server Management Studio to extract data and are using Microsoft Power BI and SAS Data Analytics to analyse and visualise the data. However, FIU analysts are not supported by automated analytical software tools that allow for integration and cross-matching of data coming from different sources, and have to consult and cross-check SARS with other data manually. This significantly reduces their efficiency and may result in missed opportunities to enrich their analysis with relevant information from other data sources, such as PTRs and cash declarations. There are plans to update the analytical system by acquiring automation tools. This, together with the expansion of direct LEA access to the FIU database, would enable the FIU's analytical staff to spend more of their time on developing deeper analysis, and less on gathering and checking data, and responding to routine information requests.

Operational needs supported by FIU analysis and dissemination

163. The FIU produces a wide range of financial intelligence products as reflected in Table 3.3, which are disseminated domestically and abroad. These support the operational needs of relevant LEAs, which include the investigation and prosecution of ML/TF and predicate offences, as well as assets forfeiture, to a high degree.

164. The FIU devotes a significant proportion of its resource to support the operational needs of LEAs. Half (six analysts and two investigators) of the FIU's intelligence resources are assigned to the Operations Team who directly support LEA's criminal investigations and developing intelligence products. The Response Team is the next largest (with two analysts and four Intelligence Support Officers) who are primarily engaged in responding to requests for information from LEAs. The balance of resource (two analysts and two data analysts) sit in the Strategic Team.

Table 3.3. FIU Products Disseminated to Law Enforcement Agencies

Product Breakdown (by year)	2016	2017	2018	2019	2020 (until March 2020)	Total
Information Reports	708	831	968	995	149	3 651
Intelligence Reports	70	146	102	61	16	395
SAR Spreadsheets	73	65	65	69	10	282
Strategic Reports	NA	10	7	14	NA	31
Proactive Financial Targets Lists	NA	7	22	12	NA	31
Cash-based Score Cards	NA	NA	NA	8	2	10
Country Profiles	NA	NA	NA	17	NA	17
Total (by year)	851	1 059	1 164	1176	177	4 427

Tactical Analysis

165. The FIU Information Reports are the most common reports released by the FIU. These can be in response to requests for information, be proactively released in response to something identified in the PFT process, or be released in an ongoing and structured manner as part of the FIU's provision of direct support to an investigation.

166. FIU Intelligence Reports, represents the most in-depth analysis of specific tactical cases by the FIU, and make up 9% of reports disseminated. Other types of tactical products include Information Reports and SAR spreadsheets, which are used to quickly and regularly disseminate financial intelligence to the relevant competent authorities based on the understanding of their operational needs - but do not include the same degree of analysis by the FIU. The PFT list is also circulated – (as noted above) - and this process can be used in combination with strategic intelligence products to identify priorities for further in-depth tactical analysis.

167. Since 2019, the FIU has developed Country Remittance Profiles. These analyse remittance flows between specific jurisdictions and New Zealand, based on SAR and PTR reporting. These are used to identify areas of risk, detect unregistered money remitters and other targets for investigations, and to prioritise the placement of overseas liaison officers.

168. While the FIU's focus on known targets corresponds to the operational needs of LEAs, it does not yet fully exploit the potential of financial intelligence to detect criminal activity by persons not already known to law enforcement. This could contribute significantly to detection and investigation of laundering of the proceeds of crime, particularly those committed abroad in the absence of an initial request/information from the foreign counterparts. Realising this potential would require the FIU to have more sophisticated tools. to devote more of its analytic resources to developing financial intelligence. It would also require willingness on the part of LEAs to start criminal investigations based on FIU proactive intelligence reports.

Strategic analysis

169. The FIU conducts strategic analysis to identify themes, trends and emerging risks on a range of topics including the Terrorist Financing Risk Assessment, scams, virtual assets, and alternative remittance networks. This analysis is disseminated mainly in the form of Strategic Reports, of which 31 were produced between 2017 and 2019. These contribute to competent authorities' understanding of the ML/TF and organised crime environment and also inform and influence senior decision makers both within and outside of Police.

170. An example of the value gained from strategic reports is the analysis conducted of money flows between New Zealand and particular receiving countries. This analysis aimed to identify the main domestic risk areas and to assess the different risks posed by different remittance corridors, so as to identify possible financial targets for law enforcement. Through this analysis, a number of unregistered money remitters were identified which in turn led to investigative leads for the relevant authorities. Operation Tyche (below, box 3.2) also illustrates how strategic intelligence products can lead to the development of tactical financial intelligence, in collaboration with Police.

171. The FIU also produces Joint Strategic Analysis products with other authorities such as the National Intelligence Centre. Strategic Analysis does not only contribute to specific reports: the FIU played the central role in preparing New Zealand's NRA, which is itself a high-level strategic intelligence product informing the whole AML/CFT system.

Box 3.2. *Operation Tyche*

Operation Tyche was a National Organised Crime Group (NOCG) investigation initiated from the FIU intelligence. Through the PFT process, the FIU identified an emerging trend involving cash depositors from an Asian country, banking extremely large amounts of cash throughout Auckland. The working hypothesis formed was that the reported activity was an alternative remittance system which was being used to launder the proceeds of drug offending.

FIU analysts presented their preliminary analysis at the monthly Targeting and Co-ordination meeting, attended by NOCG, ARU and FIU management, where it was agreed an FIU intelligence package would be prepared for NOCG. The FIU intelligence package comprised a strategic intelligence report which included analysis of SAR transactions amounting NZD 184 million, and target profiles of the four primary cash depositors, including pattern-of-life analysis, an overview of deposit activity, and analysis of IP data to enhance understanding of the network.

The FIU intelligence package was disseminated to NOCG in early 2018, resulting in NOCG targeting of the primary cash depositors and other members of the network. This resulted in several subsequent off-shoot investigations, one of which is a major money laundering investigation codenamed Operation Martinez, conducted by the Money Laundering Team from 2019 to 2020, resulting in the prosecution of third party launderers who operated a financial services business, and the restraint of NZD 7 million in assets. The FIU provided ongoing, operational support throughout each of these subsequent operations, including real-time analysis of incoming SARs and liaising with the FCPN to stimulate reporting on key targets.

TF intelligence

172. New Zealand's FIU has two analysts dedicated to monitoring possible terrorism financing. They work in direct contact with a dedicated counter-terrorism investigation unit in the Police National Security Group. This unit can draw on additional financial investigation expertise from within the FIU and broader Police Financial Crime Group if and when required. Analysts from the FIU and the National Security Group collaborate on analysing SARs identified through the TF prioritisation process. The number of such SARs is low: 330 SARs were flagged as TF-related between 2013 and 2019 (0.46% of total SARs). This is consistent with New Zealand's low terrorism financing risk profile. There was an increase in the number of SARs citing the terrorism financing indicator following the Christchurch attacks, but this reflected heightened sensitivity among reporting entities (while the threshold for suspicion was very low, this reporting cannot be qualified as defensive), and not a change in the underlying activity or risk.

173. Between 2016 and 2019 the FIU has initiated six investigations related to financial elements, to support CT investigations. Over the same period it has provided direct assistance to 40 counter-terrorism investigations.

174. The FIU actively responded to the Christchurch attack, devising and implementing a new process to collect, analyse and disseminate TF-related intelligence as a matter of high priority, in the immediate aftermath of the attack and for the following months during the period of heightened risk of copycat or retaliatory attacks. Financial intelligence was shared with and requested from foreign FIUs via the Egmont channel. (See IO9).

Use of FIU's financial intelligence by the competent authorities

175. The most relevant specialised Police units - the Money Laundering Team and Asset Recovery Unit - see significant value in the FIU's products and devote significant resources to investigations based on FIU intelligence reports, including those relating to previously unknown targets. Other Police units seem to make less use of FIU intelligence as the starting point for investigations, but do make significant use of financial intelligence to support ongoing criminal investigations. In response to this demand, the FIU's prioritisation and analysis emphasise supporting ongoing criminal investigations, and disseminations of financial intelligence related to known targets of LEAs' investigations. While producing proactive intelligence through the PFT process, there is scope to increase this through the comprehensive analysis of international funds transfers and large cash transactions. FIU products are also used by Customs for detection and investigation of TBML, smuggling and other criminal offences.

Table 3.4. FIU Intelligence Provided in Support of Domestic Criminal Investigations

	2016	2017	2018	2019	Total
ML Investigations supported by FIU	35	52	77	108	291
Other offences assisted by FIU	197	390	452	429	1 482
Total	250	442	529	537	1 773

176. It is difficult to track or measure the degree to which financial intelligence disseminated by the FIU contributes to the outcome of a specific investigation. Statistics do not provide a full picture of the extent to which FIU products triggered proactive investigations based on new targets identified. However, assessors have reviewed some cases triggered by the FIU's analysis, which demonstrate that the FIU's analysis was of high-quality and reflected a good understanding of LEA's needs. These investigations were triggered by different types of FIU products, including intelligence reports, information reports and PFTs. As illustrated in some cases (Operations Tyche, Gandolf and Nova) strategic intelligence products developed by the FIU are used to refine their prioritisation and analysis, which enables the FIU to develop tactical intelligence in response to LEA's needs.

177. Financial intelligence is used by sector supervisors (DIA, FMA and RBNZ) both for strategic purposes (to understand existing and emerging sector risks amongst its reporting entity population) and at a tactical level to support the preparations for onsite inspections of reporting entities. Prior to an onsite visit, sector supervisors request relevant information regarding the reporting entity under inspection from the FIU, which helps them to understand the type, volume, and quality of SARs submitted, the extent to which the entity is aware of its reporting obligations, and to assess its level of compliance and detect potential misuse.

Co-operation and exchange of information/financial intelligence

178. The FIU's Tasking and Co-ordination process involves the NOCG, ARU, MLTs and District Investigators, who meet to discuss selected investigations where they see value in further work by the FIU. The PFT is also discussed at this meeting as a tool to focus on relevant information. The FIU provides both resource and operational support for proposals which are taken-up.

179. The FIU also participates in various multi-agency groups which provide further opportunities to co-operate and exchange information and intelligence such as the Combined Law Agency Group (CLAG), and the Financial Intelligence Risk Group and the Financial Crime Prevention Network (FCPN).

180. Through the FCPN, the FIU has a public-private partnership between Police, Customs, and financial institutions. It currently includes the five largest banks, which have a combined retail market share of 89% .The FCPN can act as a forum to share financial information on criminal investigation targets, information on high-risk customers not yet subject of a criminal investigation, as well as to co-ordinate joint activity at both the tactical and strategic level. There are also plans to expand FCPN membership to other reporting entities and to enable them to use it to share SAR information with each other. The FCPN's work agenda includes issues relating to major risk areas such as TBML, virtual assets, on-line child sexual exploitation, use of TCSPs, etc.

181. Since November 2019, the FIU has begun to release 'FCPN Alerts' to alert financial institutions about information relevant to criminal and national security investigations so that they can identify relevant activity and submit SARs. This can be used to refine and focus reporting institutions on emerging types of illicit activity, or to prompt detailed reporting on specific targets of ongoing law enforcement investigations. Between November 2019 and August 2020, there have been 42 FCPN Alerts, which have resulted in 273 high-quality SARs submitted in direct support of investigations. One example of this approach is set out below in box 3.3.

Box 3.3. Use of FCPN to obtain financial intelligence to support investigations - Operation Albatross

An investigation was initiated by the FIU into suspected right-wing activity and illegal disclosure of information by an employee of the New Zealand Defence Force. As part of the investigation, The Financial Crime Prevention Network was issued an urgent bank alert seeking information on this target. The information received from banks via the FCPN mechanism, combined with further intelligence, resulted in charges for accessing a computer system for a dishonest purpose and for disclosing information that prejudiced the security or defence of New Zealand.

Overall Conclusions on IO.6

182. Financial intelligence is regularly used by competent authorities to support investigations into ML/TF and related predicate offences, trace assets, enforce forfeiture orders and identify risks. The value of the FIU's intelligence products, and their use in investigations, is demonstrated in a number of cases cited in this report, and further cases reviewed by assessors.

183. A key strength of the FIU is its collaborative relationships with LEAs, in particular with NOCG, ARU, Customs, and IR. LEAs request and receive financial intelligence in line with identified ML/TF risks, and have a large degree of influence on the FIU's priorities and targets for detailed analysis, both through the PFT process, through follow-up to disseminations of less detailed intelligence products (information reports and SAR spreadsheets) and through their wider interactions with the FIU. The FIU's tactical intelligence reports therefore seem highly reflective of the needs of law enforcement, and materially support their ongoing criminal investigations

184. While the FIU's focus on known targets corresponds to the operational needs of law enforcement authorities, it does not yet appear to fully exploit the potential of financial intelligence to detect criminal activity by persons not already known to law enforcement, and this is reflected in the relatively small number of investigations initiated on the basis of FIU reports. This is offset to some extent by the role of feedback from police units in focusing the FIU's prioritisation and targeting. Strategic intelligence products enable relevant police units to identify activities and persons of concern, which are then prioritised by the FIU for deeper analysis. Dissemination of raw SARs also enables law enforcement units to identify further targets for FIU attention. By these means, the FIU and Police units can jointly and iteratively develop financial intelligence on new targets, even when this is not done through a single stage of FIU analysis.

185. The provision of more sophisticated tools for prioritisation, database integration and analysis would significantly enhance the FIU's ability to directly identify previously unknown targets based on the information available to it. Such tools would also enable the FIU's analysts to work more efficiently and develop their intelligence products further.

186. The FIU receives a significant volume of SARs/STRs/PTRs from financial institutions and MVTS operators, consistent with the risk profile and exposure of these sectors. However, the reporting from the DNFBP sectors, including TCSPs, is limited, reflecting the recent introduction of reporting obligations for these sectors. About 2 700 of reporting entities (mostly DNFBPs) have not yet registered with the FIU reporting system, however taking into account the materiality of these sector and mitigating measures, this shortcoming does not have a significant impact on the FIUs access to financial intelligence. The FIU should continue its guidance and outreach activities to ensure that these reporting entities understand

their reporting obligations, are able to quickly and seamlessly report SARs and have access to information on typologies and indicators.

New Zealand has achieved a substantial level of effectiveness for IO.6.

Immediate Outcome 7 (ML investigation and prosecution)

ML identification and investigation

Organisation of Money Laundering Investigation

187. The 2012-13 National Risk Assessment identified New Zealand's then low rate of prosecution for money laundering offences as a problem, and in 2014, New Zealand authorities formulated policy measures to address this. These included legislative changes, training targeting ML prosecutions and the allocation of dedicated funding to train financial investigators within the New Zealand Police and other LEAs. The changes also continued with the establishment of dedicated Money Laundering Teams (MLTs) within the Police in 2017, and the adoption in 2018-19 of a target for money laundering prosecution as a high-level performance indicator for the police as a whole.

188. Several different bodies conduct ML investigations in New Zealand, primarily within the Police. The Serious Fraud Office, Inland Revenue and Customs Service also investigate money ML when appropriate or parallel to their predicate investigations.

189. The investigative units within the Police that investigate predicate offences as well as money laundering offences are the Financial Crime Group - which includes the MLTs, as well as being the parent unit of the FIU. Other units involved in ML investigation include the National Organised Crime Group (NOCG), Police Fraud Squad, and Police Districts' Organised Crime Units. The Police's Asset Recovery Unit (ARU) which is also part of the Financial Crime Group, works closely with all the relevant units and agencies, for asset recovery investigations, and regularly supports criminal investigations through the presentation of financial related evidence in criminal proceedings.

190. The MLTs were established as a dedicated resource to investigate money laundering. The MLTs target high risk entities, including professional facilitators and alternative remittance, as identified by the NRA. Their investigations are primarily driven by FIU referrals that are aligned with the NRA. MLT investigative teams include police investigators alongside forensic accountants and analysts. The MLTs investigate money laundering independently, e.g. running investigations of high-level third-party money launderers. They also work in parallel with other Police investigations of predicate offending. In addition, MLTs support Police workgroups, including NOCG, with financial analysis and provide advice on investigative methodologies and money laundering charges. Since their creation in 2017 there has been an increase in money laundering related cases and prosecutions.

191. New Zealand Police adopted a high-level target in 2018-19 for investigation and prosecution of money laundering activity as one of the performance measures associated with its high level target for asset recovery (set out below in the analysis of IO8). This set a goal for the number of money laundering investigations that result in prosecution, which was published in the Police Annual Report. For the period of 2018-19, the target was set at 30 to 40 (and 35 achieved).

192. The Serious Fraud Office (SFO) is a specialist law enforcement agency responsible for addressing serious and complex financial crime in New Zealand. While its cases often involve elements of money laundering, the SFO will typically focus primarily on pursuing and prosecuting the predicate offending. Pure money laundering investigations remain under the purview of the Police.

193. The Customs Service undertakes parallel money laundering investigations linked to predicate offences within areas of its responsibility including money-laundering arising from cash smuggling and TBML. Since Customs established its Financial Crime Unit (FCU), it has provided financial analysis assistance to identify money laundering and to support asset restraint. Tax crime is dealt with through civil remedies available under the Tax Administration Act, and through criminal prosecution where the case is severe, and where there is sufficient evidence and public interest. Inland Revenue has also recently prosecuted money laundering offences linked to tax crimes.

Investigation of Money Laundering Activity

194. The LEAs make use of full range of investigative techniques in both predicate and related money laundering investigations. These include production orders, search warrants, undercover operatives, and interception of communications through the use of surveillance devices. The LEAs are skilled and trained to conduct financial investigations to support both investigation of predicate offences and parallel money laundering investigations. Training to become a New Zealand Police detective covers conducting investigations of financial crime, including money laundering and predicate offences. Police have also developed a specialist ML course which is attended by investigators across LEAs, throughout the Pacific and Australia. The excellent training of ML investigators is reflected in the skilful manner in which they are able to conduct complex investigations of financial crimes and gather evidence.

195. There is strong communication and co-ordination among the various law enforcement agencies and competent authorities in New Zealand, which facilitates information exchange, and inter-agency and joint investigations. While MOUs are used to formalise co-ordination arrangements and relationships, the close-knit law enforcement community in New Zealand enables close co-operation and co-ordination even in the absence of such formal arrangements. Different units and agencies are able to identify opportunities for timely intervention and ensure de-confliction where necessary. Within the Financial Crime Group of the Police, the specialised groups such as the FIU, ARU and MLTs operate in an integrated way to maximise intelligence, prosecution and confiscation outcomes. This arrangement fosters effective co-ordination, and the sharing of financial intelligence in support of ML/TF and related predicate investigations at the national level.

196. Money laundering cases in New Zealand are identified as a result of parallel financial investigation alongside an investigation of serious predicate offence, or based on receipt of financial intelligence or information provided from a foreign partner. Recent case studies show that New Zealand is increasingly able to successfully identify and investigate ML activity related to predicate crime investigations as part of its pursuit of criminal proceeds. Several cases set out below in box 3.4 - illustrate how New Zealand is able to identify and investigate ML activity and also the range of techniques and tools used by investigators including their use of international co-operation to pursue evidence.

Box 3.4. Money Laundering Investigations

Operation Notus

In 2017/18, the National Organised Crime Group supported by the Waikato ARU investigated an organised crime group involved in the sale and distribution of methamphetamine and cannabis and the associated laundering of profits. The investigation involved the full range of covert investigation techniques included electronic (wire taps) and physical surveillance. FIU intelligence was a feature of this investigation along with financial information obtained via a mutual assistance request to Australia.

Twelve persons were charged with various drug and money laundering offences. NZD 1.6 million in assets were restrained including 8 residential properties, 17 vehicles, 6 motorcycles, 5 boats, 2 jet skis and the contents of 27 bank accounts. For ease of prosecution the matter was split into separate trials the first of which has occurred and resulted in guilty verdicts for money laundering for the eight defendants. Sentencing will occur in early 2021.

Operation Menelaus

In 2019, the MLT undertook investigations into drug activity where drug packages were intercepted en-route to their delivery. Based on surveillance, NZ police ascertained details of the drug trafficking activity as well as the related money laundering, including cash drops.

The MLT requested information from the FIU. Financial transactions were monitored and several SARs were disseminated to the investigating team. An Egmont request placed by the FIU led to information from an overseas partner. Investigative techniques included the interception of private communications, surveillance via tracking equipment and physical surveillance. NZ authorities intercepted conversations relating to these money transfers where the offenders discussed the need to deposit small amounts of money into different banks due to the AML controls in place.

Three persons were charged in relation to third party laundering and charges of structuring. Prosecution remains ongoing. NZD 5 million in assets were restrained with the offenders currently awaiting trial.

Operation Manuka (see also IO8)

In 2018, investigations were conducted into an organised crime group dealing with drugs purchased from abroad and sold in NZ for substantial profits. Online accounts on the dark web and cryptocurrency were used to pay for the imported drugs. The money was used to purchase expensive vehicles that were then re-sold and the proceeds were transferred to bank accounts of the offender and accounts of his friends and relatives. A digital forensic expert was used to trace the cryptocurrency. Although the internet site had been closed, the expert

identified a purchaser which led to further information regarding the scale of the operation.

NZ Police obtained production orders to obtain banking information, which revealed that money had also been moved to UK banks and used to purchase UK property. With the assistance from UK associates through their police liaisons as well as through MLA, it was learnt that Travelex money cards were loaded up with cash and funnelled overseas, where the money was then withdrawn.

The main offender was found guilty for drug offences as well as money laundering and was sentenced to 4.5 years' imprisonment in total. A profit forfeiture order was issued for the property with an approximate value NZD 1.75 million (estimated value of drugs imported). The forfeiture order has been enforced in the United Kingdom. His partner, who had no previous convictions, but who assisted with the ML associated with NZD 187 000, was sentenced to 18 months' imprisonment which was ultimately converted to 6 months' community service.

Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

197. The pursuit and recovery of criminal proceeds is one of the key targets for the New Zealand Police, and their investigations into money laundering activity support this goal. New Zealand authorities recognise that targeting money laundering is consistent with their strategy to disrupt organised crime and the wider policy objective of making New Zealand safe. Police have clearly set out a high-level target for depriving criminals of the proceeds of criminal activity, with a focus on asset recovery, which is the basis for a "follow the money" approach across the police.

Table 3.5. Money Laundering Investigations/Prosecutions by Type of Predicate Offence

Year ML Offence Occurred / Predicate Offence Type	2015	2016	2017	2018	2019
Drug Predicate Offences					
Case Files	6	6	6	10	8
Individuals charged with ML	5	2	15	14	27
Counts of ML laid	10	2	48	17	134
Fraud/Obtained by Deception Predicate Offences					
Case Files	15	22	19	63	114
Individuals charged with ML	7	6	2	55	69
Counts of ML laid	12	8	8	76	91
Receiving/Theft/Burglary Predicate Offences					
Case Files	9	1	-	1	1
Individuals charged with ML	1	1	-	1	1
Counts of ML laid	4	1	-	1	1
Other Predicate Offences					
Case Files	-	2	8	5	14
Individuals charged with ML	-	-	-	-	3
Counts of ML laid	-	-	-	-	12
Total					
Case Files	30	31	33	79	137
Individuals charged with ML	13	9	17	70	100
Counts of ML laid	26	11	56	94	238

198. The information on money laundering cases and charges set out above in Table 3.5, shows the impact of the legal and organisational reforms introduced which is visible by the significant growth in the number of money laundering cases investigated, the number of individuals charged, and the number of charges laid. This increase was driven mainly by ML prosecutions related to drug and fraud predicate offences, and is in line with identified risks.

199. There are some areas where it is not clear that money laundering is pursued to the extent expected based on the risk environment, particularly laundering by gatekeepers, and laundering of the proceeds of tax offences.

a. *Gatekeepers:* The police target drugs and organised crime as part of their "prevention first' strategy and in their investigations identify channels for money laundering including through professional gatekeepers, real estate and alternative remittance providers. The MLTs have been working on targets that are in line with the NRA. However, only a few cases (such as Operation Nova, set out below in Box 3.7) resulted in those facilitators being prosecuted on ML charges which suggests focus in response to risk.

b. *Tax Offences*: Tax offending is identified in the NRA as a significant source of proceeds, and the Inland Revenue actively pursues tax fraud and/or tax evasion. While money laundering is considered a serious aggravating factor, there are very few cases where money laundering conviction has been obtained as a result of an Inland Revenue investigation into tax crimes. However, the authorities consider that the act of laundering the money in tax offences, occurs mostly as part of the predicate offence rather than in a discrete phase, particularly when these matters involve pure self-laundering (for example businesses not declaring cash revenue) and generally do not

include a discrete ML component. In such cases civil penalties are sufficient to address the offending. Inland Revenue runs an internal committee to review every criminal case to determine if there is an ML offence to pursue. A ML charge is considered (or other criminal justice measures pursued where ML convictions are not possible to secure) where there is a high degree of sophistication in the tax offending or discrete steps taken to launder proceeds. Operation Masala (Box 3.5) is a case where prosecution was pursued in addition to recovering the proceeds of crime.

Box 3.5. Operation Masala

In early 2012, IRD commenced a comprehensive audit into the financial affairs of a chain of restaurants. Members of the family that controlled the restaurant were found to be engaging in wide spread tax evasion of over NZD 700 000 and laundering of the money over 6 years and 17 different companies. NZD 8 million was forfeited from the sale of property. In 2020, the main offender pleaded guilty to 34 charges of tax evasion and 9 charges of money-laundering and was sentenced to 3 years' and 2 months' imprisonment. His accountant pleaded guilty to 9 charges of money-laundering and was sentenced to 10 months' home detention. The principal offender's partner was sentenced to 9 months' home detention for her part in concealing NZD 6.5 million in cash sales.

Prosecution of Money Laundering Offences

200. New Zealand authorities undertake parallel financial investigations of criminal networks to understand the role of individuals within the criminal enterprise and the location of proceeds of crime. Police and other law enforcement agencies are focussed on responding to criminal threats and disrupting organised criminal activity, and conduct financial investigations to support those objectives, including investigations and prosecution of money laundering activity, some of which represent sophisticated money laundering or laundering by third-parties and gatekeepers.

201. Case studies show that financial investigations are more frequently used to support restraint and recovery of assets, alongside prosecution for the predicate offence, as compared to supporting prosecution on money laundering charges. There seems to be a difference between the extent to which there are investigations of money laundering activity (which is largely consistent with New Zealand's risk profile), and the extent to which there are prosecutions for money laundering offences, with a higher than expected number of ML investigations not proceeding to prosecution.

202. In some cases, money laundering activity was investigated and evidence gathered about this activity was used to support the prosecution of the predicate offence as well as in asset recovery, but the authorities decided not to prosecute money laundering charges. The Yan case is an example where prosecution was not pursued against professionals and other third parties who were involved in the laundering the proceeds of crime - although in that case this was largely because of evidential deficiency and the practical difficulty in securing adequate evidence on offending that took place in another country, two decades earlier, from hostile and/or dead witnesses. Nevertheless, that case did result in recovery of significant proceeds, as set out below in Box 3.10, under IO8. Authorities noted that differences in the applicable standards

of proof mean there are also cases where it is possible to recover proceeds of crime (which require a civil standard of proof), but not to proceed with a money laundering prosecution (which requires a criminal standard of proof).

203. In New Zealand, the choice of charges to be preferred is largely left to the Crown Prosecutors, who make the decision based on a range of considerations under the Solicitor-General's Prosecution Guidelines, which are broadly categorised as evidential sufficiency test and public interest test. Under the Solicitor-General's guidelines, charges are expected to reflect the criminality of the defendant's alleged conduct which has historically often resulted in the more serious predicate offence being charged rather than money laundering. The Solicitor General's Prosecution Guidelines sets out the expectation that the prosecutor should take into account the resources spent on prosecuting multiple charges and defendants in proportion to the seriousness of the offending and any likely sentence so as to strike a balance between effective and dissuasive prosecutions and over-burdening the court system. For self-laundering cases in particular - where the facts are the same for the ML and the predicate offences, the conviction of the predicate offence is able to attract a high sentence, and where consideration of the ML conduct leads to uplift in the predicate sentence - not pursuing the money laundering charge is considered to be a pragmatic approach to prosecution on the ground as it may provide little additional benefit for either sentencing or asset recovery.

204. Some law enforcement officers reflected a reluctance to expend resources to pursuing money laundering prosecutions where a conviction for the predicate offences and/or the confiscation of large sums of criminal proceeds were considered to be sufficiently dissuasive. However, this view is not shared by specialist units tasked with ML investigation. This may indicate that awareness of the 2014-17 changes has not yet reached all parts of the police. While statistics reflect that the high level policies have worked to increase prosecution of ML, New Zealand should continue to reach out to the operational officers conducting investigations to increase their understanding and appreciation of the importance of pursuing ML charges in addition to asset recovery so as to ensure that the current trajectory is sustained.

205. New Zealand authorities consider that disruption of criminal activities through the pursuit of the predicate offence as well as the proceeds of crime provides a pragmatic response against the criminal threat but have recognised the danger that this leads to an emphasis by investigators on asset recovery over money laundering, and insufficient emphasis on the prosecution of third party money launderers who are not linked to a predicate offence. There has been a sustained strategic push to mitigate this risk since 2014-15. Since the creation of MLTs in 2017 and targeting of ML prosecution as a measurable strategic goal for Police, the situation has improved notably. As such, these initiatives to increase ML prosecution have been timely.

206. Table 3.6 below shows the significant increase in ML investigations as well as ML prosecutions (where ML charges were preferred) in 2018 and 2019 as compared with 2016-17. The impact of the 2014 legal and prosecution reforms was thus only visible from 2018 onwards.

Table 3.6. Resolutions/Status of ML Cases

Year ML Offence Occurred / Case Status	2016	2017	2018	2019	2020 (until March 2020)
Totals by Year					
Number of ML Case Files	31	33	79	137	45
Status of Case Files at the time of the Mutual Evaluation On-Site					
Investigations still ongoing	-	3	5	26	23
Investigation concluded – insufficient evidence to charge	4	8	6	6	3
Cases where ML charges laid and then not proceeded with	4	1	3	5	-
Cases where ML charges sub-judice	-	1	11	52	10
Cases where ML charges proceeded and resolved	9	6	41	15	4
Total ML cases proceeded to trial	9	7	52	67	14

207. In order to sustain this positive trend in pursuing ML prosecutions in the longer term, NZ authorities should further sensitise LEAs and Crown Prosecutors to the high-level policy and operational strategies which emphasise the role of prosecution for money laundering offences as a tool to disrupt transnational drug distribution networks, overseas criminal organisations, and dedicated ML networks; and combat the abuse of trust and shell companies in NZ. LEAs on the ground should be familiar with the ML prosecution goals and policy in the same way as they are familiar with NZ's asset recovery targets and policy. In light of NZ's framework where prosecutions are conducted by Crown Prosecutors from private law firms, it is crucial for NZ authorities to communicate and reinforce the public interest in pursuing money laundering prosecutions to the Crown Prosecutors. This could be by developing guidelines on money laundering prosecutions, which would supplement the Solicitor-General's Prosecution Guidelines, as well as other forms of appropriate outreach activities.

Types of ML cases pursued

208. New Zealand authorities have demonstrated that they are able to prosecute and obtain convictions for a range of money laundering cases, including stand-alone and self-laundering, third-party laundering and the laundering of foreign predicates. New Zealand has also demonstrated that it has capability to investigate complex multi-jurisdictional money laundering supported by bilateral agreements. The assessment team based these conclusions on a wide range of case studies presented by New Zealand, which set out the investigation, prosecution and conviction of various types of money laundering, and through discussions with the LEAs. Key cases are set out in boxes below and throughout this chapter which illustrate New Zealand authorities' capacity to investigate and prosecute different types of money laundering. Several of the cases noted in this chapter demonstrate the capacity to *investigate* the relevant type of money laundering activity, even in the absence of a prosecution for the ML offence.

Table 3.7. Money Laundering Prosecutions by Type of Offender

Year ML Offence Occurred / Offender Type	2016	2017	2018	2019	2020 (until March 2020)
Self Laundering					
Individuals Charged with ML	6	7	23	76	8
Counts of ML Laid	7	14	26	153	8
Third Party Laundering					
Individuals Charged with ML	2	9	27	18	1
Counts of ML Laid	3	40	45	77	1
Money Laundering where it is unknown/unclear whether self laundering or third party					
Individuals Charged with ML	1	1	20	6	1
Counts of ML Laid	1	2	23	9	1
Money Laundering by Unwitting Mules					
Persons formally warned in writing for ML	4	-	2	10	1
Persons formally warned verbally for ML	-	2	2	16	3

Box 3.6. Operation Nova
(Complex Money Laundering network organised by gatekeeper professions)

Operation Nova was a 2018 investigation of the Comanchero Outlaw Motorcycle Gang, which uncovered a sophisticated money laundering operation. The gang was developed by deportees from Australia with links to transnational organised crime networks.

Over the course of the investigation, various trusts and businesses linked to the offenders were established to facilitate money laundering required to introduce cash into the legitimate financial system, which in turn enabled them to undertake large financial transactions including the purchase of property and vehicles. During the course of the investigation the Financial Intelligence Unit (FIU) disseminated 83 distinct reports detailing approximately 100 Suspicious Activity Reports to the investigation team, which assisted with identification of the financial networks facilitating the drug offending and subsequent laundering of criminal proceeds.

This was a complex financial investigation with the analysis undertaken by an ARU accountant which reconstructed financial activities across 131 separate bank accounts involving approx. 100 000 relevant individual transactions. This reconstruction identified the association of

those charged along with the Trusts and Companies involved in the offending. Investigative techniques involved physical and electronic surveillance. Foreign law enforcement partners involved in this investigation included Australian Federal Police, Australian Criminal Intelligence Commission, New South Wales Police, The US Drug Enforcement Agency, Dept. of Homeland Security, Fiji Police, Interpol, Canadian Boarder Services Agency, Interpol, and Australian Transaction Reports and Analysis Centre (Australian FIU) Consequently, all the Comanchero Outlaw Motorcycle Gang Office-holders and a number of associates were taken into custody.

Key facilitators including a lawyer and an accountant were arrested and prosecuted, seriously impacting the offenders' ability to further integrate proceeds of crime into the legitimate financial system where they could enjoy its full benefits.

NZD 3.7 million worth of assets were seized which included luxury vehicles and jewellery. Eight individuals were arrested including the vice president of the motorcycle gang who was sentenced to 4 years' and 8 months' imprisonment. The group's lawyer who was a key facilitator in laundering the money faced 13 money laundering charges and was sentenced to 2 years' and 9 months' imprisonment in February 2020.

Box 3.7. Operation Heracles *(3rd party money laundering)*

A Joint-National Organised Crime Group and Customs investigation was conducted that centred on a group of individuals associated with the importation and supply of cocaine in New Zealand. The investigation team identified that the group had used a number of third parties to assist with money laundering activities in New Zealand.

Investigative techniques included a surveillance device warrant, full analysis of bank records, investigation of substantial cash purchases, investigation regarding the purchase of high end assets, analysis of betting accounts, and liaison with Auckland casino. A mutual assistance request, as well as an Egmont request were made regarding assets located abroad. Customs also co-operated with the Australian Department of Immigration and Border Protection. The Financial Intelligence Unit assisted with facilitating Egmont exchanges, and disseminated three reports to the investigation team, containing details of Suspicious Activity Reporting.

As a result of this operation, four individuals were charged with drug offences and two were sentenced for money laundering only, one of the third party money launderers was successfully extradited to face prosecution. The four individuals were sentenced to imprisonment in February 2020 for terms ranging from 14 to 27 years, including uplifts for ML activity. The sentences for the ML charges ranged from 3 years to 5 years and 6 months.

209. New Zealand has successfully prosecuted complex money laundering cases involving complex money laundering networks, professional facilitators, foreign predicate offences, third-party money laundering, and stand-alone money laundering. The overall rate and nature of money laundering prosecutions are broadly consistent with New Zealand's risk profile.

Effectiveness, proportionality and dissuasiveness of sanctions

210. In New Zealand, money laundering is punishable by up to seven years' imprisonment, and the offence of obtaining or possessing property with intent to engage in money laundering is punishable by up to five years' imprisonment (s 243(2) and (3) of the Crimes Act). Under s 39(1) of the Sentencing Act 2002, the courts may impose a fine instead of imprisonment.

211. The maximum sentence prescribed for ML is proportionate to other economic crimes in line with that for fraud (7 years imprisonment), bribery (7 years), obtaining by deception (7 years), or false promotion (10 years). The New Zealand Court of Appeal has held that individuals who launder money for drug dealers are nearly as culpable in the eyes of the law as those who participate directly in the drug distribution. However, if the act of obtaining and concealing the funds is the same, then the courts have also relayed messages that discourages pursuing of both money laundering and predicate charges for such self-laundering type cases.

212. New Zealand courts determine the appropriate sentence based on the individual facts of the case, considering both the seriousness of the offending and the circumstances of the offender. Particularly in cases of self-laundering, when the ML offence is co-penalised with the predicate offence, a single sentence is applied reflecting both the predicate and ML offences, with the ML offence considered as an aggravating factor when considering the appropriate tariff based on guidelines for the predicate offence. Judges determine sentences based on a wide range of elements relevant to each individual case, and do not always record what effect the ML activity specifically has on the final penalty. For such cases, it is therefore not always clear the extent to which conviction for ML leads to an additional sanction.

Table 3.8. Sentences Imposed for Money Laundering Offences

Year ML Offence Occurred [9] / Sentence Type	2015	2016	2017	2018	2019	Total
Custodial Sentences						
Imprisonment	2	5	7	16	16	46
Home Detention	4	2	3	9	2	20
Community Detention	-	-	2	4	-	6
Non-Custodial Sentences						
Intensive Supervision	-	-	-	15	2	17

9 The year recorded is the year the ML offences were committed. This is not the year the conviction was obtained and/or the year the sentence was imposed.

Year ML Offence Occurred [9] / Sentence Type	2015	2016	2017	2018	2019	Total
Community Work [10]	1	1	3	18	2	25
Fines/Reparations [10]	-	1	1	19	3	24

Table 3.9. Length of Custodial (prison) sentence imposed for Money Laundering Offences

Custodial (prison) sentences by length for ML charges	2012	2013	2014	2015	2016	2017	2018	2019	Total
0 – 12 months	0	0	0	0	1 case	1 case	8 cases	14 cases	24
13 – 24 months	1 case	0	2 cases	2 cases	2 cases	1 case	5 cases	0	13
25 – 36 months	2 cases	0	0	0	1 case	2 cases	0	1 case	6
37 – 48 months	0	0	0	0	1 case	1 case	2 cases	0	4
> 48 months	1 case	0	0	0	0	2 cases	1 case	1 case	5

213. The range of sentences passed for money laundering prosecutions have included both custodial involving prison sentences and non-custodial options. Sentences that do not involve imprisonment such as community work, home detention, intensive supervision and fines are not uncommon and a significant proportion of sentences for ML are non-prison sentences. The penalties applied for serious ML cases do include custodial sentences for several years. Several cases above illustrate comparatively light sentences given to convicted money launderers, including Operation Masala, and Operation Manuka (Box 3.7). One third of ML convictions result in imprisonment, with half of those sentences for a term of 12 months or less (although this may to some extent reflect a peak in conviction of lower-end money mules relating to offending in 2019, while the more complex cases for 2019 remained sub judice at the time of the onsite). To a large extent this reflects the fact that serious stand-alone money laundering is infrequent in New Zealand, and that money laundering is more frequently co-penalised with the predicate offending. Overall the penalties applied for ML offences are consistent with New Zealand's ML risk profile and with its wider criminal justice system.

214. New Zealand ML investigations routinely include legal persons. The prosecution may not have evidence to establish that the legal person possessed the necessary mens rea to commit ML (e.g. if the legal persons are used in facilitation of ML rather than committing ML themselves). Where shell companies are implicated in ML schemes, New Zealand pursues alternative criminal justice outcomes such as restraint of assets, including proceeds of crime and businesses. Deregistration can also be used where the Registrar has reasonable grounds to believe that the company is not carrying on

10 The majority of community work sentences (76%) and orders for fines/reparations (92%) are imposed as a component within a package of sentencing. For example, a sentence imposed for an ML offence committed in 2018 included 12 months intensive supervision, 200 hours of community work and a reparations order of NZD 5 909.

business and there is no proper reason for the company to continue in existence. See for example the Taylor group of companies where the Registrar received intelligence relating to a group of companies, as result of some companies being implicated in ML and other criminal activity by FIU intelligence (see IO5 para 474), and ultimately determined that it was appropriate to exercise its deregistration powers in respect of approximately 1850 companies. In 2008 a company was prosecuted for various ML charges under the Crimes Act and the court imposed a fine approximately 3 to 4 times the gains the company made, under the Sentencing Act. There have been no further prosecutions and conviction of a legal person for money laundering since this case, so it is not possible to determine the sanctions applied to legal persons under the Crimes Act.

Alternative Measures

215. Where there are challenges to obtaining a conviction for money laundering, New Zealand authorities use various tools to disrupt and sanction money laundering activity, including through the pursuit of alternative offences where possible, as well as pursuit of criminal assets, tax investigations, and deregistration of companies.

216. New Zealand makes full and effective use of the range of asset recovery tools available under its Criminal Proceeds (Recovery) Act, which is set out in more detail under IO8, below. The pursuit and recovery of criminal proceeds is one of the key targets for the New Zealand Police and an essential element of their strategy to disrupt organised crime and make New Zealand safe. The Inland Revenue also makes significant use of its civil (monetary penalty) regime to pursue proceeds in cases where it is difficult to establish a criminal tax offence to a criminal level of proof. While there is evidence that this has a significant dissuasive and disruptive effect, confiscation is not generally accepted as an alternative to money laundering prosecution and has not been considered so for the purposes of this evaluation.

Overall Conclusions on IO.7

217. New Zealand has demonstrated that it has the capacity to investigate, prosecute, and obtain convictions for a range of money laundering cases, representing the main different proceeds-generating crimes, and including stand-alone and third-party money laundering, and the laundering of foreign proceeds, as well as complex money laundering operations.

218. The pursuit and recovery of criminal proceeds is one of the key targets for the New Zealand Police, and their strong investigative capacity for money laundering activity support this goal. However, based on case studies, it appears that the authorities' focus was often on the prosecution of predicate offences and the pursuit of the proceeds of crime to disrupt criminal activities, which has impacted the prosecution of money laundering cases overall. This was based on a pragmatic approach towards addressing ML activity particularly where New Zealand authorities faced difficulty of obtaining evidence.

219. However, developments after 2017, which include increased resourcing that went into the creation of dedicated MLTs, increased and dedicated training as well as setting goals for the prosecution of ML

activity have begun to show results where money laundering prosecutions have increased and is becoming a more important tool in response to serious crime. Statistics indicate that ML prosecution in 2018 and 2019 are promising, and consistent with New Zealand's ML risk profile, and this progress should be sustained for the long-term.

New Zealand has achieved a substantial level of effectiveness for IO.7.

Immediate Outcome 8 (Confiscation)

Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

220. Confiscation of proceeds and instrumentalities of crime is an important policy objective in New Zealand. The Police operational 'Our Business' strategy established in 2018 sets asset recovery as one of five top-level targets for policing, with a target volume of criminal assets to be restrained as NZD 500 million by 2021. The Police as an entire organisation are actively working to meet the target, which aims to focus police efforts on the financial facilitation of crime.

221. New Zealand's civil forfeiture regime is considered to be an integral part of its crime disruption strategy that aims at making New Zealand an unattractive place for money laundering and the hardest place for criminals to undertake business. The deterrent and preventive effect of confiscation, by visibly recovering the proceeds of illegal acts, and making sure crime is seen not to pay, are well-recognised and thus confiscation is a central feature of the New Zealand '*Prevention First*' Strategy.

222. New Zealand's Criminal Proceeds (Recovery) Act (CPRA) is the key legislation underlying the civil forfeiture regime and it provides an effective framework to detect and trace criminal proceeds as well as property of equivalent value through profit forfeiture orders. Criminal conviction is not required for asset forfeiture, as the standard of proof for forfeiture is conducted based on the balance of probabilities (as opposed to 'beyond reasonable doubt') that the asset is related to significant criminal activity or that an individual has benefited from crime.

223. New Zealand's policy and strategic objectives to actively pursue criminal proceeds are operationalised by the Asset Recovery Units (ARUs), specialised units which works across Police operations to initiate parallel restraint and forfeiture proceedings alongside criminal investigations undertaken by police and other LEAs. The ARUs can also initiate proceedings outside the context of a criminal investigation. The ARUs are based in the four regional centres of Auckland, Hamilton, Wellington, and Christchurch to provide national coverage.

224. On average, 95 asset recovery cases are opened each year. The total volume of assets restrained in 2015 - April 2020 was approximately NZD 597 million. When compared to the estimated volume of criminal proceeds laundered per year in New Zealand, indicated in the NRA, the restraint rate is approximately 8% of an annual volume of criminal proceeds (NZD 1.35 billion, based on an average value of NZD 113.5 million restrained per year). Even taking into account some amount of imprecision, this criminal asset restraint rate is impressive for a recognised small low crime jurisdiction

and in comparison with the estimated global average of 2.2% of criminal proceeds frozen or restrained.

225. About 30% of assets restrained were forfeited. This is partially explained by the length of time of confiscation proceedings which can take on 2 years on average. However, the time taken can range widely from multi-year proceedings for complex cases to shorter time periods for others. The percentage of restraint action that was abandoned after having restrained the assets was only 0.33% which is very low.

226. New Zealand's Sentencing Act also includes provisions for forfeiture of instrumentalities of crime in the context of a criminal conviction. This tool is a central element of the sentencing regime. New Zealand provided a number of cases with confiscation of instrumentalities – mostly vehicles and residential property used for production/concealment/transportation of drugs.

Table 3.10. Total Value of Assets Taken from Criminals (in million NZD)[11]

Amounts in NZD	2015 - 2016	2016 - 2017	2017 - 2018	2018 - 2019	2019 - 2020	Total
Proceeds Restrained	104	119	64	79	231	597
Proceeds Forfeited	16	78	27	27	23	171
Instrumentalities	0.2	0.3	0.9	0.9	0.2	2.43
Restraint abandoned	0.445	0.42	0.474	0.517	0.265	2.123

How do authorities decide, at the outset of a criminal investigation, to commence a financial investigation, with a view to confiscation

227. If a criminal investigation involves criminal proceeds, law enforcement authorities refer the case to the ARU. The ARU does not require that a prosecution has been commenced. The ARU mostly receives referrals in two types of cases: suspected criminal activity from which proceeds may be generated or accumulation of property in apparent conflict with their known legitimate income. Investigations into the unexplained income can be initiated when there is an identified discrepancy with wealth and tax information however to achieve forfeiture, the income must ultimately be evidenced to have been derived from crime (to a civil standards).

228. ARU referrals and their quality are increasing as a result of training and awareness raising measures across police and other government agencies. Also, unlike past referrals which involved mostly low-value proceeds of crime which were spent by criminals on consumables, the referral to ARU increasingly relate to high value investments such as property in alignment with a response to risk. Generally, the number of asset recovery cases are growing.

229. All agencies involved in detection and investigation of ML/TF undertake efforts to build awareness of the importance of asset forfeiture work, and the strategic and tactical components required to effectively operate. There are regular training courses

11 Almost the whole volume of proceeds is forfeited under the CPRA regime, however Table 3.10 also includes proceeds confiscated under the Misuse of Drugs Act (although its volume is insignificant). Fines, restitution to victims and other payments are made out of forfeited assets.

covering asset trace, seizure and confiscation attended by Police, ARU staff, Crown Solicitors, IR and Customs staff.

230. With respect to resourcing, the ARU teams comprise 80 employees, including accountants, analysists and investigators. Accountants and analysts are attached to each of the regional ARUs teams. The usual structure of an ARU team is a supervisor (Detective Sergeant), 3-4 Investigators, and 2 accountants / analysts. The IR has approximately 710 staff directly involved in tax related financial investigations. Customs has established a dedicated Financial Crime Unit that focuses on investigating financial components of predicate offence and ML offences at the border (with 10 staff).

231. New Zealand has a sophisticated and effective asset management system managed by the Official Assignee (OA) that works well to maintain the value of assets seized. Professional consultants and liquidators are hired for management and realisation of complex assets, such as businesses and shares. Seized cash and funds allocated on bank accounts are deposited into a trust account administered by the OA. The OA is currently updating its Standard Operating Procedures to cover issues related to seizure and confiscation of virtual assets which are the subject of ARU investigations.

232. The value of property sold by the Official Assignee in satisfaction of orders in 2015-2020 is NZD 191 million, which is even higher than the total value of forfeiture orders issued. This was explained by the value appreciation of some assets (such as property) and also testament to the ability of the good work of the Official Assignee in asset preservation.

233. Confiscated assets are transferred to the Proceeds of Crime Fund. The Fund provides a funding pool from which Government agencies can bid for funding for initiatives outside of their normal annual budget. Initiative funded by the Proceeds of Crime Fund include those related to asset recovery framework, such as Expansion of Asset Recovery and Financial Investigations project, recovery of legal costs for civil recovery actions under the CPRA, Upstream Disruption Project by Customs, etc.

Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

234. New Zealand has demonstrated its successful implementation of its policy objectives on asset confiscation through statistical data and a range of cases. The cases reflect that the New Zealand authorities focus strongly on detection, seizure and confiscation of proceeds and instrumentalities related to various predicate offences.

235. Financial intelligence products that are disseminated by the FIU (including the Proactive Financial Targets list) as well as information obtained through ARU's direct access to goAML, are effectively used for detection of criminal accounts and assets subject to further restraint and confiscation. The ARU follows up with production orders to obtain information from financial institutions and have demonstrated their capability to use investigative tools to evidence beneficial ownership in an environment often challenged by legal privilege.

236. New Zealand authorities also pursue assets located abroad through using the mutual legal assistance process to register New Zealand order in foreign courts. New Zealand is active in the identification and tracking of assets through employing a range of international co-operation channels such as mutual legal assistance, Egmont, Interpol, ARIN-AP, and through New Zealand liaison officers stationed in countries of a strategic importance with regional responsibilities (Pacific and Asia, Europe and the United States) to collect information and co-operate with law-enforcement authorities

on specific issues. In some cases, such as Operation Manuka (see box 3.7, in IO7, above), the use of liaison officers was instrumental in obtaining information from abroad and ensuring seizure of assets in the United Kingdom, even when use of formal channels led to less effective outcomes.

237. With respect to tax offences, the IR can apply for freezing orders directly through the Crown Law Office, although the ARU remains responsible for seizing and confiscating assets in criminal tax matters. In practice, the ARU and IR collaborate closely to ensure that all sanctions are considered and relevant orders are sought at the appropriate time.

238. Confiscation of instrumentalities of crime is a part of the sentencing regime. Statistics provided by New Zealand reflects active measures on confiscation of instrumentalities of crime. The vast majority of confiscated instrumentalities are vehicles, residential property used for drugs transportation and production, and cash.

239. On the whole, New Zealand has effectively confiscated different types of assets, including residential and non-residential property, cash and bank accounts, shares and companies' assets, vehicles, etc. In accordance with statistics provided by the Official Assignee, currently there are about 2 000 assets under custody and control with a combined value of NZD 597 million, with 54% of them properties (orchards, residential and businesses properties), 41% in bank accounts, cash, shares, and cryptocurrency, and 4% as vehicles.

Box 3.8. Confiscation of virtual assets

New Zealand seized approximately NZD 23 million of virtual assets (including Bitcoin, Chainlink, and Pivx coins amongst others.) from an individual involved in selling illegally obtained copyrighted films and ML in New Zealand and the US. The investigation was triggered with the US IRS sent via the Egmont channel. New Zealand Police used production orders to banks on financial information and IP addresses, production orders on transport services, and covert surveillance. Restraining orders were obtained without notice to restrain funds in the bank account and virtual assets.

Confiscation related to foreign predicate offences and proceeds of crime moved to other countries

240. Where another jurisdiction is involved, New Zealand has demonstrated its willingness to co-operate to pursue assets and enter into asset sharing or repatriation arrangements in accordance with guidelines on asset sharing issued by the Attorney General's Office. New Zealand pursues proceeds generated through foreign predicate offending (see the Table below). New Zealand also actively pursues proceeds of crime located off shore when the opportunity presents.

241. The NRA defines the risk of laundering of proceeds of foreign predicate offences in New Zealand as 'high'. The risks are related to money laundering facilitated by New Zealand shell companies with bank accounts in Europe or offshore jurisdictions, often operated by a New Zealand TCSP, with the use of New Zealand financial system as a conduit and the use of New Zealand real estate. Although only a small number of cases

involve the laundering of proceeds of crime through real estate by overseas criminals, these are high-value cases, and the overall amount of proceeds involved is significant.

242. New Zealand shared 9 complex asset recovery cases between 2014 and 2020 relating to foreign predicate offences which present about 49% of all assets restrained (NZD 293 to 596 million). This is consistent with the level of risk. The assets restrained ranged from property, real estate, vehicles, shares, cash, bank accounts and cryptocurrency. New Zealand appears to be alive to the fact that it may be an attractive place for investment of laundered criminal proceeds from abroad, and should continue to focus on detection and seizure of proceeds of foreign predicate offences.

Box 3.9. Recovery of proceeds of foreign predicate offences

Operation Gone

Operation Gone is an investigation into an illegal Pyramid scheme in two countries where the proceeds were laundered through New Zealand (total volume of proceeds in New Zealand was approximately NZD 71 million).

Pursuant to a joint investigation with the foreign authorities, New Zealand Police have restrained assets, including property, cash, and vehicles of associates who assisted with the remittance of funds through New Zealand. The associates were convicted for offences under the AML/CFT Act for offences including failing to report suspicious transactions and structuring, and are awaiting sentencing.

Yan Case – Asset Sharing

Between 2012 and 2014, William Yan received significant sums of money that were proceeds of fraud, which was subsequently concealed in various ways, including transactions through a casino and third-party banking facilities including underground banks and correspondent banking. Legal persons and trusts were used to hide the identity of property whose legal beneficial ownership was traced to Yan. Other properties were placed in the names of family members and extensive investigative tools were used to prove that the beneficial ownership resided in Yan.

During this investigation 795 bank accounts were reviewed (of which over 400 related to offshore bank accounts); 74 assets were restrained; 313 court orders were obtained; 177 computers, phones and other data storage devices were seized for analysis; and 1329 additional physical exhibits were located and seized pursuant to a warrant.

In 2016, the Commissioner of Police was granted a forfeiture order against William Yan, in relation to offending related to the laundering of money from fraud committed overseas 17 years prior to the restraints proceedings being initiated.

In total, the forfeiture order against William Yan and two associates was NZD 42.85 million. NZD 27.85 million of this was repatriated (upon

Cabinet approval) to the country where the fraud took place. The remaining NZD 15 million was retained by New Zealand.

Yan was prosecuted for ML and sentenced to 5 months home detention to allow for Yan's voluntary return to China to face criminal charges in China with expediency and to avoid the need for an extradition process.

Vinnik case

Aleksander Vinnik was arrested on by the Greek authorities in 2017 at the request of the United States of America (US) for various money laundering associated charges. While he was then successfully extradited to France on unrelated money laundering offending but remains subject to an extradition request by the United States. Vinnik and his associated company formed in Seychelles operated a US based digital currency platform which conducted its business in the absence of any AML/CFT compliance, attracting criminals to the platform to launder illicit income derived from hacking, ransomware, fraud, identity theft, corruption and drug offending. Vinnik is also the subject New Zealand investigations given the involvement of a New Zealand formed company which was holding funds alleged to be owned by Vinnik.[12]

243. New Zealand demonstrated its willingness and ability to pursue proceeds of crime located offshore when opportunities present (e.g. Operation Manuka See Box 3.4 in IO7). Between 2016 and 2019, New Zealand made five asset restraint requests and two forfeiture requests to foreign jurisdictions (United Kingdom and Fiji), resulting in offshore assets worth NZD 8 615 000 being restrained and NZD 1 432 600 forfeited. New Zealand has also repatriated proceeds of crime outside of the formal asset forfeiture process. In one case in 2017, New Zealand repatriated NZD 12 866 310 from Hong Kong, China as part of a settlement order. At the time of the onsite, New Zealand also had an ongoing domestic action to restraint funds to the value of NZD 140 million to be repatriated to New Zealand from another overseas jurisdiction. No cases were identified where New Zealand authorities missed the opportunity to trace, seize and recover proceeds of domestic crimes moved abroad. However, without an estimate of the total potential volume of proceeds of domestic crime moved from New Zealand each year, it is not possible to assess the extent to which all related proceeds are identified and pursued.

Confiscation of falsely or undeclared cross-border transaction of currency/BNI

244. New Zealand recognises the importance of addressing falsely or undeclared cross-border transaction of currency and bearer negotiable instruments (BNI). The Customs' Statement of Intent 2019-2023 includes the goal that 'all non-compliance is addressed'.

245. The Customs authorities effectively detect non-declared cash. Customs has targeted passenger flows as the key mechanism for the transfer of cash across the border. There are very few instances detected of cash moving via unaccompanied goods (freight) or via the mail stream (either inwards or outwards). To ensure the risk

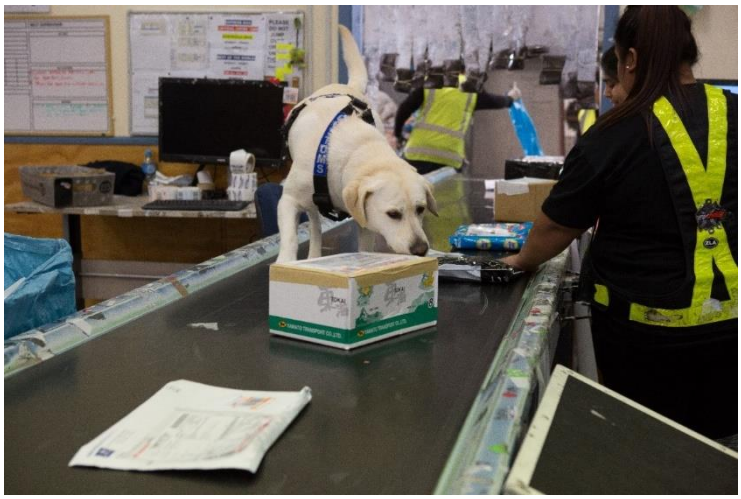
12 In April 2020, New Zealand Police restrained the equivalent of NZD140 million in various currency in an offshore bank account. The funds have been recovered to New Zealand and investigation are ongoing. This matter has been a complex multi-jurisdictional investigation involving co-operation with foreign counterparts.

remains low, Customs uses intelligence to deploy cash dogs to identified high-risk goods pathways for undeclared cash.

246. At New Zealand's international airports, Customs maintains a number of cash detector dogs that are regularly deployed to identify undeclared cash. Customs also regularly discover undeclared cash during baggage searches.

Photo: New Zealand Customs operates risk based screening of cargo, passengers, baggage and mail with cash detector dogs.

Here a cash detector dog screens incoming mail in the Auckland mail centre



247. New Zealand's border control partners also contribute to detecting undeclared cash. For example, where aviation security staff detect large amounts of cash during x-rays of hand luggage for outgoing passengers and MPI x-ray the luggage of arriving passengers, a Customs officer will be notified to take action.

248. With respect to bearer negotiable instruments, these do not currently appear to be a major money laundering risk in the New Zealand border context.

249. New Zealand is developing a systemic response to major/emerging risks related to cash smuggling. For example, Customs is working to build more international connections with its major trading partners as well as comprehensive matching of import and export records relating to the same transaction, in order to identify where trade-based money laundering may be occurring. Customs is also engaging with international partners to consider developing responses to emerging money laundering risks such as identification of stored value cards transiting the border.

The obligation to report the cross-border transportation of cash

250. Under the AML/CFT Act, any person carrying NZD 10 000 or more in cash or BNI must complete a 'border cash report' (BCRs) on arrival or departure and present that form to a Customs officer. The completed BCRs are collected by Customs officers at airports and other ports of entry or departure and forwarded to the FIU for collation and analysis. Currently, the forms are filled in on paper and then manually retyped into the FIU database. Customs intends to have an electronic system for BCRs launched by the end of 2020 (though it depends on the required legislative changes).

Table 3.11. Completed BCRs from 2016 to 2019 by Direction of Travel

Year	BCRs Completed on Arrival	BCRs Completed on Departure	Direction of Travel Not Recorded	Total
2016	3 817	1 196	373	5 386
2017	3 877	870	286	5 033
2018	4 850	815	206	5 871
2019	4 524	951	58	5 533
Total	17 068	3 832	923	21 823

Response to undeclared or mis-declared cash

251. Under New Zealand legislation, undeclared cash that is imported (or exported) becomes a prohibited good that is subject to seizure and the non-declaration is an offence. Customs officers have the powers to investigate further and have used this in collaboration with Police, IR and ARU to uncover the commission of other offences, such as drug trafficking, tax offences as well as including money-laundering offences. For example, in 2019, approximately NZD 160 000 was seized from two departing foreign nationals who failed to declare the cash on departure. Their claim that the cash was proceeds from their bakery was investigated together with the FIU and IR. However, between 2015 and 2019, only one money laundering prosecution was initiated. While Customs considers money laundering charges in all applicable cases, the focus appears to be on the predicate offences (which normally carry higher maximum penalties).

252. Where non-declaration is not related to further offences, Customs officers are guided by a clear algorithm and questioning guideline to decide whether the non-declaration is bona-fide and options to proceed, including written warning, seizure, summary compositions and prosecution. The vast majority of cases were considered bona-fide, and no seizures were applied and prosecutions are rare.

253. Generally, only a small proportion of non-declared cash is confiscated. In 2019, 611 cases of undeclared cash were detected (NZD 11 million). Out of these, 64 were warned and 84 were issued summary compositions (NZD 18 950). One prosecution resulted in a court imposed fine of NZD 2 000. Only in ten of these cases were there seizures (amounting to NZD 741 000). New Zealand authorities explained that the low confiscation was due to the fact that in most cases, the traveller had a reasonable excuse (such as misunderstanding of the requirements or language difficulty). The table below shows that there is an upward trend in the volume of seizures due to multiagency operations against cash smugglers and cash controller networks (from 2 seizures of total volume of NZD 69 000 in 2016 to 16 seizures of NZD 940 000 in 2020).

Table 3.12. Cash Seizures

Year	Amount of Undeclared Cash (in NZD)	Number of Seizures
2016	69 500	2
2017	72 700	1
2018	126 500	4
2019	740 900	10
2020	940 500	16
Total	1 950 100	33

254. The low proportion of confiscation of non-declared cash and the predominant application of low summary compositions raises concerns as to whether the proportionate and dissuasive sanctions are being applied. Having said that, it is recognised that cash smuggling is not the most preferred method of illicit transnational cash movement in New Zealand and is not a significant risk for New Zealand.

255. Customs information and alerts are shared with both domestic enforcement authorities as well as foreign customs authorities. BCRs are submitted manually to the FIU. They are entered into a spreadsheet and 'non-compliant' (i.e. where Customs have caught a person at the border with cash) BCR's are entered into goAML. Checks of BCRs are made against customs' intelligence indices and any additional information relevant to suspicious or unusual reports is provided to the Police. Customs intelligence analysts who evaluate reports from frontline Customs officers may also proactively advise the FIU of any incident of interest involving border cash reporting or cash/liquid asset movements by way of a Tactical Intelligence Report.

256. Customs uses a range of co-operative arrangements with other customs administrations, particularly its key trade and regional partners (including Australia, Canada, Chile, China, Fiji, Hong Kong, Japan, Korea, Thailand, United Kingdom and the United States). These MOUs typically include provisions relating to the exchange of information on matters of common interest including, as appropriate, money laundering and the cross-border movement of cash and other liquid valuables. In addition, Customs has liaison officers posted in in United Kingdom, Belgium, Thailand, Indonesia, Hong Kong, China, Australia and the United States. A Pacific Liaison Officer also covers co-operation with the Pacific customs administrations. These liaison officers assist Customs to identify and co-operate with equivalent agencies and build up the necessary relationships to ensure such co-operation works effectively.

257. Customs also identifies potentially suspicious activities to pass to its partners overseas (see case studies below). These types of joint investigations, particularly around TBML are likely to increase as Customs expands its financial investigation capability and as more integrated data sharing mechanisms come online.

Box 3.10. Large cash holdings into New Zealand

An Australian resident piloted his own plane into Queenstown. It was discovered that he had a large quantity of cash on the plane that he had not declared. He was under the misapprehension that he did not need to declare it if it stayed on the plane (and therefore left New Zealand with him when he departed). While there was no concern identified about the nature of the cash and why he was carrying it, Customs informed the Australian Border Force (after he left New Zealand) that he was carrying a large amount of cash in the plane to allow them to investigate and question him further.

Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

258. New Zealand demonstrated its ability to recover assets in a range of predicate offences consistent with its national priorities and risk profile. The majority of seizures and confiscations relate to money laundering, drug trafficking, fraud and tax crime as identified in the NRA as being the predicate offences that generate the most criminal proceeds. About 86% of asset recovery cases (70% - by estimated case value) are related to drugs, gangs and organised crime.

Table 3.13. Restraints by Offence (in million NZD)

Main Offence	2015 - 2016	2016 - 2017	2017 - 2018	2018 - 2019	2019 - 2020
Money Laundering	19 570	71 270	11 330	20 970	152 230
Drugs	34 510	40 600	27 830	23 160	34 290
Fraud	5 460	3 810	16 130	`23 590	18 870
Tax Crime	43 640	-	9 340	11 630	2 450
Other Offences	2 850	0 280	0 620	0 520	22 900

259. With regards to asset recovery, out of NZD 125 million forfeited since 2016, approximately NZD 57 million (47%) related to drug offences, NZD 50 million (41%) – fraud and NZD 14 million (11%) – to tax offences.

260. The data also shows that the most of assets recovered related to government priorities in respect of disrupting organised crime networks and drug distribution.

Table 3.14. Asset Recovery Linked to Drugs, Gangs and Organised Crime

By Case Count	86%
By Estimated Case Value	70%
By Current Restraints	61%

Overall Conclusions on IO.8

261. New Zealand pursues recovery of criminal proceeds, instrumentalities and property of an equivalent value as a policy objective and a high-priority. The ARUs have demonstrated their strong capabilities in pursuing tainted assets (direct proceeds of crime), benefits from crime (equivalent value), and instruments of crime. Both statistics and case studies reflect a strong commitment to asset recovery, with various types of assets related to main criminal offences confiscated. The value of assets recovered in relation to foreign predicate offences represent a significant percentage of the total value. New Zealand has a sophisticated and effective asset management system to maintain the value of assets seized. Customs effectively detect non-declared cash at international borders and appropriately follow-up with investigations into potential underlying criminal activity and money laundering. However, measured to address non-declared cash at the borders do not appear to be dissuasive. Nevertheless, this is not a major shortcoming in light of New Zealand's risk profile. It is therefore concluded that New Zealand produce confiscation results that are consistent with the NRA to a very large extent.

New Zealand is rated as having a high level of effectiveness for IO.8.

Chapter 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

a) New Zealand has investigated possible terrorism financing in relation to the Christchurch attacks, and authorities use financial intelligence when investigating cases with a connection to terrorism (e.g. the publication of objectionable material about terrorist acts online). New Zealand has not prosecuted any terrorism financing cases to date, which appears to be consistent with its risk profile as articulated in its national risk assessment.

b) New Zealand has dedicated resources with responsibility for monitoring possible terrorism financing within the FIU and in the National Security Group (NSG) of the New Zealand Police. There is strong co-operation and co-ordination between the NSG, FCG (including the FIU) and other relevant agencies, and the NSG draws on financial investigation expertise from within the FCG as required.

c) The New Zealand Police, which are responsible for terrorism financing investigations, have established standard operating procedures for managing terrorism financing investigations.

d) Following the Christchurch attacks, the New Zealand Police and other government agencies demonstrated their capacity and effectiveness in undertaking and supporting terrorism financing investigations, consistent with the standard operating procedures, and through extensive and timely international co-operation.

e) New Zealand took active steps to understand its TF risk exposure following the emergence of the foreign terrorist fighter threat, and took steps commensurate with these risks, including to improve co-ordination among relevant agencies.

f) New Zealand has an established governance framework for inter-agency strategic co-ordination on counter-terrorism and AML/CFT more broadly.

Immediate Outcome 10

a) New Zealand has a strong legislative framework for the implementation of TFS without delay, including giving immediate and automatic effect to UN Security Council designations under New Zealand law.

b) New Zealand has made active use of designations by the Prime Minister pursuant to New Zealand's implementation of UNSCR 1373 in the Terrorism Suppression Act 2002 (TSA) in relation to global and regional organisations, but at the time of the on-site visit had not designated any individuals, due to a number of factors, including that associated individuals were considered to be automatically subject to TFS by virtue of their association with designated entities. The effectiveness of this approach depended on the level of sophistication of TFS implementation by reporting entities, which in practice varied significantly.

c) Notification of updates to counter-terrorism TFS lists is done via goAML in a timely manner, but only reaches reporting entities which are registered on goAML (see IO.6 for details on reporting entity registration with goAML). At the time of the on-site visit, the remainder, mainly DNFBPs, did not receive notification of updates to counter-terrorism TFS lists.

d) Reporting entities appear to have variable understanding of TFS due to limited guidance and outreach by relevant authorities, as well as the lack of a mandate for supervisors to undertake supervision of reporting entities for TFS implementation.

e) In its supervision of registered charities, ML/TF compliance is one of the priority areas for Charities Services. However, there remains a small portion of NPOs that are not registered of which authorities have limited visibility.

f) No assets have been frozen in New Zealand pursuant to its TFS regimes. While this may be consistent with New Zealand's terrorism financing risk profile, it is not possible to confirm this in the absence of other measures that might provide some assurance about effective TFS implementation, i.e. the limited TFS guidance, and the lack of outreach to and supervision of reporting entities for TFS.

Immediate Outcome 11

a) New Zealand implements counter-proliferation TFS without delay. However there are deficiencies, including a lack of mechanism for communicating new designations or changes in designations to reporting entities, and no requirement to report freezing actions taken under the Iran and DPRK Regulations. While no assets have been frozen nor any TFS cases identified, authorities have prosecuted a contravention of export restrictions under UNSC DPRK sanctions.

b) At the time of the on-site visit, there was no process in operation to notify reporting entities of updates to Iran and DPRK TFS lists, through goAML or otherwise.

c) The variable understanding of TFS by reporting entities and the lack of supervision also lessened the impact of measures implemented in response to older cases of proliferation connected to New Zealand, i.e. the resident director requirement.

Recommended Actions

Immediate Outcome 9

a) Authorities should continue to work through the Counter-Terrorism Co-ordination Committee, the AML/CFT Co-ordination Committee and another appropriate mechanisms to respond to new and emerging TF risks faced by New Zealand and drawing on the operational experiences of the Christchurch investigation.

b) Authorities should ensure that prosecutors have the required legislative tools to prosecute terrorism financing in all instances, particularly in relation to financing individuals who travel to a state other than their state of residence for purposes related to terrorist acts or providing or receiving terrorist training.

c) The New Zealand Police should continue to build on its efforts to develop the understanding of financial intelligence relating to terrorist financing within the National Security Group of the New Zealand Police.

Immediate Outcome 10

a) Competent authorities should work to ensure all reporting entities receive timely updates to counter-terrorism financing sanctions designations.

b) An appropriate agency or agencies should be given clear powers and mandate to supervise and enforce counter-terrorism financing TFS obligations, including establishing clear supervisory expectations for preventive measures to avoid TFS contraventions (e.g. timing and frequency of customer and transaction screening) and conducting outreach to reporting entities about these expectations.

c) New Zealand should continue to build on its already active use of UNSC Resolution 1373 designations under the TSA and consider designating further terrorist entities in line with risks identified in the National Risk Assessment.

d) As part of future reforms to the TSA, New Zealand should address technical compliance shortcomings related to TFS authorisations (see Recommendation 6) to mitigate the possibility of these being misused in future.

e) New Zealand should consider options to increase monitoring or supervision of those charities identified as having a moderate vulnerability to abuse for terrorism financing under the NRA.

Immediate Outcome 11

a) Competent authorities should work to ensure all reporting entities receive timely updates to counter-proliferation financing sanctions designations from an appropriate authority.

b) An appropriate agency or agencies should be given clear powers and mandate to supervise and enforce counter-proliferation TFS obligations including, establishing clear supervisory expectations for preventive measures to avoid TFS contraventions (e.g. timing and frequency of customer and transaction screening) and conducting outreach to reporting entities about these expectations. In addition to high-risk financial institutions, supervision should prioritise other high-risk reporting entities identified through the planned proliferation financing risk assessment.

c) New Zealand is encouraged to complete its planned work to assess its risk of proliferation financing, including engagement with the Counter-Proliferation Forum as appropriate. Once completed, the outcomes should be used to target enhanced outreach on TFS obligations, the introduction of TFS supervision, and to inform whole-of-government co-ordination on counter-proliferation financing TFS.

d) New Zealand should ensure that outreach and guidance to reporting entities makes clear, the respective roles of the Police, MFAT and other agencies with respect to counter-terrorism and counter-proliferation TFS.

e) New Zealand should consider developing proliferation financing investigation SOPs along the lines of the TF investigation SOPs to support future investigations.

262. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39, and elements of R.2, 14, 15, 16, 32, 37, 38 and 40.

Immediate Outcome 9 (TF investigation and prosecution)

Prosecution/conviction of types of TF activity consistent with the country's risk-profile

263. Terrorism financing is criminalised under the Terrorism Suppression Act 2002 (TSA) broadly in line with international standards. New Zealand has not had any prosecutions for terrorism financing to date, but two prosecutions for terrorism offences had been initiated in advance of the onsite visit (the first following the terrorist attacks on the Christchurch mosques in March 2019, and a second in February 2020). At the time of the onsite visit these cases were not concluded, and one case was

subject to suppression orders.[13] The Christchurch investigation included investigation of TF but the terrorist attacks were found to be entirely self-funded. The level of investigations and prosecutions appears to be consistent with New Zealand's terrorism financing risk profile as articulated in its National Risk Assessment.

264. New Zealand has a reasonable understanding of its terrorism financing risk. While its National Risk Assessment (NRA) acknowledges that in New Zealand support for terrorist causes is low and that there is an absence of terrorist networks, it remains exposed to small scale and low value terrorist financing that may seek to abuse its vulnerabilities. Within the context of an overall lower terrorism financing risk, New Zealand's domestic risks relate primarily to lone actors for which self-funding is assessed as the likeliest means of finance. International risks include the risk of radicalised individuals in New Zealand providing support to overseas groups and the risk of traditional laundering by established networks through New Zealand's financial system and legal structures.

265. New Zealand's exposure to TF associated with foreign terrorist fighters is limited. A small number of individuals with New Zealand passports travelled to conflict zones, and these individuals have only limited ongoing connections to New Zealand. New Zealand does not publish statistics on foreign terrorist fighters; however, one case came to public prominence when the individual publicised his involvement in foreign terrorist fighter activities on social media.

TF identification and investigation

266. New Zealand has demonstrated a strong and effective operational capacity to investigate potential terrorism financing, as shown by the investigations following the Christchurch attacks.

267. New Zealand has dedicated resources within the Financial Intelligence Unit (FIU) (two analysts) and the National Security Group (NSG) of the New Zealand Police (one analyst) with responsibility for monitoring possible terrorism financing. The Police National Security Group has a dedicated counter-terrorism investigation unit comprising 23 officers who can escalate and respond quickly to events and draws on financial investigation expertise from within the FIU and broader Police Financial Crime Group (FCG) as required. These analysts are in continuous contact with each other, including in response to FIU analysts' manual review of all terrorism-related SARs and any additional SARs identified through the weekly screening process (refer to IO6).

268. At the time of the Christchurch terrorist attacks, the Police were developing standard operating procedures (SOPs) for investigating terrorism financing for use across the FCG, including the FIU, and the National Intelligence Centre, National Security and Investigation Team (NSIT) and Security Intelligence and Threats Group (SITG). These SOPs were put into operation for the investigation of the Christchurch terrorist attacks and have since remained in operation. Under the SOPs, the roles and responsibilities of the FIU and the NSG and the SITG are set out clearly. The SOPs also provide for engagement and opportunities for sharing of information and intelligence across government agencies such as supervisors and the New Zealand Security Intelligence Service.

13 Following the on-site visit, the terrorist responsible for the 15 March 2019 attacks pleaded guilty to 51 charges of murder, 40 counts of attempted murder and one charge of terrorism. On 27 August 2020, he was sentenced to life imprisonment without parole.

269. The FIU and NSG regularly meet formally which, in turn, feeds into a regular briefing for the Police senior executive. The liaison between FIU and NSG appears to be effective in ensuring all relevant information is shared and has helped to develop capacity within the NSG to understand and respond to financial intelligence developed by the FIU. The NSG highlighted the value of the financial intelligence received from the FIU, but authorities considered that further work could be done on how to prioritise individual cases under investigation.

270. Within the FIU, all SARs in which a reporting entity has listed 'terrorism financing' as an indicator, are reviewed by dedicated terrorism financing analysts. The number of such SARs is relatively low in absolute terms and as a percentage of the total number of SARs, numbering 330 SARs from 2013 to 2019 inclusive, or 0.46% of total SARs. This appears consistent with New Zealand's lower terrorism financing risk profile. There was an uptick in SARs citing the terrorism financing indicators following the Christchurch terrorist attacks. The FIU has since focused on educating reporting entities beyond the large banks about terrorism financing indicators, which is consistent with the action plan attached to the 2020-2022 National AML/CFT Strategy, which has helped to reduce the levels of lower quality reporting. The FIU has initiated a small number of terrorism-related investigations based on its holdings and has provided support to investigations initiated by other agencies. The FIU has also used the Financial Crime Prevention Network public private partnership to gather financial intelligence related to these investigations.

Box 4.1. Case Study - 2019 Attacks in Christchurch

On Friday, 15 March 2019 two shooting attacks occurred at mosques in the city of Christchurch. In total, 51 individuals were killed in the attacks, with a further 49 injured.

The attacks were perpetrated by one individual. The perpetrator faced 51 charges of murder, 40 charges of attempted murder, and one charge of committing a terrorist attack, to which he pleaded guilty on 26 March 2020. On 27 August 2020, he was sentenced to life imprisonment without parole.

New Zealand authorities sought to reconstruct the perpetrator's financial activity. In the hours following the attacks, the FIU began to provide information to investigators based on its holdings and information received from overseas counterparts. Formal tasking to the Financial Crime Group began on the morning following the attacks.

Within 48 hours following the attacks, the New Zealand Financial Crime Group, including the ARU and FIU, were able to reconstruct, and analyse the accused's financial transactions across multiple bank accounts, both domestic and foreign.

The ARU managed the investigative capacity of the reconstruction while the FIU facilitated much of the international liaison to obtain transaction histories for foreign accounts. This involved a significant reallocation of resources within the FIU to provide surge capacity to support the investigation.

> As a result of these investigations, New Zealand Police determined that the terrorist attack was entirely self-funded.

271. While financing by third parties was found not to be a factor in the Christchurch terrorist attacks, authorities used all available CFT tools effectively to support the broader investigation. Financing of terrorism was considered and pursued comprehensively from the beginning of the investigation. New Zealand Police had the capability to follow the money and draw on the sources of financial intelligence available from multiple channels. This FIU reallocated resources to provide surge capacity and through its established networks with international partners provided early and relevant financial intelligence to support the investigation. Reporting entities responded quickly in reviewing their databases and providing information to the FIU. Other agencies across government, including the Inland Revenue Department, used their relationships with international partners to obtain information to support the investigation. In addition, New Zealand pursued formal mutual legal assistance requests in support of the investigation, including obtaining banking records from overseas, which enabled authorities to develop a fuller picture of the perpetrator's activities.

272. On 8 April 2019, the Government of New Zealand established a Royal Commission of Inquiry into the Terrorist Attack on Christchurch Mosques, to examine matters relevant to the lead-up to the attacks (but not authorities' response once the attacks had commenced). The Royal Commission's terms of reference include making recommendations as to what changes, if any, should be implemented to improve relevant State sector agency systems, or operational practices, to ensure the prevention of such attacks in the future. These recommendations could concern changes to legislation, policy, rules, standards, or practices. At the time of the on-site visit, the work of the Royal Commission was continuing.[14]

TF investigation integrated with –and supportive of- national strategies

273. Law enforcement, operational and intelligence agencies are included in New Zealand's comprehensive CT strategic governance framework, including actively contributing to policy development. The Counter-Terrorism Co-ordination Committee (CTCC) is chaired by the Department of Prime Minister and Cabinet and includes the Government Communications Security Bureau, MBIE, the Ministry of Defence, MFAT, NZ Customs, NZ Defence Force, NZ Police and the NZ Security Intelligence Service. The CTCC, in turn, reports to the senior executive-level Security & Intelligence Board. The AML/CFT Co-ordination Committee includes policy agencies, supervisors as well as the Police and Customs.

274. As noted in Immediate Outcome 1, the national CT Strategy does not include any action items related to terrorism financing and the AML/CFT Strategy includes one action item on expanding guidance on SARs for TF. New Zealand noted that the work programmes represented a point in time, and followed previous work undertaken on TF priorities identified through the 2015 National Risk Assessment. Further action items may be identified following the publication of the findings of the Royal Commission of Inquiry into the Terrorist Attacks on the Christchurch Mosques. New Zealand authorities are encouraged to feed in the practical lessons learned by

14 The report of the Royal Commission was published on 9 December 2020 at https://christchurchattack.royalcommission.nz

investigative agencies looking into the financial aspects of the Christchurch investigation as part of future CT strategic and policy planning and co-ordination.

Effectiveness, proportionality and dissuasiveness of sanctions

275. Financing of terrorism is punishable by 14 years' imprisonment under New Zealand law which is comparable to other serious offences under New Zealand law. However, as there have been no prosecutions for terrorism financing to date, it is not possible to assess how this penalty will be applied in practice and whether it will be effective, proportionate and dissuasive.[15]

Alternative measures used where TF conviction is not possible (e.g. disruption)

276. New Zealand pursues a range of measures as part of its broader Counter-Terrorism Strategy. As noted above, these are primarily directed towards the "Reduce" element of New Zealand's 4Rs approach. This work includes reducing the drivers of terrorism financing by focusing on social inclusion and partnering with communities, as well as engaging with the public and private sectors and maintaining systems to respond in the event of an attack. A range of agencies have taken steps to combat the broader terrorism threat to New Zealand. Given New Zealand's lower terrorism financing risk profile and legal framework, the use of alternative measures does not reflect an inability to prosecute terrorism financing, but complementary whole-of-government efforts to combat terrorism.

277. While no cases (other than the Christchurch investigation) have moved beyond the intelligence stage, New Zealand Police actively monitor for persons of interest, and the number of leads has increased following the Christchurch attacks. In appropriate cases, authorities have used the full suite of legislation available to respond to cases, including offences under the Crimes Act (e.g. wilful damage, assault), and offences against the Films, Videos, and Publications Classification Act 1993 for distributing extremist materials. The National Security Group works closely with the FIU to obtain financial intelligence, which is used to provide a fuller picture on persons of interest in accordance with the SOP referred to above. However, to date, the individuals that have been prosecuted under other legislation for offences connected with terrorism or violent extremism have not received funding from third parties for their activities and have generally had limited access to resources.

278. Counter-terrorism and counter-terrorism financing measures take place in the context of broader initiatives implemented by the New Zealand Government to reduce the terrorist threat. Customs established a specialist counter-terrorism team in 2002, which provides around-the-clock support to frontline officers screening at the border and provides awareness training, including terrorism liaison officer courses. Immigration New Zealand manages national security risks posed by foreign nationals in co-ordination with other agencies. In September 2019, the New Zealand Government also established a counter-violent extremism (CVE) Ministerial Group, which is chaired

15 On 27 August 2020, the individual responsible for the terrorist attacks on the Christchurch mosques received a sentence of life imprisonment without parole for murder, attempted murder, and engaging in a terrorist act. This was the first time such a sentence had been imposed. The court took into account sentencing considerations for terrorism offending in Australia and the United Kingdom, and stated that 'Personal mitigating factors, including rehabilitation, are to be given less weight. Because of the ideological motivations of terrorism offenders, community protection and general deterrence are to be afforded greater importance notwithstanding that the force of such motivations may mean that such deterrence may not be effective'. *R v Tarrant* [2020] NZHC 2192.

by the Minister for Internal Affairs, to oversee a broader CVE work programme. Finally, the Office of Ethnic Communities within the DIA works to promote social inclusion.

Overall Conclusions on IO.9

279. While New Zealand has a lower terrorism financing risk profile, and has not prosecuted any cases of terrorism financing, authorities have demonstrated both the capacity and willingness to investigate terrorism financing and have established effective co-ordination and information sharing mechanisms to support this. This was clearly demonstrated by the response to the Christchurch terrorist attacks. It is also demonstrated in the use of financial intelligence in day-to-day investigations of persons of interest.

280. New Zealand has devoted significant effort to developing a counter-terrorism strategy, an AML/CFT strategy and supporting work plans. Investigative agencies have supported the development and implementation of TF strategies through involvement in established CT and AML/CFT governance frameworks, including in response to New Zealand's limited direct exposure to the TF risk related to foreign terrorist fighters, and remain appropriately engaged in identifying and responding to emerging threats.

281. New Zealand's broader efforts to reduce the threat of terrorism assist with reducing potential drivers of terrorism financing consistent with the National Risk Assessment.

New Zealand is rated as having a substantial level of effectiveness for IO.9.

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

282. New Zealand's legislative framework supports the implementation of TFS without delay. The TSA defines "United Nations listed terrorist entity" by reference to United Nations Security Council designations for ISIL (Da'esh) and Al-Qaida sanctions and Taliban sanctions, meaning that such designations are automatically and immediately legally effective in New Zealand without further action by officials. Designations pursuant to UNSC Resolution 1373 take effect immediately upon designation by the Prime Minister.

283. Any changes to designations pursuant to ISIL (Da'esh) and Al-Qaida sanctions, Taliban sanctions or UNSCR 1373 are notified to reporting entities by the FIU through goAML. A dedicated officer within the New Zealand Police sends out updates within one business day of receiving the email notification from the United Nations Security Council, or the gazettal of a listing by the Prime Minister under the TSA (and usually more quickly for the latter). However, at the time of the onsite visit, roughly 2 700 of reporting entities were not registered with goAML and therefore did not receive notifications of changes to designations. Supervisors indicated that most of the missing reporting entities were likely to be in DNFBP sectors recently brought under AML/CFT

regulation, which include lawyers, accountants, real estate agents, TCSPs, and non-bank non-deposit taking lenders. The New Zealand Police also publishes a list of all individuals and entities subject to counter-terrorism sanctions regimes on its web site, which is updated together with the goAML notifications. This did not appear in practice to make up for the lack of goAML notifications for unregistered reporting entities.

284. New Zealand has made active use of designations under the TSA, by which it implements UNSCR 1373. Designations can be proposed by any agency or requested by foreign governments through MFAT. Any proposed designations are considered by the Terrorist Designation Working Group whose membership includes the same agencies as the CTCC and it reports to the senior executive-level Security & Intelligence Board. At the time of the onsite visit, 19 organisations were designated. All designations at the time of the on-site visit concerned entities based offshore. Officials emphasised the importance of the designations framework for supporting New Zealand's contribution to the global counter-terrorism effort. The two most recent designations (of groups based in Indonesia and the Philippines) signalled New Zealand's commitment to supporting regional counter-terrorism efforts. Authorities do not maintain statistics about how many designations had resulted from foreign requests, but noted that the designations had arisen from engagement with foreign partners (with greater or lesser degrees of formality) and on New Zealand's own initiative.

285. At the time of the onsite visit, New Zealand had not designated an individual pursuant to UNSCR 1373 and cited a number of reasons for this. First, New Zealand authorities considered that any individual associated with a designated organisation would be captured by the TFS obligations in the TSA. Second, the United Nations already lists large numbers of individuals associated with terrorist entities. While thought has been given to potential designees with connections to New Zealand (e.g. foreign terrorist fighters), at the time of the on-site visit none had been considered to be a good candidate to be listed as an individual. Finally, New Zealand stated that there was the need to prioritise effort due to the resourcing required to prepare a statement of case for designation, and the three yearly review process for all UNSCR 1373 designations.

286. While recognising that New Zealand had made active and appropriate use of domestic designations under the TSA, New Zealand's approach could be further strengthened by authorities giving consideration to additional TSA designations informed by the National Risk Assessment, or at least increasing guidance and outreach around TFS obligations extending to associates of designated persons and entities. This is especially the case when undesignated individuals are publicly known to be associated with designated terrorist organisations, given that relying on association to trigger TFS depends heavily on reporting entities and other government agencies having a sophisticated understanding of TFS obligations and capacity to identify and screen for associates. Agencies such as the Companies Office and the FIU, that rely on the listings were not screening or putting in place alerts for undesignated associated individuals when undertaking their sanctions checks, and many reporting entities relied on public or commercially available lists. Further, while not a technical compliance issue, New Zealand Police recognised the reality that proving TF cases involving undesignated entities is inherently more challenging; as such, additional designations of widely-known global and regional terrorist organisations could assist in prosecuting TF cases if they arise in future.

287. The New Zealand Police and MFAT have provided guidance on their websites on the basic legal prohibitions on dealing with the property of designated entities or making property available to them. FIU guidance also focuses on the need to file a SAR in cases where a person suspects they hold property subject to TFS. Authorities have not undertaken targeted face-to-face or on-line outreach to reporting entities about TFS obligations. While RBNZ has surveyed banks about implementation of TFS and discussed the issue during some supervision visits, the AML/CFT supervisors RBNZ, the FMA and DIA do not supervise reporting entities for implementation of targeted financial sanctions due to the lack of a clear legal mandate to do so.

288. As a result of this, there was a significant variation in the level of knowledge and understanding of TFS obligations, and in the implementation of preventive measures (e.g. timing of sanctions screening of customers at on-boarding with a number of higher risk reporting entities using 'Day 2' or even later screening; frequency of customer database rescreening with approaches as variable as daily rescreening, annual rescreening or never rescreening; and approaches to transaction monitoring). This variation was evident among registered banks and other reporting entities, although larger banks demonstrated a more sophisticated understanding of TFS in part due to their global compliance frameworks. An RBNZ survey of all 26 registered banks in September 2019 found that while all banks had some sort of policy, procedure or control, there was variation in approach. Further, when the assessment team met other reporting entities, there was also significant variation in understanding as to which agency they would contact on TFS issues. Some cited their AML/CFT supervisor while others would contact the FIU, and yet others mentioned MFAT. NZ authorities explained that is due to a 'no wrong door policy' for the reporting of such issues. While in a relatively small and joined up public sector such as New Zealand's this may not always be a problem, there are still risks that a reporting entity may not communicate with the right authority in a timely way.

Targeted approach, outreach and oversight of at-risk non-profit organisations

289. The NRA assessed that registered charities with overseas operations are at the highest risk of abuse for terrorism financing and New Zealand has a comprehensive regime in place for the monitoring of registered charities. Under the Charities Act, the Charities Registration Board is responsible for registration and de-registration of charities. In practice, many routine decisions are delegated to Charities Services within the DIA. Charities Services adopts a risk-based approach to its compliance functions. 'Money laundering and financing terrorism' is one of four overlapping priority areas for compliance work, with the others being: significant or persistent non-compliance with the Charities Act; serious mismanagement; and fraud or corrupt use of funds.

290. There are strong incentives for charities to register, including to qualify for tax concessions. There were approximately 27 000 registered charities in New Zealand at the time the NRA was drafted. Charities Services, in consultation with the FIU, has developed its compliance processes to consider risk of abuse for terrorism financing at each stage of the process. 1,600 charities have identified themselves as undertaking activities overseas and Charities Services has identified a subset of these operating in areas of higher geographic risk. Charities Services screens applicants for registration against sanctions lists, and examines the purposes of the organisation. Approximately 80 charities have been identified as higher risk (across all four priority areas) and subject to ongoing monitoring of which a small number are considered monitored due to their inherent risk of abuse for terrorism financing.

291. Charities Services has also worked effectively with other agencies to deliver outreach on terrorism financing risk to NPOs that have overseas operations. This included a webinar series held from August to October 2019, with participation from IR, MOJ, the FIU and the Council for International Development (the NPO industry body). This was a positive initiative and Charities Services should consider undertaking further outreach at appropriate intervals.

292. There is a small group of NPOs outside the registered charities cohort for which authorities have limited visibility and which the NRA assessed as presenting a moderate vulnerability to of abuse for terrorism financing. These comprise a small subset of tax-exempt non-charity NPOs (approximately 2 000) but which authorities assess as less attractive for TF for other reasons, and tax-exempt non-resident charities (approximately 300) which may present some risk of abuse for TF. While these are subject to varying levels of scrutiny for taxation and charitable purpose reasons, the risk of TF abuse is not part of such oversight.

Deprivation of TF assets and instrumentalities

293. To date, no assets have been frozen in New Zealand pursuant to counter-terrorism sanctions regimes. This may, to some extent, reflect the terrorism financing risk profile in New Zealand. However, in the absence of other indicators that might provide some assurance that this is the case, it was not possible to draw a conclusion. As noted above, reporting entities had a variable understanding of TFS obligations, received limited guidance and were not supervised for TFS. There had also never been a suspicious property report filed, even as a false positive, despite the presence of some (albeit lower) TF risks including the existence of a limited number of foreign terrorist fighters with some connection to New Zealand.

294. At the time of the on-site visit, there had been no financing of terrorism prosecutions in New Zealand (consistent with New Zealand's risk profile) and therefore no associated restraint or forfeiture of TF assets and instrumentalities. However, the general legislative framework under the Criminal Proceeds (Recovery) Act 2009 would apply to the terrorism financing offence in the same way as other offences.

295. Additionally, the TSA includes a power for the Prime Minister to direct that the Official Assignee take control of property owned or controlled, directly or indirectly, by a designated terrorist entity, or property derived or generated from such property. This power is, in effect, an administrative restraint power (forfeiture still requires a court order). This power is additional to those required in the FATF Standards and may provide enhanced flexibility to restrain TF assets and instrumentalities should the need arise in future.

Consistency of measures with overall TF risk profile

296. New Zealand has an overall lower TF risk profile. The NRA identifies two specific terrorism financing risks to New Zealand. One is that radicalised individuals will support overseas groups and that TF networks will abuse New Zealand's vulnerabilities to transnational laundering.

297. New Zealand's legislative framework for implementing counter-terrorism TFS immediately and automatically is a strength of the system. New Zealand has also made active use of designations pursuant to New Zealand's implementation of UNSCR 1373, but should continue to consider to the benefits of making further use of designations even in the context of a lower TF risk profile.

298. The technical compliance shortcomings with respect to authorisations noted in Recommendation 6, including the 'essential human needs' exception to TFS obligations, present some theoretical risks in New Zealand's context given the risks noted in the NRA and the existence of New Zealand NPOs operating (legitimately) in higher-risk jurisdictions, but these risks did not appear to be material in practice. Nonetheless, these technical shortcomings should be addressed to avoid possible abuse in future.

299. Even considering New Zealand's terrorism financing risk profile, as an open economy New Zealand's reporting entities face some sanctions exposure which would be mitigated by more comprehensive post-listing implementation of TFS through ensuring timely notice of changes to designations to all reporting entities; enhanced guidance, education and outreach; and by giving an agency or agencies a clear legislative mandate to supervise for TFS.

Overall Conclusions on IO.10

300. New Zealand's legislative framework ensures that the legal obligation to implement TFS is effective immediately upon designation by the UN Security Council or by the Prime Minister for TSA designations. Communication relating to these designations is, however, hampered by approximately 2 700 of New Zealand's reporting entities not being registered to directly receive such notifications, especially among the more recently regulated DNFBP sectors.

301. New Zealand has listed a number of global or regional terrorist organisations under the TSA, but at the time of the on-site visit had not listed any individuals, including associates of designated terrorist organisations. New Zealand's implementation of TFS could be further strengthened by additional listings informed by the NRA and/or increased outreach and guidance to ensure reporting entities understand the full extent of TFS obligations.

302. The absence of meaningful supervision of reporting entities, combined with the limited guidance on TFS implementation and the lack of outreach to reporting entities contribute to the lower levels of understanding of TFS measures by some reporting entities and potentially reduced their effectiveness. Increased guidance and outreach would assist reporting entities in understanding the roles of different competent authorities within New Zealand's TFS framework.

303. New Zealand has applied focused and proportionate measures to registered charities, the NPO cohort assessed as being at highest risk for abuse for TF. There are a small number of NPOs that are not registered charities for which the potential for abuse for terrorism financing was noted in the NRA, which are not subject to monitoring or oversight to reduce this risk.

New Zealand is rated as having a moderate level of effectiveness for IO.10.

Immediate Outcome 11 (PF financial sanctions)

Implementation of targeted financial sanctions related to proliferation financing without delay

304. In 2019, New Zealand assessed its proliferation risks and found overall risks were low. New Zealand's proliferation exposure related primarily to sensitive technologies, including New Zealand's growing high-tech sector. Authorities also identified potential risks related to trans-shipment through New Zealand with its reputation meaning that exports from New Zealand could be assumed to be legitimate. Authorities have also commenced work on a further risk assessment focused on proliferation financing.

305. Counter-proliferation TFS are implemented in a similar way to counter-terrorism TFS, although under different legislation (the United Nations Act 1946). The United Nations (Iran—Joint Comprehensive Plan of Action) Regulations 2016 and the United Nations Sanctions (Democratic People's Republic of Korea) Regulations 2017 are made pursuant to that Act. Both sets of regulations define 'designations' by reference to United Nations Security Council designations for Iran and DPRK, meaning that such designations are automatically and immediately legally effective in New Zealand without further action by officials.

306. Unlike counter-terrorism sanctions designations, at the time of the on-site visit the authorities did not publish a consolidated list of persons and entities subject to Iran and DPRK targeted financing sanctions. Additionally, there was no process in place to notify reporting entities or others of updates to Iran and DPRK designations, although the MFAT website included links to the UN Security Council web site lists. The assessment team was informed that agencies were working to distribute updates to reporting entities via goAML.[16] This will be a significant step to improve communication of the information to many reporting entities, even if some deficiencies remain because not all of New Zealand's reporting entities are registered with goAML.

Identification of assets and funds held by designated persons/entities and prohibitions

307. At the time of the on-site visit, no property had been frozen pursuant to counter-proliferation TFS in New Zealand. As with counter-terrorism TFS, the legislative obligation to freeze assets is clear and results in implementation without delay. Nonetheless, the limited guidance and outreach to reporting entities about counter-proliferations TFS and lack of supervision mean that it is not possible to draw a conclusions about how effectively assets are being identified pursuant to TFS.

308. Authorities are, however, active in the implementation of broader counter-proliferation measures and have prosecuted one company for contravening export restrictions imposed as part of New Zealand's implementation of UNSC DPRK sanctions.

16 Authorities indicated that notification of changes in counter-proliferation TFS to reporting entities registered in goAML was implemented after the on-site visit.

Box 4.2. Pacific Aerospace prosecuted for DPRK export

In September 2016, a P-750 XSTOL aircraft manufactured by New Zealand company Pacific Aerospace Limited (PAL) was demonstrated at the Wonsan air show in North Korea, in DPRK colours. As a result of media attention, the Customs Service commenced an investigation as to how the New Zealand manufactured aircraft came to be in the DPRK.

The investigation revealed that PAL sold and delivered the aircraft to a Chinese company (Beijing General Aviation Company) in September 2015. The plane was then on-sold to another Chinese company (Freesky Aviation Company Limited). PAL was advised that Freesky intended to base the aircraft in the DPRK, where it would be used for tourism purposes.

Pursuant to the sanctions regulations, aircraft and their parts are defined as luxury goods, and therefore prohibited exports to the DPRK. PAL's sale of the P-750 to Beijing General Aviation Company was not a breach of the sanctions regulations on the part of PAL. However, breaches of sanctions regulations arose when PAL, on three separate occasions, supplied warranty parts to Freesky, knowing that the parts would be sent to repair the aircraft based in the DPRK.

Customs led the investigation and laid three charges relating to export of the warranty parts – for indirectly exporting a specified good to the DPRK, and for making an erroneous export entry. In October 2017, PAL entered guilty pleas to the three charges for the indirect export of three aircraft parts to the DPRK. It also entered a guilty plea to one charge under the Customs and Excise Act 1996 for making an erroneous declaration about parts exported inside the aircraft but not declared.

PAL was fined NZD 74 805 in relation to the three sanctions breaches and NZD 1 000 for the charge under the Customs and Excise Act. PAL is the first company to have been investigated and prosecuted under New Zealand's sanctions regulations.

PAL has acted to ensure future compliance and now advises the Ministry of for Foreign Affairs and Trade (MFAT) of all its foreign aircraft sales, regardless of destination.

309. Customs is active in targeting strategic goods of potential proliferation concern through alerts against tariff classification and country of destination. When any goods are identified that are strategic in nature, or destined for a sanctioned country, Customs is alerted and the goods are stopped from export until such time as sufficient documentation or permits are presented to allow those goods to be released. Any goods which subsequently do not have the correct documentation provided would be subject to further Customs scrutiny. MFAT also facilitates requests for ministerial consent under the Iran or DPRK sanctions regimes, which can involve engagement with other agencies about end users. To date, all such applications for ministerial consent have related to exports of goods and services rather than TFS.

310. The Companies Office screens its database against the DPRK sanctions list every six months and has reported one false positive. It does not screen its database against Iran sanctions.

311. Following the 2009 SP Trading case in which a New Zealand registered company was implicated in the illegal shipment of arms from DPRK to Iran, New Zealand introduced a resident director requirement.

FIs and DNFBPs' understanding of and compliance with obligations

312. As noted above, authorities provide limited guidance on the implementation of TFS, and do not undertake outreach to reporting entities on TFS implementation, which also applies in relation to UNSCRs on proliferation financing. This, combined with a lack of supervision, likely contributed to reporting entities demonstrating significant variation in their understanding of, and approach to implementing TFS, from not taking any steps to implement TFS through to large multinational reporting entities with systems designed to fulfil their legal obligations globally. Additionally, there was a lack of clarity among reporting entities as to which authority or authorities they should approach with any sanctions related questions or issues, or to apply to for an authorisation or consent in relation to a transaction that was subject to sanctions.

Competent authorities ensuring and monitoring compliance

313. Sectoral risk assessments developed by the AML/CFT supervisors include some high-level information on proliferation financing with links to sources of further information. Nevertheless, as noted above, reporting entities are not supervised for implementation of TFS, which also applies in relation to UNSCRs on proliferation financing. The AML/CFT Act does not provide for any agency to perform this function, meaning that supervisors have no clear legislative mandate to carry out supervision activities with respect to TFS.

314. This lack of supervision contributes to the wide variation in the approach to implementation of TFS among reporting entities, including timing of screening at the onboarding stage with a number of higher risk reporting entities adopting 'Day 2'or even later screening. It may also have an impact on the resident director requirement introduced in response to the SP Trading case. Given authorities' lack of visibility about whether a director is acting as a nominee director (and for whom they are acting), the effectiveness of the resident director requirement would be strengthened by efforts to ensure effective implementation of TFS by TCSPs, lawyers, accountants, and any banks with which the legal person holds an account.

Overall Conclusion on IO.11

315. New Zealand's legislative framework ensures that the legal obligation to implement TFS is effective immediately upon designation by the UN Security Council. However, at the time of the on-site visit, reporting entities were not notified of changes to designations. Reporting entities exhibited a wide variation in their understanding of TFS, reflecting the absence of meaningful supervision for TFS implementation, limited guidance and the lack of outreach to reporting entities on TFS. The resident director requirement introduced in response to historic proliferation cases would be enhanced by improved understanding of TFS among TCSPs, lawyers and accountants.

New Zealand is rated as having a moderate level of effectiveness for IO.11.

Chapter 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings

a) New Zealand covers all FIs, DNFBPs and most VASPs under the AML/CFT Act as reporting entities. HVDs however are not required to comply with the full range of obligations. There are also a range of legislative gaps in the AML/CFT Act. These gaps, particularly in relation to PEPs, MVTS, wire transfers, internal controls, higher risk countries, the definition of TCSP and real estate CDD obligations, impact New Zealand's overall effectiveness. Overall, reporting entities' understanding and implementation of their AML/CFT obligations is mixed across the sectors and within sectors.

b) For understanding of ML/TF risks and AML/CFT obligations, there is a better understanding in larger and more sophisticated reporting entities, and in sectors where AML/CFT obligations are better-established. Banks and other large financial institutions demonstrated a good understanding of their ML/TF risks and obligations, including the cross-border aspects of the ML/TF risks. Larger MVTS providers demonstrated a more comprehensive understanding of risk, while smaller MVTS providers rely more heavily on 3rd party providers to understand risk. Among DNFBPs, casinos and some TCSPs have a good understanding of ML/TF risks and obligations. The newly supervised DNFBPs' (Phase 2 reporting entities) and VASPs' are largely still developing their understanding of their ML/TF risks and how AML/CFT obligations apply to their business.

c) The implementation of AML/CFT controls by banks and other large financial institutions is of a good standard. However, there are areas that could be enhanced, including PEP and sanctions screening, CDD on existing customers and group-wide ML/TF risk management. Implementation by the MVTS sector is variable, with the AML/CFT programmes of smaller MVTS providers seemingly driven by their need to maintain access to banking services rather than by supervision. For some remittance networks, there is insufficient oversight by the principal remitter of the activities of its agents. The AML/CFT controls implemented by Phase 2 reporting entities are less sophisticated and are still developing. The implementation of AML/CFT controls by casinos and TCSPs could also be enhanced further.

d) The level of STR and SAR reporting by DNFBPs is low, particularly by TCSPs, law firms, accounting practices and real estate agents. The challenges faced by reporting entities in the registration and filing process with the NZPFIU portal presents a barrier to effective reporting.

Recommended Actions

a) New Zealand should further develop the understanding of the ML/TF risks by the newly supervised DNFBPs and VASPs, including through additional outreach by DIA on their expectations in relation to the entities' risk assessment processes.

b) New Zealand should enhance the understanding and implementation of the smaller FIs, newly supervised DNFBPs and VASPs of their AML/CFT obligations. This should include clarifying what activities are captured activities under the AML/CFT Act for law firms and accounting practices.

c) New Zealand should take steps to rectify the identified technical compliance issues regarding preventive measures to ensure New Zealand's AML/CFT framework is brought in line with the FATF Standards. This should include addressing the technical shortcomings in relation to DPMS.

d) New Zealand should take steps to ensure that MVTS network providers and agents are appropriately managed and monitored for compliance in accordance with the FATF Standards, including ensuring effective supervision and implementation of AML/CFT obligations in complex MVTS networks.

e) New Zealand should strengthen implementation of measures in relation to identification and approval of PEP relationships, and designated persons under TFS, including mandating that reporting entities screen customers' names to ascertain PEP/sanction designation status prior to establishing business relationships.

f) New Zealand should ensure that all reporting entities are registered with the NZPFIU reporting system. New Zealand should take measures to resolve the practical issues encountered by reporting entities when they register, file reports and receive communications through the NZPFIU reporting system.

g) New Zealand should continue its efforts to improve SAR reporting from under-reporting sectors, particularly TCSPs, law firms, accounting practices and real estate agents. This should include providing education and guidance to the reporting entities on identifying TF/PF suspicious activities, such as sector specific typologies and indicators

316. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23, and elements of R.1, 6, 15 and 29.

317. The AML/CFT Act is the main piece of legislation setting out the AML/CFT obligations of reporting entities in New Zealand. The Act was enacted in 2009 and came fully into force in June 2013. The Act originally captured banks, financial institutions, MVTS providers and casinos, with some TCSPs added in 2013 (Phase 1 reporting entities). The AML/CFT Act was amended in 2017 to include all remaining DNFBPs, including lawyers, conveyancers, accountants, real estate agents and RITA, with a limited scope of applicability to the HVD sector (Phase Two).[17] New Zealand has also granted a number of exemptions to certain activities and services (see IO.1). While the AML/CFT Act does not specifically refer to them, VASPs are covered by the pre-existing definition of financial institution in the AML/CFT Act. This means the requirements in the Act are not tailored to VASPs (e.g. for CDD or wire transfer rules) and not all types of VASP are covered (such as wallet providers which only provide custody services for virtual assets and do not also facilitate exchanges or transfers).

318. The AML/CFT Act sets out the preventive measures reporting entities must comply with. While the Act generally covers the necessary components, there are a number of issues with New Zealand's technical compliance with the FATF Standards that impact its effectiveness. These gaps, particularly in relation to PEPs, MVTS, wire transfers, internal controls, higher risk countries, the definition of TCSP and real estate CDD obligations, impact New Zealand's overall effectiveness.

319. Considering the relative materiality and risk in the New Zealand context, the implementation of preventive measures by the relevant sectors was weighted as follows:

a) **Most heavily weighted:** Large banks largely demonstrated effective implementation of preventive measures commensurate with their risks. However, implementation by smaller banks is varying.

b) **Heavily weighted:** Implementation of preventive measures in the MVTS sector is variable. TCSPs appear to have a good understanding of ML/TF risks and obligations, but their implementation of controls could be enhanced further and the low level of STR reporting is of concern. The ML/TF risk understanding and implementation of AML/CFT obligations by law firms, accounting practices and real estate agents is mixed. Larger firms and those with an international presence demonstrated implementation of measures commensurate with their ML/TF risks while smaller firms' AML/CFT programs are still developing.

c) **Medium weight:** Large derivative issuers demonstrated effective implementation of preventive measures proportionate to their risks. Implementation of preventive measures by NBDTs is varying. Casinos appear to have a good understanding of ML/TF risks and obligations, but their implementation of measures need to be enhanced. HVDs are subject to a limited scope of the AML/CFT requirements and appear to be at an early stage of compliance. Implementation of preventive measures by

17 In New Zealand, DPMS are captured as a type of HVD.

VASPs is also at an early stage, with a lack of clarity about how the AML/CFT Act applies to their activities.

d) **Low weight:** Understanding of risks and implementation of preventive measures by life insurers and other smaller financial institutions is less comprehensive.

320. The assessment team's findings on IO.4 are based on interviews with private sector representatives, reviewing monitoring findings, data and statistics from supervisory activities, discussions with supervisors, data on STRs and SARs, discussions with the NZPFIU and information from New Zealand authorities, including the NRA and SRAs, with respect to materiality and risk of each sector.

321. The assessment team met with a small number of reporting entities from the relevant sectors and some representative industry bodies. The assessors interviewed seven banks, two securities market participants, one managed investment scheme manager, three MVTS providers, two real estate agents, one TCSP, one casino, one law firm, one accounting practice, one VASP and one HVD (which was a DPMS). While these meetings cannot be taken to be representative of all reporting entities, they did not reveal any serious inconsistencies with the sector-wide findings outlined in the NRA, SRAs and supervisory reports.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF risks and AML/CFT obligations

322. The AML/CFT Act sets out clear requirements for the New Zealand reporting entities to identify, assess and understand their ML/TF risks. The supervisors have issued comprehensive guidelines to assist reporting entities in understanding their obligation to conduct a risk assessment and implement commensurate measures. Overall, there is good understanding of ML/TF risks and AML/CFT obligations in larger firms and Phase 1 reporting entities. Phase 2 entities, particularly smaller firms, are in the process of developing their understanding of their ML/TF risks and AML/CFT obligations.

323. The NZPFIU directly involved private sector entities in the most recent NRA process, mainly through member banks of the FCPN and industry bodies. For the SRAs, the supervisors used information sourced from reporting entities in course of their supervisory relationships (e.g. annual report data, reporting entities' risk assessments and AML/CFT programmes, onsite inspections). DIA and FMA also engaged directly with the private sector in the development of their SRAs, while RBNZ did not.

Financial institutions and VASPs

324. The banking sector is dominated by four subsidiaries of Australian banks. They mostly operate under their group policies that set the broader frameworks, principles, high-level documents and group-wide risk assessments. They develop their New Zealand-specific compliance programs to meet the specific AML/CFT Act requirements. Some obligations may be carried out in Australia or another country in a centralised manner (e.g. transaction monitoring).

325. Banks demonstrated a good understanding of their ML/TF risks. The results of their businesses ML/TF risk assessment are generally in line with the outcomes of the NRA and RBNZ SRA. Banks have assigned resources to implement processes and procedures to pro-actively identify, assess and document these risks based on various

risk factors. Risk assessment are documented and reviewed annually as well as on ad hoc basis in response to specific risk events. For example, banks updated their risk assessments after the Christchurch attacks in 2019 and following the issues identified around smart ATMs in Australia in 2017 (see Box 5.1).

326. Banks also have a comprehensive understanding of their AML/CFT obligations. Banks that are part of international financial groups are able to leverage on the knowledge and compliance infrastructure available from their overseas parent companies. However, they were able to demonstrate that their compliance programs are independent and tailored to the specific New Zealand requirements. The FCPN contributed to the information sharing and their understanding of new and emerging ML/TF risks.

327. As for smaller banks, NBDTs and life insurers, the RBNZ noted that there are some issues in ML/TF risk assessment process. These were mainly attributed to the reporting entities' lack of distinction between the inherent versus residual risk concepts. This resulted in inaccurate assessment of risks, and inconsistent ratings with RBNZ's SRA.

328. Well-established FMA reporting entities demonstrated a good understanding of ML/TF risks and obligations. These include large brokers/custodians, DIMS providers and issuers of securities who are also subject to regulation under other FMA regimes. Such reporting entities invested in compliance risk management tools, assigned sufficient resources to implement robust compliance programs and demonstrated commitment to such systems and controls. The FMA advised that the understanding of ML/TF risk by smaller FMA reporting entities is developing. Small financial advisors are however also subject to the compliance requirements of product providers with mature compliance processes. This supports their understanding of their customers' ML/TF risks.

329. The understanding of MVTS providers of their ML/TF risks and obligations is mixed. Larger, multinational MVTS generally have a sound understanding of their AML/CFT obligations and ML/TF risks. Larger MVTS providers typically operate with a network of agents. MVTS providers are not required to include agents in their AML/CFT programs and agents are not required to be licenced or registered in their own right (R.14). While some agents may be reporting entities in their own right, many agents provide this as an ancillary service. In more complex MVTS structures, with agents and sub-agents, this can lead to a lack of clarity as to who is responsible for AML/CFT compliance and insufficient oversight of compliance by the network provider.

330. Smaller MVTS providers are developing their understanding of ML/TF risks and obligations. From the businesses met, it appears that they are investing in compliance systems and controls in response to pressures from banks to maintain access to banking services. The assessors were concerned that there could be over-reliance on third party consultants to conduct risk assessments and establish compliance programs for such businesses. This is supplemented by the remittance businesses' knowledge and understanding of specific cultural characteristics. While such understanding is key to profiling customers, such MVTS providers risk becoming complacent by relying on the perception of a pre-defined behaviour.

331. Most VASPs are covered under the AML/CFT Act's pre-existing categories of financial institutions. Due to the newness of the sector in New Zealand, the existing language of the legislation does not easily accommodate the nature of transactions and

customer relationships in the sector. This has caused a challenge for VASPs in understanding their obligations. During the onsite, the DIA and FMA released VASP-specific guidelines, which should assist. The sector was included in the NRA and SRA processes; however, the level of understanding of risks by the reporting entities in this sector cannot be determined at this time.

DNFBPs

332. Some TCSPs and casinos have been reporting entities since 2013 under the AML/CFT Act. All other DNFBPs and RITA have only been reporting entities since 2018/2019 as part of the Phase Two reforms. Prior to this, they did have limited obligations (such as STR reporting) under the FTR Act.

333. The TCSP interviewed by the assessment team had a good understanding of ML/TF risks associated with its business. This includes the risks arising from international operations and dealing with customers domiciled overseas, and implemented a risk-based AML/CFT programme. It has processes to initiate CDD information gathering prior to establishing a customer relationship through questionnaires and preliminary searches on the purpose of the relationship, tax residency and tax compliance status in home jurisdictions. DIA's supervisory engagement with TCSPs affirms that the level of understanding of ML/TF risk and AML/CFT obligations is well-developed.

334. Casinos have a good understanding of their ML/TF risk including awareness of international risks associated with their business. For example, New Zealand authorities noted a good example where a casino worked with Customs to develop guidance for international guests bringing cash to gamble with in the casinos. However, the measures implemented by casinos to address their risks are not always commensurate with the specific risks associated with their business and appear to be more focused on the gambling business e.g. using transaction monitoring to identify problem gamblers.

335. As law firms are relatively new to the AML/CFT Act, the level of understanding of ML/TF risks and AML/CFT obligations varies across the sector. Larger law firms with international offices or networks have developed a good understanding. They have developed internal company surveys and have used the NRA, SRA and guidance to inform their risk assessment. They treat the risk assessment as a living document with ongoing review and updates. Smaller and medium sized law firms are still in the process of developing their understanding. DIA's supervisory engagement with the sector found that many internally developed ML/TF risk assessments and AML/CFT programmes were of a high standard. Some ML/TF risk assessments were generic, with AML/CFT programmes not specific to the reporting entities' business. Some parts of the legal sector also do not agree with the sector rating assigned by the SRA process. ML/TF activity is seen as activity carried out by a few complicit individuals, rather than a sector-wide vulnerability. Compliance cost and administrative burden is also a challenge for smaller law firms.

336. Similar to law firms, larger accounting practices with international engagement have a good understanding of ML/TF risks and AML/CFT obligations. They are investing resources to comply with their obligations. Small and medium-sized accounting firms have less understanding of their ML/TF risks and AML/CFT obligations. This could be compounded by the lack of understanding by these reporting entities of the specific category of activities that trigger obligations under the AML/CFT Act. Similar to law firms, some parts of the sector do not agree with its risk rating

assigned in the SRA. Cases of ML ascribed to a few 'bad apples' rather than a sector-wide vulnerability.

337. Understanding of ML/TF risks and associated obligations by real estate agents varies as well due to their recent capture under the new AML/CFT regime. Some real estate agents have a basic understanding of risks, but are struggling to formulate a clear understanding of the risk assessment requirements. They have relied on off-the-shelf templates bought from external providers to complete this process.

338. Under the AML/CFT Act, there are no requirements for HVDs to understand their ML/TF risks and there appears to be limited understanding of their risk.

339. RITA was also added as a reporting entity in the Phase 2 reforms, in relation to betting or the operation of accounts or provision of vouchers. DIA advised that they worked with RITA in preparation for the commencement of its AML/CFT obligations. RITA has conducted a ML/TF risk assessment and had assigned a dedicated AML/CFT compliance resource. By capturing RITA as a reporting entity, New Zealand has applied AML/CFT requirements beyond the sectors prescribed in the FATF Standards.

Application of risk mitigating measures

Financial institutions and VASPs

340. Generally, banks and large securities markets participants implement policies and controls commensurate with the level of risks identified through their individual risk assessments. Such reporting entities demonstrated commitment to a strong compliance culture and invested in resources by implementing a 'three lines of defence' model. Results of the thematic review on 'Smart ATMs' is a good example of reporting entities' applying mitigating controls to a known risk.

Box 5.1. Smart ATMs thematic review

RBNZ initiated the "Smart ATMs" thematic review in 2017 following an investigation by AUSTRAC, the Australian AML/CFT supervisor, into a large Australian bank and intelligent deposit machines. The review aimed at obtaining information on the cash deposit transactions through ATMs in New Zealand and the procedures and controls in place for identifying, managing and mitigating the ML/TF risks of such transactions. RBNZ found that the surveyed banks had a good awareness of the ML/TF risks associated with cash deposits via an ATM or fast/express deposit type service. The survey concluded that some ML/TF risks exist with cash deposit via Smart ATMs. However, the volumes of deposits conducted via these channels were lower in New Zealand than Australia. The banks had applied other mitigating controls, such as lower deposit thresholds and restrictions for non-customers. RBNZ communicated the key findings from the survey were communicated to all registered banks who completed the survey. RBNZ conducted further verification and validation of survey responses via on-site inspections.

341. Nonetheless, there are some issues with the implementation of risk-mitigating measures by FIs. The RBNZ has observed instances in smaller reporting entities where AML/CFT controls were not clearly based on identified, such as the implementation of transaction monitoring rules that are not linked to risks or vulnerabilities identified by the reporting entity. Some of the FMA-supervised reporting entities also view the risk-based approach to be subjective. They consider that they need more firm guidance addressing their AML/CFT requirements in practical terms with more specificity, rather than referring to the objectives of the AML/CFT Act.

342. There are also instances of de-risking, particularly in relation to business relationships with MVTS providers and VASPs. This may indicate that some banks are terminating business relationships instead of implementing mitigating measures commensurate with the identified ML/TF risks. Most of the banks interviewed explained that they consider business with VASPs beyond their risk appetite.

343. Implementation of AML/CFT systems and controls commensurate with risk in the MVTS sector is varying subject to the size and international presence. Large multi-national remitters apply risk-based AML/CFT measures and controls, which are regularly updated. This includes applying CDD measures in accordance with customer risk rating, country rating and mode of delivery. CDD is updated as a result of on-going monitoring. Some larger MVTS providers rely on agents to distribute their services, onboard customers and receive cash to book wire transfers. Due to the legislative deficiencies in New Zealand's framework for MVTS (see R.14), the assessors are concerned about the management of MVTS agents. In particular, the level of due diligence and vetting applied during the selection process of agents, the procedures to monitor agents' compliance performance and the extent to which agents' are captured in the MVTS provider's AML/CFT programme is inadequate. Smaller MVTS providers apply AML/CFT controls, such as customer risk rating and monitoring, which are partially risk based. It is not clear if such controls are updated based on risk assessment of changes in business model or delivery methods.

344. As they are newly regulated sector in New Zealand and due to a lack of specific legislative provisions referring to VASPs in the AML/CFT Act, VASPs have encountered certain challenges in understanding their AML/CFT obligations and applying the required measures appropriate to their risks. The DIA issued a guideline for VASPs in March 2020, which is expected to support VASPs to develop their levels of compliance.

DNFBPs

345. TCSPs have developed policies and internal controls proportionate to their risks including elements such as assessing customer risks, higher risk jurisdictions and complex structures. Through its supervisory engagement of TCSPs since 2013, DIA notes the presence of strong basis for understanding of ML/TF risks, application of a risk-based approach and a reasonable level of implementation of mitigating measures.

346. There are three casinos in New Zealand operating six sites. It appears from the discussion with the assessment team that casinos are aware of the complexity of their business involving cash, foreign holding accounts, international junket operators, international transactions and stored value instruments. The implementation of mitigating measures appears to be only partially linked to the ML/TF risk. For example, the implementation of day two PEP screening is not commensurate with risks identified by casinos for dealing with foreign PEPs. Similarly, casinos' risk assessment recognizes the risk of their international business but third-party payments are not sufficiently addressed by their measures.

347. Implementation of proportionate AML/CFT measures varies across the legal and accounting sectors subject to size and international engagement. Larger firms with international presence or networks are able to leverage their group's compliance knowledge and resources to implement appropriate AML/CFT controls as compared to smaller firms. Some law firms and accounting practices encounter challenges in understanding the category of activities that trigger obligations under the AML/CFT Act. For real estate agents and conveyancers, the implementation of measures varies among reporting entities in the sector as a factor of their understanding of their risks but overall is less sophisticated. Overall, the level of implementation of mitigating measures by the newly supervised DNFBPs is developing. A common factor noted by the DIA through its monitoring is a disconnect between a reporting entity's risk assessment and its AML/CFT programme.

348. There are no requirements for HVDs to implement AML/CFT measures appropriate to the ML/TF risks associated with their business.

349. In the absence of a licensing/registration regime for TCSPs, HVDs and some accounting practice firms, it is not clear whether all such entities have self-declared themselves as reporting entities to their AML/CFT supervisor and are implementing the required preventive measures.

Application of CDD and record-keeping requirements

Financial institutions and VASPs

350. The banks and large securities market participants are generally aware of, and have in place, adequate CDD and record keeping measures. Some banks deployed centralized customer on-boarding teams and assurance checks. There are situations where funds are accepted in the account with a restriction to disbursement, subject to completion of the CDD verification process. Banks may accept establishing business relationships with incomplete CDD information under special circumstance for financial inclusion purposes. However, no withdrawals are conducted prior to the completion of the CDD process.

351. Reporting entities in these sectors are also aware of their beneficial ownership information requirements. They use various methods to identify the ultimate persons holding ownership and control of their customers. Some have also developed scenarios to run through their entire database to identify common addresses and related parties. However, there are instances where reporting entities rely on self-declaration by persons to confirm if they are acting in a nominee capacity.

352. Smaller reporting entities such as NBDTs and life insurers have varying levels of compliance with CDD requirements. RBNZ's monitoring activity has noted that the CDD policies and procedures implemented by some of these reporting entities are less detailed. RBNZ has also noted that the quality of CDD by some NBDTs may vary among lending versus depositing relationships. Beneficial ownership identification and verification issues did not come as major findings in the RBNZ on site reports of NBDTs in the years 2017 and 2018. However, issues have been identified in life insurers' compliance with EDD and beneficial ownership requirements and insufficient record keeping measures in relation to SARs, staff vetting and training.

353. Case studies were provided which demonstrated that the effective implementation by FMA reporting entities of CDD, EDD and ongoing CDD measures. These have resulted in reporting entities declining new customers, terminating

existing relationships and revealing identity theft situations. Effective implementation of CDD measures among FMA supervised reporting entities varies depending on the size and sophistication of the reporting entity. Overall, FMA considers that there has been an improvement in the levels of CDD compliance over the years.

354. The ongoing due diligence update of legacy customer appears to be a challenge for most reporting entities, particularly in the banking sector. Some are awaiting further clarification as to the supervisors' expectations and others are applying measures to update such records on a risk basis. It is not clear if there is a point at which supervisors' expect all customers to have undergone CDD to the level required in the AML/CFT Act.

355. Some reporting entities have experienced challenges with the implementation of electronic identity verification tools. Reporting entities identified a need for more specific guidance from their AML/CFT supervisors on the expected features of the technology to be applied.

356. Some MVTS providers have implemented technology-based systems to collect, maintain and update CDD information and records. It does not appear that such measures are equally implemented by reporting entities across the sector. Smaller businesses appear to apply less sophisticated CDD and record-keeping processes given their smaller customer base and limited remittance corridors.

357. The VASPs interviewed by the assessment team implement CDD measures based on their existing interpretation of the Act. These requirements were designed for reporting entities with conventional business operations and have not been customized to fit the nature of this business. Supervisory engagement with the sector indicate that record keeping measures are in their early stages.

DNFBPs

358. TCSPs have implemented CDD measures and controls and demonstrated a reasonable level of understanding of their beneficial ownership requirements in general. However, their implementation of CDD measures on beneficial owners of trusts could be further enhanced. Supervisory engagement by the DIA indicates that since 2013, the TCSPs sector's compliance with enhanced CDD and beneficial ownership requirements has remained mixed, though improving overall. Compliance with record keeping requirements is generally reasonable.

359. Casinos have processes in place for CDD, including through face-to-face interactions by the casinos' trained staff and through open source information. The challenge remains in identifying and verifying source of funds/wealth information in real time commensurate with the nature of their business. DIA considers the application of record-keeping measures by casinos to be well-developed and notes that casinos implemented sophisticated technology-based systems for record-keeping, CDD and ongoing monitoring.

360. One casino provider in New Zealand uses junkets. Prior to hosting an international junket operator/organiser of a group commission programme, casinos must complete a suitability assessment of the organizer as prescribed by the DIA. Assessments are lodged with the DIA for comments and advice of any additional checks. There is no prescribed set of CDD requirements for organizers to implement when conducting CDD on players. However, casinos are required to conduct their own CDD as part of their obligations under the Gambling Act.

361. Large law firms have policies in place to conduct CDD and ongoing reviews of customer relationships and leverage on their international network to maintain their CDD information up to date. However, identification of source funds is an ongoing challenge. As for the other newly supervised sectors (accounting firms, conveyancers, real estate agents, and HVDs), DNFBPs were subject to the previous customer identity and record keeping requirements under the FTR Act. According to DIA, CDD is viewed as one of the main challenges for some reporting entities, with a particular challenge in understanding beneficial ownership and source of wealth/source of funds.

362. For the real estate sector specifically, real estate agents in New Zealand are only required to apply the CDD requirements to the party on whose behalf they are acting unless they conduct an occasional transaction with the other party such as receiving an advance payment. This is inconsistent with the FATF Standard to conduct CDD on both the purchasers and the vendors of the property. It results in a lack of complete visibility of the end-to-end real estate transaction, including detection of any links among the parties involved by any of the reporting entities. Further, some real estate agents use a third-party trust account service to facilitate the advance payments among the vendors and purchasers of properties. The third-party trust account service holds funds with the Public Trust (a reporting entity supervised by FMA). It is unclear who is responsible for monitoring the transactions and detecting unusual patterns in this account, as real estate agents have little visibility over the payments made to and from this account.

Application of EDD measures

Financial institutions and VASPs

363. Implementation of EDD measures varies among reporting entities, depending on their size and international exposure. The large, sophisticated reporting entities have invested in name screening tools to identify PEPs and persons designated under TFS. Smaller reporting entities may undertake PEP and sanction checks manually from the relevant websites. The FIs met by the assessment team are aware of the requirements with respect to dealing with customers from higher risk jurisdictions and implemented controls to comply with such requirements.

364. For PEPs, the AML/CFT Act does not include domestic PEPs. Some of the banks have processes to identify domestic PEPs but reporting entities do not generally identify domestic PEPs or undertake EDD measures.

365. One concern around implementation of EDD is that reporting entities are applying a 'Day 2' screening process to identify PEPs and persons designated under TFS. This may result in establishing a relationship and activating an account with a customer prior to ascertaining their PEP or designation status. Another concern is the re-screening of the customer database occurs at distant intervals such as weekly, monthly and, in some cases, annually. These issues are due, in part, to the lack of guidance from the relevant authorities and absence of supervision for TFS implementation (see IO.3 and IO.10). However, international banks, as part of their group processes have in place processes to screen customers pro-actively to comply with their PEP and TFS compliance requirements. In 2019, RBNZ surveyed banks for implementation of measures pertaining to compliance with TFS obligations. The survey identified that banks generally have certain measures in place such as assessments of TF risks prior to issuing new products, implementation of TFS policies

covering customers and employee screening, transaction screening, alert reviews, escalation, training and reporting to senior management.

366. Reporting entities in New Zealand are also required to apply EDD measures on business relationships with trusts. New Zealand mandated such EDD requirements in line with the results of the NRA where trusts were identified as the main type of legal arrangements and the most relevant from an ML/TF risk perspective. Reporting entities explained the practical challenges they encountered in terms of time and resources in undertaking EDD on all trusts, particularly when there is not a register of trusts in New Zealand that could facilitate the process. While recognising the inherent ML/TF risks posed by trusts, reporting entities did not view all trusts as equally high risk.

367. Banks providing correspondent banking services did not raise any major challenges in implementing enhanced measures to new correspondent banking relationships. Some banks have designated specialized teams for this purpose. EDD on correspondent banking relationships is often conducted by overseas head office teams in the case of banks that are part of an international financial group. In addition to EDD measures, they discussed examples of transaction monitoring scenarios, implemented specifically for monitoring activity in correspondent banking accounts. Prior to the onsite, a major ML investigation was launched in Australia impacting the parent bank of one of New Zealand's large banks. Amongst other things, this investigation related to the bank's approach to correspondent banking. At the time of the onsite, it was unclear the extent to which the alleged deficiencies in Australia were also present in New Zealand.

368. As for channels involving new technologies such as electronic verification and digital onboarding of customers, banks reporting entities implementing measures and controls proportionate with the risk of anonymity arising from such situations. Most of the banks interviewed confirmed adopting biometric features to verify the identities of customers in non face-to-face situations.

Box 5.2. Examples of customer relationships ended by brokers upon conducting EDD

Example 1: An existing trust client of a broker appointed a trustee company, which was based in a high risk jurisdiction. Given the new association to this jurisdiction, the broker requested the account be closed.

Example 2: An existing client had an account with a broker for a low risk New Zealand based superannuation product. After a number of years of no activity, the existing client requested the broker open accounts for the client's children. This triggered notification from a sanctions screening service that an individual related to the existing client was jailed for three years for accepting bribes. Considering this new information, the broker then requested all associated accounts be closed.

369. Multinational MVTS providers have systems in place to identify PEPs and sanctions designations pro-actively and prior to commencing business relationships. They leverage group-wide resources and infrastructure and apply a centralized monitoring process. They also demonstrated awareness of the requirements with respect to dealing with customers from higher risk countries as well as wire transfer requirements.

370. Some of the less sophisticated MVTS providers also use commercial lists from third party providers to comply with these requirements. They rely on their front line staff knowledge of the communities in their most popular corridors to identify PEP customers manually. The assessment team was informed that all wire transfers are screened prior to executing them including those uploaded by the agents linked to the company's systems. However, there remains a risk that cash is accepted by the agents prior to the screening process. The assessment team is concerned that settlements through third party accounts could hinder the effective implementation of wire transfer requirements. Such settlement arrangements have resulted from the lack of access to banking services by some MVTS providers due to de-risking.

371. VASPs interviewed implemented some of the EDD measures. This includes identifying source of funds/source of wealth for transactions above a pre-defined threshold, PEP screening and measures for non-resident customers. VASPs are awaiting further clarification as to the applicability of the other measures, such as whether New Zealand's wire transfer rules were applicable to their business.

DNFBPs

372. TCSPs are generally aware of the EDD requirements for foreign PEP customers. They have implemented processes to screen customer names to identify PEPs and TFS designated persons prior to establishing a relationship through third party system providers. However, re-screening is conducted annually and therefore changes in customer PEP status or TFS designation are not captured in a timely manner. They also have measures in place for dealing with customers from high risk countries. Such measures are linked to the country risks identified as part of their ML/TF risk assessment.

373. Casinos use external service providers as a source of updated sanctions and PEP lists to comply with these requirements. Similar to other reporting entities, they implement a 'Day 2' process of customer name screening, which creates a challenge when a PEP is identified to collate all the required EDD information and source of funds. It may also result in establishing a relationship with a customer prior to ascertaining their designation status. Casinos also apply EDD measures to their relationships with international junket operators. Such measures are linked to their ML/TF risk assessment and take into consideration the country risks of the junket operators. It is not clear how the requirement to transfer relevant originator information is complied with when the casino transfers funds to a customer's overseas account

374. Implementation of all of these measures by the newly supervised DNFBPs is mixed and mostly less sophisticated. Challenges were highlighted by these reporting entities in implementing EDD to trust relationships particularly the identification of beneficial owners in the absence of a trust register. HVDs are exempt from these EDD requirements.

Reporting obligations and tipping off

375. Reporting entities in New Zealand are subject to a number of reporting requirements under the AML/CFT Act. New Zealand amended the Act in 2017 to extend the scope of reporting to include SARs in addition to STRs. New Zealand again amended the AML/CFT Act in 2018 to introduce PTRs. This expands NZ's reporting requirements beyond the FATF Standards. Under the PTR requirements, reporting entities are required to report any transaction conducted through them in respect of an international wire transfer of a value equal to or above NZD 1 000 or a domestic physical cash transaction of a value equal to or above NZD 10 000.

Reporting generally

376. The NZPFIU has as an online reporting portal for STRs, SARs, PTRs and secure communications. At the time of the onsite, there were 4 171 reporting entities registered with the NZPFIU. The reporting portal differentiates between a STR and SAR and reporting entities are required to categorize their filing accordingly. STRs represent the clear majority of reports received from reporting entities.

377. Reporting entities highlighted a number of practical limitations with the NZPFIU reporting system. Some reporting entities noted that technical difficulties in the registration process for the NZPFIU reporting system had discouraged them from completing their registration. This is a particular issue for smaller reporting entities, who make few STRs or SARs and are unfamiliar with the system. Approximately 2 700 reporting entities have not registered with the reporting system, consisting mostly of DNFBPs. There is a concern that the unregistered reporting entities will not be able to meet their reporting obligations in a timely manner and do not have direct access NZPFIU notifications, guidance and training that is mainly communicated through the portal. This is mitigated to some extent by the requirement for DNFBPs to register with their supervisor from which they receive guidance. There are also provisions to report SARs orally and the reports are followed up with registration and electronic submission. However, the extent to which these provisions are used by the unregistered reporting entities is unclear.

378. Reporting entities from a wide range of sectors and capabilities also advised that STR/SAR filing is labour intensive and time consuming. Several reporting entities reported that the system presented a real barrier to effective reporting, with technical restrictions on uploading more than one transaction at a time noted as being a particular issue. Reporting entities also found the use of the pre-existing NZPFIU reporting system for PTR filings to be challenging, since the system was not originally designed for that purpose. Some reporting entities reported that the reporting template in the NZPFIU reporting system is not adapted to the context of their business or the transactions in their respective sectors. For DNFBPs, the assessment team noted a lack of clarity as to the exact information to be reported in PTRs and who needed to report in a transaction chain. Some reporting entities, particularly some DNFBPs, were of the view that such reporting is of more relevance to banks.

379. The NZPFIU considers that the issues faced by reporting entities with its reporting system will be addressed through its Service Delivery Transformation Project. The NZPFIU has also published a SAR Guideline and provides training to reporting entities where they are taught how to submit SARs and understand what is suspicious. The NZPFIU publishes quarterly statistics and guidance and advisories related to SARs. In recent years, the NZPFIU placed more attention on educating reporting entities on TF indicators to address defensive and misguided reporting (see

IO.9). Some of the reporting entities met by the assessment team expressed the need for more guidance on identifying TF/PF suspicious activities including sector specific typologies and specific PF indicators in the NZPFIU reporting system. Reporting entities also noted that since 2017 the NZPFIU stopped publishing quarterly typologies reports which reporting entities considered useful to help them identify suspicious activities. However, members of the FCPN have access to current typology information provided by the NZPFIU in the context of FCPN's active case operations.

380. Reporting entities, particularly banks, raised concerns about the potential clash between their tipping-off and EDD obligations. However, most of the banks met explained that they have developed internal procedures to handle EDD processes without tipping off the customer. The NZPFIU and supervisors have also worked with reporting entities to ensure a pragmatic approach is taken. FCPN member banks participating in active investigations with the NZPFIU are able to not conduct EDD or exit customer relationships based on information provided by the NZPFIU to avoid tipping-off the subjects. New Zealand authorities advised that they are considering a regulatory exemption covering such situations.

381. The NZPFIU provides feedback to individual reporting entities on filing of SARs informally and on a case-by-case basis. Nonetheless, the NZPFIU states that providing structured feedback to the reporting entities is recognized as an area for improvement. The ability to do this is restricted by the sensitivity of information and time period around the investigations and prosecutions of ML cases. The NZPFIU also advised that defensive reporting was detected as isolated instances, rather than as a trend. In general, the NZPFIU and supervisors considered that the quality of reporting had generally improved with time. In the early years of the AML/CFT Act, the NZPFIU found that reports lacked quality and useful information. Following continued and outreach and education, the NZPFIU has observed that the quality has improved.

Table 5.1. Submitted STRs/SARs by reporting entities

Reporting entity	2016	2017	2018	2019	Total
Financial institutions					
Banks	5 471	5 556	7 295	7 893	26 215
Brokers, custodians and managers of managed investment schemes	12	58	56	69	195
Derivatives issuers	7	12	46	77	142
Currency exchange	165	105	124	79	473
Life insurance	1	3	0	1	5
MVTS	2 905	2 727	2 892	3 578	12 102
NBDTs	275	258	373	648	1 554
Payment providers	0	0	2	1	3
Securities dealers	8	8	3	10	29
Other FIs[18]	37	54	115	136	342
Total - FIs	*8 881*	*8 781*	*10 906*	*12 492*	*41 060*
DNFBPs					
Accountancy practices	0	0	4	28	32
Casino	81	83	88	73	325
HVDs	2	1	0	10	13
Law firms and conveyancers	8	9	89	127	233

18 This includes debt collection, financial advisors, financial leasing, investment companies, NBNDTLs, safe deposits, tax pooling, trust and loan companies, trustee corporation and charitable trusts.

Reporting entity	2016	2017	2018	2019	Total
Real estate agents	1	1	1	166	169
RITA	6	36	31	26	99
TCSPs	3	2	3	1	9
Total - DNFBPs	*101*	*132*	*216*	*431*	*880*
VASPs					
VASPs	0	1	7	18	26
All reporting entities					
Total	*8 982*	*8914*	*1 1129*	*1 2941*	*4 1966*

Financial institutions and VASPs

382. The number of SARs, including STRs, reported across all financial institution types has steadily increased over time. The highest reporting is from banks (26 125 STRS/SARs between 2016 and 2019), which is consistent with the sector's size. This is followed by MVTS providers (12 102 STRs/SARs between 2016 and 2019). There is generally a low level of reporting by FMA-supervised reporting entities, which was also noted in previous supervisory monitoring cycles. The FMA states that the reporting level has improved in response to a series of targeted training workshops and is currently more appropriate to the ML/TF risk of the sector. However, the assessment team considers the existing level of reporting to be relatively low taking into account the size, risk and high liquidity of some sub-sectors such as derivative issuers. In addition, the level of reporting by payment providers is very low considering the nature of the sector's business and the ML/TF risks associated with it. Although, some payment providers may be captured as other reporting entities, there were only 3 SARs filed between 2016 and 2019.

383. Most FIs have a reasonable understanding of their legal obligations to file SARs. There is a good level of sophistication in the use of automated transactions monitoring systems, but there is a need for improvement in TF monitoring scenarios. There are concerns in relation to the ability of agents of MVTS providers to identify suspicious transactions or unusual behaviour and escalate to the MVTS provider since they are not captured by this element of the AML/CFT program of the provider.

384. There has been increasing reporting by VASPs, with 26 SARs submitted to the NZPFIU between 2016 and 2019. The VASP met by the assessment team demonstrated awareness of the reporting obligations and implemented measures to identify reportable transactions. However, the existing features of the NZPFIU reporting system are not designed to accommodate filing of data and indicators that are of a particular relevance to VASPs such as blockchain addresses and other technical information.

DNFBPs

385. Between 2016 and 2019, the NZPFIU received 9 STRs from TCSPs. A further 12 STRs were received by other reporting entities undertaking TCSP services (e.g. law firms acting as a TCSP). There is also no detectable increase in reporting since the Phase 2 reforms in 2018. This is very low considering the sector's high vulnerability to ML and the maturity of its AML/CFT supervision which commenced in 2013.

386. Casinos have been subject to STR obligations since 2013 and appear to have a reasonable level of understanding of these obligations. Between 2016 and 2019, casinos reported 333 STRs. Although casinos have not included scenarios/rules through their automated transaction monitoring mechanisms capable of detecting

patterns of behaviour, they further rely on their trained business development and operations staff to identify spikes in activity and risky behaviour. The NZPFIU considers such reports to be useful for investigations being detailed and supplemented by intelligence products.

387. Reporting by the other DNFBPs (law firms, accounting practices and real estate agents) was historically low despite the fact that these entities were subject to the requirement under the FTR Act. The number has dramatically increased in 2019, which follows the inclusion of these sectors in the AML/CFT Act. Nonetheless, reporting by these sectors remains low in light of the ML/TF risks. Identifying suspicions activity remains a recurring challenge for these sectors, with most of the reporting relating to conspicuous placement of cash. The methods used to identify suspicious activity in these sectors are generally less sophisticated, but this could be appropriate for the size and nature of their respective businesses. The NZPFIU confirms that the quality of the reports filed by the new DNFBPs is good, despite the low volumes. HVDs are not required to submit SARs, but are able to do so voluntarily. Between 2016 and 2019, HVDs made 13 STRs/SARs.

Internal controls and legal/regulatory requirements impending implementation

Financial institutions and VASPs

388. Banks and securities market participants interviewed by the assessment team demonstrated a matured compliance culture and commitment to their AML/CFT obligations. They are sufficiently resourced and have a defined compliance governance with access to a board of directors committee. They place emphasis on ongoing training of compliance officers and board members. Larger reporting entities are sufficiently resourced to conduct the independent AML/CFT audit review internally through their internal audit functions. For some reporting entities, RBNZ identified the AML/CFT compliance officer as a key person risk and required reporting entities to hire additional support and resourcing to address this risk.

389. Information sharing among financial group members is only permitted if they form a designated business group. No information on customers, accounts, transactions, analysis of transactions or activities, which appears unusual and STRs filed can be shared with the parent company or other subsidiaries or branches outside New Zealand. Some sharing of information with overseas operations is however done through customer consent and terms and conditions.

390. MVTS providers generally have internal control structures appropriate for their business including dedicated compliance resources, employee training programs and independent audit reviews conducted by their external auditors.

391. Implementation of internal control procedures is in early stages in the VASPs sector. AML/CFT compliance functions may not be currently performed by a designated compliance resource, with independent AML/CFT reviews assigned to an external auditor.

5

DNFBPs

392. TCSPs and casinos generally have internal control structures appropriate for their business including dedicated compliance resources, employee training programs and independent audit reviews conducted by their external auditors.

393. Implementation of internal controls in the newly supervised DNFBP sector is varying subject to size and international engagement. Larger law firms and accounting practices have designated compliance resources as part of defined internal control structures to oversee the entities' effective implementation of AML/CFT controls as compared to smaller reporting entities with less resources and simpler procedures. With the relatively recent commencement of Phase 2, the number of reporting entities in New Zealand has increased. A common concern that was raised by the reporting entities is the insufficient number of independent auditors available to conduct the bi-yearly AML/CFT independent audits as required by the AML/CFT Act. There are also no standards applicable to the independent auditors to ensure the consistency and quality of these reviews. The authorities advised that they were considering this issue.

394. Legal professional privilege was brought up as a potential area that requires further attention as some reporting entities in the legal sector need more clarity in relation to SAR filing and independent audit reviews versus their legal professional privilege obligations. DIA included a specific section in the Lawyers and Conveyancers Guidelines on the subject. DIA considers that the impact of legal professional privilege on the application of internal controls and procedures remains unclear.

Overall Conclusions on IO.4

395. Overall, there is a satisfactory level of understanding of ML/TF risks and implementation of preventive measures by large banks and FIs despite some concerns around the timeliness of implementation of certain measures. The level of understanding of risks and obligations by the MVTS sector is variable and there are concerns around the distribution of AML/CFT responsibilities by some MVTS networks due to their agency structure. For the DNFBP sectors, there is a mixed and uneven level of awareness and understanding of ML/TF risks and implementation of preventive measures, which may reflect some sectors' recent inclusion in the AML/CFT Act. Issues in the NZPFIU reporting system are obstructing the reporting entities' effective compliance with their reporting obligations and there is under-reporting by some DNFBP sectors. Further, there are aspects of New Zealand's AML/CFT regime that do not meet the FATF Standards, impacting the effectiveness of New Zealand's AML/CFT regime.

New Zealand is rated as having a moderate level of effectiveness for IO.4.

Chapter 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

a) New Zealand has three AML/CFT supervisors (RBNZ, FMA and DIA). However, no agency has a mandate to supervise reporting entities for their implementation of TFS obligations.

Financial institutions and VASPs

b) New Zealand authorities generally apply effective licensing/registration measures, albeit some technical deficiencies were identified. Most FIs are required to register on the FSPR but current measures to ensure the completeness of the FSPR are insufficient. This is a particular issue for detecting unlicensed MVTS providers.

c) The supervisors maintain an overall good understanding of the inherent ML/TF risk profiles of their respective sectors, through their SRAs, and individual FIs through their risk profiling models. The understanding of risks relating to VASPs is still developing. The scope and depth of supervision for each financial sector are broadly commensurate with their respective risk levels, except for the banking sector which is due in part to insufficient resources in RBNZ's AML/CFT supervision function.

d) The supervisors generally take remedial actions in an effective manner. However, the range of sanction powers available to the supervisors under the AML/CFT Act is inadequate, particularly the low range of pecuniary penalties available and the lack of administrative penalties. The sanctions that have been applied do not appear to be fully effective, proportionate and dissuasive.

e) FIs generally have good communication and working relationships with the supervisors. Training, outreach and the provision of feedback and guidance is generally strong, although some guidance could be updated. Case examples indicate that actions taken by supervisors have had a positive impact on AML/CFT compliance.

DNFBPs

f) Licensing bodies of DNFBPs apply licensing and screening measures to a varying degree. TCSPs, HVDs and some accounting

practices are not subject to licensing or registration requirements, which impacts DIA's ability to supervise these sectors.

g) DIA has a sound understanding of ML/TF risks of casinos and TCSPs. DIA is developing a more comprehensive understanding of ML/TF risk for the Phase 2 sectors, as the AML/CFT regime for these sectors is nascent.

h) DIA applies the same risk-based supervisory framework to DNFBPs as it does to FIs under its supervision. AML/CFT supervision for Phase 2 sectors is at an early stage. This has been conducted in an effective and well-managed way, but in the future DIA will need to progressively shift its emphasis from education towards supervision and enforcement.

Recommended Actions

a) New Zealand should address the shortcomings relating to licensing and registration of FIs and DNFBPs. New Zealand should consider setting up a registration regime specific to the AML/CFT Act to ensure the completeness of reporting entities being supervised.

b) Sanctions available to AML/CFT supervisors should be enhanced to ensure there is a sufficient range of proportionate and dissuasive sanctions. This should include increasing the range of pecuniary penalties for non-compliance and providing AML/CFT supervisors with powers to impose administrative sanctions.

c) New Zealand should ensure the appropriate scope and depth of supervision for all the different categories of its supervisory population taking into account the sector-specific vulnerabilities, particularly the higher risks of the banking sector, and provide appropriate levels of resourcing to RBNZ.

d) Supervisors should continue to deepen their understanding of the ML/TF risks within the sectors and institutions that they supervise by extending the data sources (e.g. SAR statistics) used for the risk assessments. DIA should also further develop its understanding of risks relating to Phase 2 reporting entities and VASPs.

e) An appropriate agency or agencies should be given clear powers and mandate to supervise and enforce TFS obligations, including establishing clear supervisory expectations for preventive measures to avoid TFS contraventions (e.g. timing and frequency of customer and transaction screening) and conducting outreach to reporting entities about these expectations (see IO.10).

f) Supervisors should continue to provide up-to-date guidance and feedback to reporting entities and ensure that this is timely and fit-for-purpose to enable them to apply AML/CFT measures, particularly with regard to PTR requirements. DIA should strengthen sharing of supervisory information with the licensing bodies of DNFBPs.

396. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, 15, 26-28, 34, 35 and elements of R.1 and 40.

397. The conclusions in IO.3 are based on statistics and examples of supervisory actions provided by New Zealand; guidance issued by the competent authorities; discussions with RBNZ, FMA, DIA and other licensing authorities; and representatives of reporting entities. See Chapter 1 for the description for each supervisor and their responsibilities, as well as the ranking of each sector in terms of New Zealand's risks, context and materiality

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

Financial institutions and VASPs

398. Reporting entities are not licenced or registered under the AML/CFT Act. Instead, they are registered and licensed under a combination of other pieces of legislation. The vast majority of FIs[19] in New Zealand are required to register on the FSPR. Most Core Principles FIs in New Zealand, including registered banks and FIs licensed under the *Financial Markets Conduct Act 2013* (FMC-licensed firms), are subject to separate licensing and screening measures, albeit with some technical deficiencies (see R26).

399. RBNZ is responsible for the licensing of registered banks, NBDTs and life insurers. The licensing process for registered banks is robust, and includes ongoing checks of fitness and propriety (e.g. criminal record checks and home regulator checks) for chief executive officers, directors, senior managers and persons having significant interest in registered banks. Between 2016 and 2019, there was only one new registered bank and no application was declined or withdrawn. Similarly, the number of NBDTs and life insurers remained stable. Only one NBDT and two life insurer licences were granted between 2016 and 2019. While RBNZ also conducts ongoing suitability checks on directors and senior officers of NBDTs and life insurers, beneficial ownership information of NBDTs and life insurers is not obtained and verified to the same extent as registered banks. A case example (see Box 6.1) was provided to show that RBNZ could, on a case-by-case basis, obtain beneficial ownership information of an applicant and work with other authorities (like the NZPFIU) during the licensing process. The shortcoming in beneficial ownership raises concerns, particularly for NBDTs, as they provide products and services that are similar to registered banks.

19 Except for providers of tax pooling, factoring, payroll remittance, debt collection, cash transport and safety deposit boxes, which do not have any licensing or registration requirements.

Box 6.1. Licensing case examples

Example 1: NBDT licensing application

RBNZ received an NBDT licence application from a new FI and was aware of a related company subject to AML/CFT supervision by the DIA. RBNZ's AML/CFT team contacted the supervision team at DIA to obtain relevant AML/CFT information. DIA advised RBNZ to contact the NZPFIU, which revealed that there were significant numbers of SARs involving one of the parties associated with the NBDT licence application. The application was subsequently withdrawn by the applicant.

Example 2: FMA declining licensing application

FMA declined an application for a derivatives issuer licence because the directors failed the fit and proper assessment, among other things.

During the licencing application, FMA checked the names and addresses provided against the Companies Office register and found multiple inconsistencies. Further investigation revealed the director had deliberately misled the FMA in his application by stating that he resided in New Zealand when in fact he resided in Hong Kong, China.

FMA sought more information from the Hong Kong Securities and Futures Commission (SFC). This revealed that one of the directors was the sole shareholder in a company that had received a public warning from the SFC for providing false company addresses and misleading statements about its operations.

FMA was not satisfied that the directors were fit and proper persons to hold their positions. Additional issues were identified, including in relation to operational infrastructure, and that neither director had sufficient or relevant, skills or experience to manage and operate a derivatives issuer licence business. FMA declined the application.

400. FMA assesses FMC-licenced Fis,[20] licensed supervisors and financial advisors on an ongoing basis against sets of eligibility criteria, which include fit and proper tests on directors, senior managers and controllers of relevant FIs. Statistics and case examples (see Table 6.1 and Box 6.1) were provided to demonstrate effective implementation of licensing controls, including declining applications on the basis that the directors of the applicant failed the fit and proper tests.

20 Including retail derivatives issuers; equity crowd-funding platforms; retail MIS managers; peer to peer lending providers and DIMS providers

Table 6.1. Number of licensing application withdrawn or declined by FMA

Effective date	07/2015 – 06/2016	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019	Total
MIS manager	0	0	1	0	1
Equity crowd-funding platform	1	0	0	0	1
DIMS provider	0	0	2	1	3
Peer to peer lending provider	0	0	0	1	1
Derivatives issuer	2	1	5	2	10
Licensed Supervisor	0	0	0	0	0
Financial advisor	2	1	7	8	18

401. FIs that are not required to be licensed by RBNZ and FMA,[21] including brokers, custodians and most DIA-supervised FIs, like MVTS providers, are required to be registered on the FSPR,[22] which is maintained by the MBIE. MBIE applies ongoing screening to directors, senior managers and controlling owners (50% or above) of registered FIs. Since 2010, there were 29 instances where a disqualified person was identified as part of criminal history checks conducted by the FSPR. Case examples suggest that the screening can effectively identify any disqualified persons.

402. VASPs fall under the FI definition in the AML/CFT Act[23] and the definition of financial services in the FSP Act. In New Zealand, DIA is the lead AML/CFT contact for VASPs and the AML/CFT supervisor for most VASPs, while FMA is the AML/CFT supervisor for some VASPs depending on the services provided (e.g. issuing derivatives that are linked to the price movement of a virtual asset). At the end of 2019, DIA supervised 22 VASPs and FMA supervised one VASP. VASPs must register on the FSPR and, where appropriate, be licensed by FMA as well.

403. The FSPR is one of the primary sources for the supervisors, particularly DIA, to identify reporting entities under their supervision. Although FMA and MBIE have made significant efforts to combat the misuse of FSPR and actively exercise their deregistration power where appropriate, it appears that insufficient focus has been devoted to ensuring the completeness of FSPR. This is a particular challenge for DIA, which does not have its own AML/CFT registration or licencing process separate to the FSPR. Currently FMA and MBIE primarily rely on complaints, whistle-blowers, and referrals from international and domestic agencies to identify potential unregistered FIs for further investigations. It is not clear which agency has responsibility for identifying unregistered MVTS providers and no evidence of any co-ordinated proactive activity in this area (see R14). This is of particular concern due to the relatively high ML/TF risk posed by this sector and the vulnerabilities associated with alternative or underground remittance identified in New Zealand's NRA (see IO.1).

21 Except for providers of tax pooling, factoring, payroll remittance, debt collection, cash transport and safety deposit boxes, they are not subject to any licensing and registration requirements as stated in R.26. For the avoidance of doubt, they are subject to AML/CFT supervision by DIA.

22 Financial service providers that are ordinarily resident in New Zealand or have a place of business in New Zealand, regardless of where the financial service is provided, should be registered on FSPR. This is aligned with the definition of FI in the AML/CFT Act

23 The AML/CFT Act does not cover all types of VASPs (see R15).

DNFBPs

404. The licensing bodies for DNFBPs (Gambling Commission, NZLS, NZSC, CAANZ, and REA) are empowered to apply screening measures to prevent criminals and their associates from holding or being the beneficial owner of controlling interests or holding senior management positions in respective DNFBPs. This usually happens during the licensing or professional certification process.

405. Licensing process for casinos is infrequent as casino operator licences and casino venue licences can last for 15 or 25 years. There was only one renewal of a casino venue licence since the Gambling Act came into effect in 2003. For this licensing renewal in 2017, the Gambling Commission demonstrated a comprehensive licensing process, including close co-operation with domestic and overseas authorities. While the Gambling Commission is only responsible for granting new licences or renewing existing ones, ongoing supervision and enforcement of the Gambling Act is conducted by gambling regulators in the DIA. Although casinos need to advise the DIA of any changes to the key persons involved, there is currently no regulatory process for reviewing the suitability of key persons. DIA identifies and investigates potential licence breaches through complaints and site visits.

406. NZLS and NZSC apply licensing controls, including local criminal background checks and, if applicable, overseas police checks, before granting practising certificates to lawyers or registering conveyancers. In addition, lawyers and conveyancers have to declare if they remain fit and proper every year at renewal of their practising or practicing certificates although NZLS and NZSC do not verify those declarations. In the period between June 2016 and June 2019, eleven lawyers were struck off and 27 suspended due to various compliance reasons. No similar figures for conveyancers were provided.

407. Not all accounting professionals in New Zealand are required to be licensed, so only chartered accountants and insolvency practitioners are subject to screening conducted by CAANZ before accreditation. CAANZ do not conduct ongoing screening but rely on passive information like complaints or court cases to identify potential breaches of licensing requirements. No information on the effectiveness of this screening process was provided.

408. Real estate agents are subject to screening at the licensing application and annual renewal by REA. The screening does not however apply to management and beneficial owners of corporate real estate agents. The screening process applied by REA, including criminal checks, is largely effective and the process has led to three applications being declined since 2016.

409. There are currently no specific measures that prevent criminals or their associates from owning, controlling or managing a TCSP or a HVD (except for second hand dealers who have to be registered under the Secondhand Dealers Act and require a police check). This is of particular concern for TCSPs in light of their high ML/TF risk.

Supervisors' understanding and identification of ML/TF risks

410. The AML/CFT supervisors (RBNZ, FMA and DIA) maintain an overall good understanding of the ML/TF risk profiles of their sectors, which is broadly informed by their SRAs, and their individual reporting entities, albeit there exist some important gaps. The latest SRAs published by the supervisors and the risk profiling models adopted by FMA only assess inherent risk without considering controls or mitigation measures in place. These risk assessments rely heavily on AML/CFT Annual Report

data from reporting entities. These are reports which reporting entities must submit to their supervisor every year and they cover a wide range of data points. The risk assessments used other key AML/CFT risk information (e.g. number of reports filed to the NZPFIU) to a limited extent.

Financial institutions and VASPs

411. Each supervisor has so far produced at least two rounds of SRAs. The latest SRAs applied similar methodologies and risk assessment framework but focused on inherent risks only. These SRAs were prepared based on a variety of data sources, including AML/CFT Annual Report data from reporting entities, domestic and international experience (e.g. information from the NZPFIU and reports published by FATF and APG). While reporting entities interviewed generally agreed with the analysis and findings identified in the SRAs, it would be beneficial for the AML/CFT supervisors to further engage the private sector during the SRA processes.

412. RBNZ published SRAs in 2011 and 2017. The SRA published in 2011 was largely based on the APG/World Bank model and relied on a private sector survey in 2009 and other international qualitative data. In 2017, RBNZ updated its SRA, which not only drew on a wider range of data sources including domestic experience gathered since implementation of the AML/CFT Act, but also provided more detailed analysis on TF. The 2017 SRA continued to assess the banking sector, including the retail and commercial banking sub-sectors, as high risk given their significance to New Zealand's financial system and the wide availability of vulnerable products and services. The NBDT sector is assessed as medium risk which reflects the relatively smaller size and volume compared to the banking sector, even though NBDTs offer some similar products and sectors to retail banks. Life insurers continue to be assessed as having low ML/TF risk. The 2017 SRA identified 12 key ML/TF potential vulnerabilities which impact reporting entities in all three RBNZ sectors. RBNZ requires reporting entities to consider these vulnerabilities in their institutional risk assessments.

413. RBNZ assesses the risk of individual reporting entities through its AML/CFT Risk Assessment Model. It utilises multiple data sources, but primarily AML/CFT Annual Report data from reporting entities. RBNZ is in the progress of shifting its AML/CFT Risk Assessment Model to one that incorporates residual risk. For example, the revised model takes into account the AML/CFT capability and culture of reporting entities that are assessed by AML supervisors after on-site inspections.

414. FMA has also published SRAs, in 2011 and 2017. Similar to RBNZ, FMA's 2017 SRA takes into account a wider range of data sources, including the data obtained through the FMA's monitoring activities, and identifies specific "red flags" for reporting entities to include in their own ML/TF risk assessments. The 2017 SRA upgraded derivative issuers from medium-high to high-risk, mainly due to the high proportion of non-resident customers. It also adjusted the risk ratings for brokers and custodians, financial advisers and MIS managers based on more comprehensive data submitted by reporting entities since 2013. For risk profiling, FMA uses a Red Flag Model for assessing the inherent ML/TF risk of individual reporting entities. The model assigns a risk rating to each entity based on the sector risk ratings and 14 additional risk factors assessed on AML/CFT Annual Report data from reporting entities.

415. DIA first produced an initial Phase 1 SRA in 2011, and has subsequently published four SRAs: one for Phase 2 entities in December 2017; one for Phase 1 entities in September 2018 and two updated SRAs for FIs and DNFBPs respectively in

December 2019. The VASP sector was assessed separately in the 2019 updated SRAs,[24] reflecting the development and growth of this sector, and newly issued guidance from international sources. All of DIA's SRAs not only provided an assessment on the inherent risk level of each sector but also identified ML/TF vulnerabilities and high-risk factors that reporting entities should pay attention to in conducting their own risk assessments. Among the financial sectors under DIA's supervision, the SRA identified MVTS providers and VASPs as high risk, with currency exchangers and payment providers rated as medium-high risk.

416. For risk profiling, DIA uses an 'Entity Risk Model'. This is a risk calculation tool used to give each reporting entity a score for their relative level of risk. Unlike the risk profiling models adopted by RBNZ and FMA, DIA's 'Entity Risk Model' calculates the residual risk of each reporting entity taking into account any available compliance assessment conducted. Risk scores under the 'Entity Risk Model' are used as the initial indication of the ML/TF risk level associated with an entity. DIA's risk-based supervisory activities also depend on adverse information or intelligence received from the NZPFIU, LEAs and overseas counterparts.

DNFBPs

417. DIA has a good understanding of ML/TF risk for casinos and TCSPs and a reasonable understanding of ML/TF risk for the Phase 2 DNFBP sectors. The 2019 SRA on DNFBPs assessed TCSPs as high-risk mainly due to high-risk products and services (e.g. acting as or arranging a person to act as nominee director/shareholder or trustee). Other DNFBP sectors except for conveyancers were assessed as having medium-high risk. Currently DIA is in the process of developing a more comprehensive understanding of ML/TF risk for the Phase 2 sectors, which have only been subject to the AML/CFT Act for 6-18 months. Most Phase 2 sectors only submitted their first annual AML/CFT reports in the 3rd quarter of 2019 and DIA is using the data from the reports to construct the ML/TF risk profiles of individual DNFBPs.

Risk-based supervision of compliance with AML/CFT requirements

Financial institutions and VASPs

418. The supervisors have reasonable supervisory frameworks to monitor AML/CFT compliance for FIs and VASPs. They all adopt a risk-based approach in their supervisory frameworks, which combine on-site inspections and desk-based reviews of different intensity, in addition to outreach activities.

419. RBNZ's AML/CFT supervision is mainly carried out by five full-time dedicated AML/CFT supervisors, with the support of around 20 prudential supervisors who also take part in AML/CFT on-site inspection and general relationship management. RBNZ applies different supervisory tools to registered banks, NBDTs and life insurers in accordance with the inherent risks of respective sectors. On-site inspection is the primary tool used for supervising and monitoring the extent to which registered banks are complying with their AML/CFT obligations. Desk-based review is the primary tool used for life insurers, and NBDTs are subject to a mix of on-site inspections and desk-based reviews. RBNZ sometimes uses thematic reviews or surveys to understand and assess new or emerging risk areas (e.g. smart ATM survey in 2017 (see IO.4); TFS

24 VASPs were previously covered as part of the payment providers sector.

survey in 2019). RBNZ demonstrated its supervisory response to negative events and co-operation with home supervisors (see IO.2) by case examples.

420. RBNZ determines the frequency of on-site inspections by a number of factors, including the risk of individual banks and the level of compliance in the previous inspection. High-risk registered banks are generally subject to on-site inspection once every two years. On-site inspections, usually conducted by two AML/CFT supervisors and one prudential supervisor, cover a range of areas including institutional risk assessment, CDD, record keeping, transaction monitoring and STR/SAR reporting. On-site inspection for a large registered bank can be up to five days while that for smaller registered banks or NBDTs only last for one or two days. Taking into account the complexity and risk of registered banks, the scope and depth of the on-site inspection appears insufficient (e.g. future inspections should focus more on the vulnerabilities identified in the SRA). The assessment team considered that this was partly due to the limited resources of RBNZ, a shortcoming also raised by the IMF in its 2016 Financial Sector Assessment Program report.

Table 6.2. AML/CFT on-site inspections by RBNZ

	07/2015 – 06/2016	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019	07/2019 – 12/2019
Bank	10	8	10	7	5
NBDT	5	9	7	3	0
Life Insurer	1	1	0	1	0
DBG member	2	0	0	0	17
Total	18	18	17	11	22

421. FMA supervises approximately 760 reporting entities through 36 fulltime staff who are responsible for both AML/CFT and wider supervisory activities. This appears adequate for it to carry out its supervisory activities. FMA has a structured approach to formulate its annual monitoring plan, and may undertake ad-hoc thematic work where appropriate (e.g. a thematic review in response to the Panama Papers in 2016). In general, FMA's monitoring plan aims to engage 50% of high-risk, 30% of medium-high, 15% of medium-low and 5% of low-risk reporting entities every year. On-site inspections and desk-based reviews are FMA's primary tools used for high-risk and low-risk entities respectively.

422. On-site inspections of larger entities usually last two to four days. They can consist of a minimum of two staff and up to four staff, which is generally consistent with the nature and size of FMA-supervised FIs. FMA conducts two types of desk-based reviews: full review or section 59 review. Section 59 reviews focus only on the independent audit report submitted by reporting entities every two years. A full review has a wider scope including review of the compliance programme and risk assessment of reporting entities. The number of both on-site inspections and desk-based reviews has increased in recent years.

Table 6.3. AML/CFT-related on-site inspections by FMA

	07/2015 – 06/2016	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019	07/2019 – 12/2019
Broker and custodian	0	7	7	16	1
Derivatives issuer	2	3	7	5	0
DIMS provider	0	2	6	2	1
Equity crowd-funding platform	1	3	3	0	0
Financial advisor	3	2	0	5	3
Licensed Supervisor	1	0	5	0	0
MIS manager	4	2	6	4	2
Peer to peer lending provider	1	0	0	0	0
Total	12	19	27	32	7

Table 6.4. AML/CFT-related desk-based reviews by FMA

	Type of engagement	07/2015 – 06/2016	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019
Broker and custodian	Full review	0	2	0	7
	s.59 review	0	7	13	8
Derivatives issuer	Full review	2	0	1	2
	s.59 review	0	0	0	0
DIMS provider	Full review	0	0	2	3
	s.59 review	0	3	11	6
Equity crowd-funding platform	Full review	0	0	0	0
	s.59 review	0	1	0	0
Financial advisor	Full review	0	8	6	5
	s.59 review	8	35	29	41
Licensed Supervisor	Full review	0	0	0	0
	s.59 review	0	0	0	0
MIS manager	Full review	4	0	5	0
	s.59 review	9	1	2	3
Peer to peer lending provider	Full review	0	0	1	2
	s.59 review	0	0	1	0
Total		23	57	71	77

423. DIA adopts a reasonable risk-based supervisory framework to supervise and monitor its FIs, such as MVTS and payment providers. DIA has been increasing its AML/CFT resources since 2013. The number of AML/CFT supervisors has increased from 8 in 2013 to 56 in 2019, who are based in Wellington, Auckland and Christchurch.

424. In the absence of its own specific AML/CFT registration power, DIA uses the FSPR to identify FIs under its AML/CFT supervision. Based on the monthly list provided by MBIE, DIA engages every entity newly registered for financial services that DIA supervises. These initial engagements may be in the form of a site visit, phone call or written correspondence. Priority is given to entities registering to operate as a MVTS provider or as a VASP. Identification of FIs that are not required to be registered on FSPR is generally done through outreach and complaints.

425. DIA's AML/CFT supervisory framework combines on-site inspections and desk-based reviews in addition to a significant number of information or education engagements. On-site inspections are usually conducted by two to three AML/CFT supervisors. They range from a half day up to several days depending on the size, complexity and maturity of the reporting entities. DIA adopts different approaches during on-site inspections. For example, entities undergoing a first on-site inspection will be mainly assessed on their overall understanding and implementation of their AML/CFT programme. A more targeted approach is used for entities with adverse intelligence or a history of non-compliance. Given the large number of reporting entities, DIA relies heavily on desk-based reviews to maximise its supervisory reach to its supervised sectors. For both on-site inspections and off-site reviews, DIA will present a review report to the entity and give compliance ratings for individual regulatory requirements and the entity's overall AML/CFT programme.

Table 6.5. AML/CFT-related on-site / off-site engagements by DIA (FIs)

	Type of engagement	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019	07/2019 – 12/2019
Money remitter	On-site	11	11	13	17
	Desk-based	17	8	22	21
Foreign exchange	On-site	9	4	1	1
	Desk-based	6	3	2	4
Other FI	On-site	3	11	12	7
	Desk-based	34	91	38	28
Total	On-site	23	26	26	25
	Desk-based	57	102	62	53

426. The AML/CFT supervision of VASPs is developing, with a significant focus currently on training and outreach. As of the on-site visit, DIA had conducted one on-site inspection and two desk-based reviews on VASPs. The overall effectiveness is too early to be assessed properly.

DNFBPs

427. DIA adopts the same AML/CFT supervisory framework for DNFBPs with a combination of on-site inspections and desk-based reviews. Supervision of casinos and TCSPs is more mature as they have been subject to AML/CFT obligations since 2013. On the other hand, the AML/CFT supervision for Phase 2 sectors (law firms, conveyancers accounting practices, estate agents and HVDs) is nascent, with frequency and intensity of supervision relatively limited. Since 2019, DIA has undertaken introductory on-site inspections and desk-based reviews on selected law firms and accounting practices. The purpose these activities is to build knowledge of these new sectors and improving their understanding and readiness for AML/CFT compliance. These supervisory engagements were predominantly education focused.

Table 6.6. AML/CFT-related on-site / off-site engagements by DIA (DNFBPs)

	Type of engagement	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019	07/2019 – 12/2019
Casino	On-site	1	0	1	1
	Desk-based	2	1	2	1
TCSP	On-site	4	8	6	11
	Desk-based	35	12	10	9
Lawyer	On-site	0	0	0	6
	Desk-based	0	0	0	61
Accountant	On-site	0	0	0	5
	Desk-based	0	0	0	22
Real estate agent	On-site	0	0	0	0
	Desk-based	0	0	0	2
Total	On-site	5	8	7	23
	Desk-based	37	13	12	95

428. All three supervisors use the independent AML/CFT audit reports as required under section 59 of AML/CFT Act as the basis for their supervisory engagements. However, reporting entities interviewed, especially small-to-medium-size FIs and DNFBPs, expressed concerns over the limited number of qualified consultants in New Zealand. As the Phase 2 sectors are yet to be subject to their first 2-year-cycle section 59 audits, there are doubts as to whether the consultant pool in New Zealand can cope with the significant increase in reporting entities, and the quality of audits that can be delivered.

429. New Zealand does not have an authority with responsibility for supervision of TFS obligations (see IO.10). While RBNZ has surveyed banks about implementation of TFS and discussed the issue during some supervision visits, RBNZ, the FMA and DIA do not supervise reporting entities for implementation of TFS, citing the lack of a clear legal mandate to do so.

Remedial actions and effective, proportionate, and dissuasive sanctions

Financial institutions, DNFBPs and VASPs

430. The supervisors generally take remedial actions in an effective manner. Reports with remedial actions are issued to reporting entities after all on-site inspections and most desk-based reviews. AML/CFT supervisors actively monitor the progress of remedial actions taken by the reporting entities. For example, RBNZ generally requires FIs to report remediation progress on a quarterly basis after on-site inspections. On some occasions, the supervisors request independent validation.

431. The supervisors are authorised to impose a range of civil sanctions under the AML/CFT Act if a reporting entity fails to comply with AML/CFT requirements. This includes the ability to issue a formal warning; accept an enforceable undertaking; seek an injunction from the High Court; and apply to the court for a pecuniary penalty. Criminal sanctions are also available for serious breaches. The supervisors demonstrated their willingness to impose sanctions where appropriate by the number of sanctions and case examples provided. The number of sanctions applied by the supervisors was generally in line with the population of reporting entities for each supervisor and the overall compliance level of each sector.

432. While the supervisors imposed disciplinary sanctions on a graduated basis in response to identified regulatory breaches, the assessment team considered further improvements were needed for the supervisors' abilities to impose effective, proportionate, and dissuasive sanctions. Among the four available sanctions powers under the AML/CFT Act, the supervisors primarily use public or private formal warnings in most non-compliance cases. Enforceable undertakings and High Court injunctions were seldom used by the supervisors. At the moment, even if the supervisors consider a pecuniary penalty is appropriate, they need to go through a very resource-intensive court process. The civil pecuniary penalties imposed in the previous cases appeared to be low in relation to the seriousness of the breaches.

433. For the Phase 2 DNFBP sectors, as DIA does not have licensing power under the AML/CFT Act, it cannot suspend, restrict or withdraw any DNFBP licence or registration as a sanction for serious non-compliance with AML/CFT obligations. Licensing bodies of DNFBPs have existing channels like disciplinary tribunals to handle serious misconduct. No bilateral channels or protocols have been established between DIA and respective licensing bodies to share information on serious AML/CFT breaches that may negatively impact the DNFBP's fitness and propriety to be licensed, however no legal impediments to sharing were noted.

Table 6.7. Remedial actions and sanctions by AML/CFT supervisors

Supervisor	Action	07/2015 – 06/2016	07/2016 – 06/2017	07/2017 – 06/2018	07/2018 – 06/2019	07/2019 – 12/2019	Total
RBNZ	Remedial action	16	16	17	11	19	79
	Public formal warning	1	2	0	0	0	3
	Enforceable undertaking	0	1	0	0	0	1
FMA	Remedial action	2	9	9	7	9	36
	Public formal warning	2	0	1	1	0	4
	Private formal warning	0	12	9	10	0	31
DIA	Remedial action	77	54	76	168	51	426
	Public formal warning	1	0	2	4	1	8
	Private formal warning	3	6	3	0	0	12
	Pecuniary penalty	0	0	1 (NZD 5.29 million)	1 (NZD 0.36 million)	1 (NZD 4.01 million)	3 (NZD 9.66 million)
	Restraining injunction	0	0	1	0	1	2
	Criminal sanction	0	0	0	0	1	1

Box 6.2. Example of sanctions applied by DIA

In 2014, DIA's initial supervisory engagement with a MVTS provider determined it to be non-compliant with its AML/CFT obligations, and a formal warning was issued to this money remitter in January 2015. Later on, intelligence indicated that Asian organised crime groups were using the provider to transfer funds to and from another jurisdiction. It was also suggested that this MVTS provider had not ceased operating as it advised DIA after receiving the formal warning.

In April 2015, DIA conducted further investigation, culminating in an on-site inspection in August 2015. During this inspection, this MVTS provider advised that hard copy CDD or transaction records were thrown away by the cleaner and electronic copies of records were also deleted due to a computer virus.

In September 2016, DIA filed civil proceedings in the Auckland High Court seeking a pecuniary penalty against the MVTS provider and a performance injunction against its sole director/shareholder. This related to 1 588 transactions with a total value of approximately NZD 105 million conducted between 2014 and 2015. Civil liability acts included failures to conduct CDD, undertake account monitoring, keep records and file STRs. DIA used NZPFIU reporting to establish the MVTS provider's civil liability act of failing to report STRs.

In September 2017, the High Court judgment determined in favour of DIA. A pecuniary penalty of NZD 5.29 million plus costs was awarded against the MVTS provider, along with injunctions barring the MVTS provider and its sole director/shareholder from providing any financial services.

Impact of supervisory actions on compliance

434. The supervisors provided some evidence of the effects of their supervision on AML/CFT compliance. RBNZ, FMA and DIA have follow-up mechanisms to monitor the progress of the remediation of identified deficiencies. These mechanisms have improved compliance with reporting institutions. Case examples provided by RBNZ and FMA demonstrate positive impact on the reporting entities which have been subject to sanctions. DIA also provided statistics extracted from annual AML/CFT reports and anonymous surveys which indicate an improving level of compliance by Phase 1 reporting entities. Interviews with reporting entities also supported the view that the actions taken by the supervisors have a positive impact on their compliance, including fostering better risk culture and understanding of AML/CFT obligations. They also acknowledged that the communication with their supervisors is generally good and they have a good working relationship.

435. For VASPs and Phase 2 DNFBP sectors, the impact of supervisory actions cannot be assessed fully. The regime is quite recent and therefore no specific information is available. However, the VASP and DNFBPs interviewed demonstrated that they are aware of the risks presented in their sectors and their AML/CFT obligations under the AML/CFT Act. This suggests that the guidance and education work conducted by the DIA has had some effect on the AML/CFT awareness in these new sectors.

Box 6.3. Example of supervisory actions having a positive impact on compliance

RBNZ identified several CDD deficiencies during an on-site inspection at a large registered bank. This resulted in a formal public warning in 2015. RBNZ found that while the bank had policies, procedures and controls for complying with its CDD requirements, it had interpreted certain requirements in the AML/CFT incorrectly. The bank took several remedial actions to enhance and strengthen its AML/CFT framework and capability, including management oversight, quality assurance on CDD, increased compliance resources, IT system enhancement and extensive in-house training programme. RBNZ subsequently conducted a focused on-site inspection on CDD and was satisfied with the remediation progress. In the following on-site inspections, RBNZ did not identify any material issues that would require the bank to undertake immediate steps to achieve compliance.

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

436. AML/CFT supervisors have provided a wide range of guidance to reporting entities to assist them in complying with their AML/CFT obligations. This includes joint triple-branded guidelines, codes of practice, sector-specific guidelines, factsheets, frequently asked questions, training videos and webinars. The guidance covers different AML/CFT areas, including institutional risk assessments, CDD, EDD, beneficial ownership, wire transfers and country assessments. They have conducted a range of outreach activities (e.g. seminars) to raise reporting entities' awareness of their AML/CFT obligations. All supervisors' websites include a dedicated AML/CFT section and keep relevant information publicly accessible.

437. In addition to the triple-branded guidelines, RBNZ promotes a clear and consistent understanding of AML/CFT obligations through newsletters and outreach programmes. RBNZ publishes an AML/CFT newsletter approximately every six months. This provides observations from on-site inspections and key compliance issues requiring clarification. RBNZ conducts its annual AML/CFT workshop as part of the NZPFIU conference. The workshop provides a forum to communicate key compliance messages and an opportunity for reporting entities to seek clarification on RBNZ's supervisory expectations.

438. FMA utilises a variety of forums and channels to promote AML/CFT obligations. FMA's AML/CFT Monitoring Reports are one of the major tools to help reporting entities better understand the FMA's expectations and improve their AML/CFT programmes. Since 2013, FMA published five AML/CFT Monitoring Reports. Each of these has focused on different AML/CFT obligations and contained examples of good practice and unsatisfactory practice. Between 2016 and 2019, FMA participated in over 20 AML/CFT conferences, seminars and forums run by different professional or industry organisations. In 2018, FMA published on its website a short, animated video on staff training in response to an identified lack of ongoing AML/CFT training by its reporting entities.

Box 6.4. Example of outreach provided by FMA

FMA was concerned, based on data from 2014-16, that its reporting entities were carrying out very low levels of STR reporting compared to other sectors supervised by the RBNZ and DIA. This suggested that its entities were not carrying out their STR obligations correctly. FMA discussed its concerns in its 2014/15 Monitoring Report. Following the release of this report, there was a 34% increase in STR reporting in subsequent year. Despite this improvement, FMA noted that its supervised entities still submitted only a fraction of the total number of STRs filed.

To address these concerns, in 2017 the FMA, in collaboration with the NZPFIU, provided targeted training and workshops to its reporting entities to educate them on reporting of STRs and on how to use the NZPFIU reporting platform. Eleven training sessions were held in various locations across New Zealand. This training has led to a dramatic subsequent increase in reporting levels. The number of STRs being filed by FMA's reporting entities increased by 20% in 2016-17 and then by 128% in 2017-18.

439. DIA attaches significant importance to guidance, training and outreach, and considers them as an important part of its AML/CFT supervision. In addition to a large number of training conferences and education events (a total of 42 engagements in 2018 and 2019), DIA also utilises other means to promote a clear understanding of AML/CFT obligations. For instance, it provides a series of webinars which are designed for compliance officers to help build understanding of AML/CFT requirements (e.g. on CDD and risk assessment). To get the Phase 2 DNFBP sectors prepared for AML/CFT supervision, DIA conducted extensive outreach activities. This includes 52 roadshow events in which over 3 600 lawyers, conveyancers, accountants and real estate agents participated. Sector specific AML/CFT guidelines were provided to these new sectors before the new regimes came into operation. DIA also published a VASP-specific AML/CFT guideline in March 2020 to articulate the AML/CFT obligations for VASPs.

440. In addition to hosting the annual Police Financial Intelligence Unit conference, the NZPFIU provides a range of guidance documents (e.g. on fraud, currency controls, and international funds transfers) to reporting entities through the NZPFIU reporting system. However, only approximately 60% of reporting entities have registered with NZPFIU. In addition, it was noted that since 2017 the FIU stopped publishing quarterly typologies reports which reporting entities considered useful to help them identify suspicious activities. New Zealand explained that typologies were provided through conferences or the NZPFIU reporting system after 2017.

441. Reporting entities interviewed generally acknowledged the usefulness of supervisory documentation and outreach provided by AML/CFT supervisors, but also commented on the lack of sector-specific guidance (e.g. TCSPs) and some guidance was out-of-date (e.g. the factsheet on "acting on behalf of a customer" published in 2013). Almost all reporting entities interviewed reflected that they received insufficient guidance from the NZPFIU or AML/CFT supervisors on how to comply with PTR requirements and there is insufficient guidance and outreach on TFS implementation (see IO.10, IO.11 and IO.4).

Overall Conclusions on IO.3

442. The AML/CFT supervisors (RBNZ, FMA and DIA) supervise, monitor and regulate FIs, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks to some extent. There is however no authority with the mandate to supervise implementation of TFS obligations. New Zealand implements a risk-based approach to AML/CFT supervision and ML/TF risk assessments have been an integral part of that approach for a number of years. The regimes for Phase 2 DNFBP sectors and VASPs are nascent, so the risk understanding and risk-based supervision of these sectors are developing. Supervisory activities are generally targeted towards higher risks albeit the intensity of supervision in the highest risk sector, banking, is inadequate, with insufficient resourcing for RBNZ. Existing licensing and registration requirements are implemented mostly effectively, albeit some important gaps exist. There is strong evidence of genuine efforts by supervisors to engage their sectors proactively and some evidence that these efforts have had an impact on AML/CFT compliance. Remedial actions are taken effectively but there are shortcomings over the range and use of sanctions.

New Zealand is rated as having a moderate level of effectiveness for IO.3.

Chapter 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

a) Information on the creation and type of different legal persons and arrangements is publicly available. Basic information on companies, partnerships and other legal persons is publicly available. Beneficial ownership information conversely is not always available. New Zealand does not have a register of all domestic trusts, however there are registers of certain types of trusts.

b) New Zealand has a comprehensive understanding of the ML/TF risks of legal persons and legal arrangements. In recent years, New Zealand has implemented measures to mitigate the risks of misuse of legal persons and arrangements, including the register of New Zealand Foreign Trusts and company director residency requirements. New Zealand has also established an Integrity and Enforcement Team to maintain the integrity of the registers held by MBIE.

c) However, substantive gaps remain in New Zealand's framework. There are insufficient measures to mitigate the risks posed by nominee directors and shareholders. There are insufficient mechanisms for authorities to obtain adequate, accurate and current beneficial ownership information. The absence of a trust register also limits the availability of basic and beneficial ownership information on trusts. While competent authorities can access beneficial information collected by reporting entities, the timeliness of access to such information appears to be a challenge.

d) A range of sanctions are available for failures to comply with information requirements. The sanctions are insufficient for some legal structures (e.g. trusts). New Zealand has effectively used its ability to deregister companies to promote compliance with information requirements. However, there are insufficient sanctions applied to individuals and to breaches of information requirements for other types of structures (e.g. partnerships, trusts).

Recommended Actions

a) New Zealand should introduce measures to improve the availability of accurate and up-to-date beneficial ownership information on legal persons, particularly limited liability companies and partnerships. This should include consideration of a beneficial ownership register as part of MBIE's ongoing consultation process.

b) New Zealand should take pro-active steps to improve the transparency of domestic express trusts and introduce measures to improve the availability of accurate and up-to-date beneficial ownership. This could include consideration of a register of trusts. This should also include reviewing its framework for mandatory enhanced due diligence for trusts to ensure it is sufficiently tailored to the ML/TF risks.

c) New Zealand should implement measures to mitigate the ML/TF risks of nominee shareholders and directors and ensure full transparency. This could include requirements on such nominees to disclose their status and the identity of the nominator to MBIE and when dealing with reporting entities.

d) New Zealand should ensure that trustees disclose their status to reporting entities when forming a business relationship or carrying out an occasional transaction.

e) New Zealand should ensure that proportionate and dissuasive sanctions are available and enforced for breaches of basic and beneficial ownership information requirements.

f) New Zealand should consider developing a complete TCSP register to be accessed by reporting entities and other agencies.

443. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25, and elements of R.1, 10, 37 and 40.[25]

444. The assessment team's findings on IO.5 are based on discussions with New Zealand authorities and reporting entities, information provided by the authorities including the NRA and SRAs, data and statistics and case studies.

25 The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

445. New Zealand legislation recognizes 10 main types of legal persons. The business registries unit (referred to as the Companies Office) within MBIE is responsible for the incorporation of companies and maintaining the corporate body registers. Most registered legal persons in New Zealand are companies, limited partnerships, incorporated charitable trusts and incorporated societies.

446. There is publicly available information on MBIE's website on the creation, types and ongoing obligations of legal person.[26] The relevant legislation is also publicly available. There are separate statutory registers, and registrars, established under each statute that provides for the creation of legal persons. MBIE maintains a record of each legal person in the relevant Register[27] including basic shareholding and directors' information. Some information is maintained by MBIE but withheld from public access such as information on limited partners. If foreign ownership is involved, the Registrar does not maintain information beyond the ultimate holding company. These registers are publicly searchable online. Members of the public can make specific requests for information from MBIE pursuant to the Privacy Act or the Official Information Act.

Table 7.1. Types of legal persons and arrangements

Legal entity	Number (at March 2020)	Number created each year (three-year average 2017-2020)
Legal persons		
Building societies	9	1
Credit unions	10	0
Friendly societies	109	0
Incorporated society	23 835	743
Industrial and provident societies	81	2
Incorporated charitable trusts	26 117	794
Limited partnerships	2 818	357
Limited liability companies	649 217	55 168
Co-operative companies	128	7
Unlimited liability companies	385	30
Legal arrangements		
Domestic express trusts	300 000 – 500 000	
Charitable trusts registered with the Charities Services	25 709	
Māori Land Trusts	20 795	
New Zealand Foreign Trusts	2 807	

447. There is no equivalent central source for information on the creation and types of legal arrangements. Significant types of trusts in New Zealand include express trusts (including family trusts), charitable trusts, Māori land trusts and New Zealand Foreign Trusts. Trusts, particularly family trusts, are very common in New Zealand (see

26 For example, https://companies-register.companiesoffice.govt.nz/help-centre/before-you-start-a-company/choosing-a-type-of-company-for-your-business/.

27 Further information available on https://companies-register.companiesoffice.govt.nz/.

Box 7.1). Information on the creation and types of legal arrangements, including trusts, and their purposes, may be obtained from various government affiliated websites such as the Public Trust website.[28] New Zealand does not however have a register of all domestically-created trusts. In the absence of a register of trusts, it is not known how many trusts there are in New Zealand. The authorities estimate it is between 300 000 and 500 000.

448. Information on foreign trusts is stored on the register of New Zealand Foreign Trusts. The foreign trust register is maintained by IR. Other trusts that derive taxable income are required to register with IR. The process to register a New Zealand Foreign Trust is described on the IR website.[29]

449. Charitable trusts may register with the DIA's Charities Services under the *Charities Act 2005*. Information about registration is publicly available on DIA's website. When a charitable trust is registered, it appears on the Charities Register, which is a publicly searchable database.[30] Not all charitable trusts are registered. Charitable trusts may also choose to incorporate as a charitable trust board, which then has a legal personality. Information on charitable trust boards is available on MBIE's website.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

450. Overall, New Zealand has developed a clear understanding of the risk of misuse of legal persons and legal arrangements.

451. New Zealand has assessed the ML/TF risks of legal persons and legal arrangements as a part of its ongoing NRA process. The New Zealand authorities' understanding of the ML/TF risks associated with legal persons and legal arrangements has deepened since 2010 through the multiple iterations of the NRA. In the first NRA, New Zealand recognized the risks of the registration of New Zealand companies with overseas-based directors and shareholders, and the risk of abuse of professional gatekeepers providing services associated with legal persons. The second NRA refined New Zealand's initial understanding of these risks. It distinguishes the vulnerabilities associated with domestic legal structures as opposed to foreign legal structures and further analyses threats such as overseas criminals and large scale TF networks. Additionally, vulnerabilities in the professional gatekeeper sectors were emphasized along with their lack of AML/CFT supervision.

452. In the third and most recent NRA update, the NZPFIU conducted separate assessments of threats and vulnerabilities. The threat assessment considered the abuse of these structures by transnational threats as conduits and as methods of moving funds by some terrorist groups. The vulnerability assessment analysed the availability of each class of legal person and legal arrangement for ML/TF abuse. Additionally, the potential impact on law enforcement work and international reputation was highlighted throughout the risk assessment.

453. As set out in the 2019 NRA, New Zealand considers that limited liability companies, limited partnerships and trusts are the structures most likely to be abused for ML/TF purposes. The New Zealand authorities consider that limited liability companies are the most vulnerable vehicle for ML/TF. They are relatively easy to set

28 www.publictrust.co.nz

29 www.classic.ird.govt.nz/international/exchange/foreign-trusts/foreign-trusts-index.html.

30 https://ct-register.companiesoffice.govt.nz/.

up, there is a large number, they can obscure ownership and there is a limited liability on the shareholder for any criminal activity by the company. Limited liability partnerships are also highly vulnerable to ML/TF, as the identity of limited partners is not disclosed publicly (as opposed to general partners).

454. For trusts, the 2019 NRA found that they are abused by criminals to obscure beneficial ownership and involved in transactions through the creation of complex legal structures. Unlike companies, trusts generally require legal advice and facilitation to set up. However, the lack of a central registry of all types of trusts limits law enforcement's ability to detect abuse of trusts. This, in combination with their widespread prevalence in New Zealand, led to the 2019 NRA finding express trusts to be highly vulnerable to ML/TF. The NRA also noted the abuse of trust services provided by professional service providers.

455. New Zealand Foreign Trusts are also of particular ML/TF risk, as they may be used by overseas money launderers to give the appearance of a transaction involving New Zealand. As there are greater mitigating measures for New Zealand Foreign Trusts (see Box 7.3), the 2019 NRA assessed these to have a moderate-high overall ML/TF vulnerability. Charitable trusts were also found to have a moderate-high overall ML/TF vulnerability, while Maori land trusts were found to have a moderate vulnerability due to the difficulties in establishing such structures and the control regime in place.

Box 7.1. Family trusts in New Zealand

Trusts are very common in New Zealand, due to the prevalence of family trusts (a type of express trust). Family trusts are commonly used as a way to hold and legally protect assets of many types, particularly family assets. This includes homes for different purposes such as the benefit of future generations, estate planning and protection against claims by creditors or in the event of relationship breakdowns. Due to changes in taxation arrangements, the New Zealand authorities advised that the use of family trusts has somewhat declined.

456. The NRA also demonstrated New Zealand's understanding of the risk of legal persons and legal arrangements being misused through the use of professional service providers. The NRA identified vulnerabilities mainly related to the use of trust accounts, creating new trusts and companies to obscure beneficial ownership, and providing services to overseas customers.

457. In line with the findings of the NRA, the AML/CFT supervisors also considered the misuse of legal persons and legal arrangements for ML/TF in their respective SRAs. The SRAs recognize trusts and shell companies as high risk factors and a key vulnerability is their potential anonymity and complexity.

Mitigating measures to prevent the misuse of legal persons and arrangements

458. New Zealand has implemented some measures to prevent the misuse of legal persons and arrangements. In recent years, New Zealand has established an Integrity and Enforcement Team within MBIE, placed AML/CFT obligations on the full range of relevant professionals (TCSPs, lawyers and accountants), added new disclosure rules for New Zealand Foreign Trusts and introduced residency requirements for directors. However, important gaps remain in New Zealand's mitigating measures, particularly

relating to the collection, maintenance and accessibility of beneficial ownership information and the misuse of nominee directors and shareholders.

459. In the registration process, companies must provide basic information on shareholders and ultimate holding companies. Limited partnerships must provide details of general and limited partners. Information obtained during incorporation is updated through the life of the legal person either annually or within a specified timeframe in line with requirements in the relevant legislation. Accuracy checks are conducted by the Integrity and Enforcement Team on a risk basis in accordance with a set criteria of red flags. Names of directors and shareholders are screened against lists of disqualified persons, terrorist lists and the UN DPRK list.

460. Beneficial ownership information is not required as part of the registration process, although this will be recorded when the basic and beneficial owner are the same person. There is no central register of beneficial ownership for legal persons, although this information can be collected by reporting entities in fulfilling their AML/CFT requirements. New Zealand companies are required to maintain a share register containing the names of shareholders. However, if the shareholder is not a natural person, no beneficial ownership information is recorded.

461. Recognising the risk posed by trusts in New Zealand, the AML/CFT Act requires reporting entities to apply enhanced CDD measures on all business relationships with trusts. This ensures that reporting entities collect information about the main parties involved in a trust. Reporting entities from the various sectors met by the assessment team explained the EDD process is burdensome and entails practical challenges in terms of time and resources assigned to identify the beneficial owners in the absence of a trust register that would otherwise facilitate the EDD process. While recognising the ML/TF risks posed, reporting entities did not consider all trusts to be equally high risk. Trustees are also not required to disclose their status to reporting entities when forming a business relationship or carrying out an occasional transaction, although this may be identified in the EDD process.

Box 7.2. MBIE Integrity and Enforcement Team

MBIE has a dedicated Integrity and Enforcement Team (IET), responsible for ensuring the integrity of the various corporate registries held by MBIE. This represents a notable good practice for registries in seeking to ensure the integrity of the information they collect. The IET relies on data analytics and exchange of data and intelligence with regulatory partners to identify risk. In particular, the IET:

- undertakes accuracy checks of new applications for registration according to a set criteria of red flags;
- screens the names of directors and shareholders versus lists of disqualified persons, terrorist lists and the UN DPRK list;
- has established a watch list of company formation agents, nominee directors, nominee shareholders and virtual offices commonly used.
- monitors open source information and public complaints to identify issues with the corporate registers; and

- works closely with partner agencies to ensure it is aware of current risks and trends relating to corporate registrations.

Through the integrity assurance programme, IET applies scrutiny measures to legal persons at various phases of registration based on complaints, media publicity, intelligence information, or requests from a supervisor. The IET is well resourced and includes 17 staff. New Zealand authorities advised that IET, in co-ordination with DIA, identified shell companies through the tracing of information of persons linked to previous registrations of shell companies and of addresses used in multiple registrations.

462. New Zealand permits nominee shareholders and directors. The ML/TF vulnerability posed by these services is mitigated to some extent by New Zealand's Phase 2 reforms, which capture reporting entities when they are acting as a nominee on behalf of a customer in a professional capacity. However, this does not sufficiently mitigate the risk posed by nominees. Nominees, both formal and informal (strawmen), are vulnerable to misuse for concealment of beneficial ownership by criminals and disqualified persons, or to circumvent the requirements for a resident director. Additionally, the presence of nominee shareholders on company shareholders registers can impact timely access to accurate beneficial ownership information by law enforcement and create a false link among companies that share the same nominees.

463. There are case examples depicting the vulnerabilities associated with the provision of nominee services by professional service providers and strawmen. In one example, a New Zealand TCSP that provided nominee services for more than 1 000 companies registered in New Zealand on behalf of overseas clients. It was suspected that at least 73 of these companies facilitated crimes in foreign jurisdictions. Other examples included informal nominees (family members and strawmen) were used to conceal beneficial ownership by criminals.

464. Considering the risks associated with TCSP services and marketing of nominee services to overseas clients, there is a concern that such professional service providers do not disclose their nominee status to MBIE and other reporting entities. In the absence of a complete register of TCSPs, IET and other reporting entities lack key information required for their ongoing monitoring and identification of ultimate beneficial owners and controllers of legal persons. There is also a gap of informal nominee service providers not captured as reporting entities under the Act (e.g. a person who is acting as a nominee *not* in the course of operating a business). The risks associated with nominee arrangements need to be sufficiently addressed through specific measures to ensure full transparency.

465. Recent reforms to the Companies Act 1993 introduced a mandatory requirement for companies and limited partnerships to have at least one New Zealand or Australian resident director. This reform ensures there is a director based in New Zealand or Australia who can be held accountable and contactable by law enforcement. However, ease of access to nominee directors means this requirement appears relatively easy to circumvent.

466. There are no explicit restrictions on the issuance of bearer shares and bearer share warrants by New Zealand companies. The risk posed by bearer shares however is adequately mitigated, as the name of each shareholder is required to be registered on a company's share registry, as well as the name of the transferee for each transfer

of shares. Conversely, there are no measures in place to mitigate the risks posed by bearer share warrants specifically. However, in practice this appears to be a minimal risk, as neither the authorities nor reporting entities were aware of any bearer share warrants being issued in New Zealand.

Box 7.3. New Zealand Foreign Trusts and the Shewan Report

New Zealand Foreign Trusts are trusts that are established overseas, by a non-resident settlor and have a trustee resident in New Zealand. If the trust does not derive New Zealand source income or distribute income to New Zealand resident beneficiaries, they are exempt from New Zealand tax. This makes them attractive to foreign investors.

The release of the Panama Papers in 2016 brought attention to the potential for exploitation of New Zealand Foreign Trusts for tax evasion, ML and other illicit activities. In response, the government initiated an inquiry into foreign trust disclosure rules. The inquiry resulted in the Shewan Report, which found that the foreign trust disclosure rules were insufficient. The report recommended several reforms to the New Zealand foreign trust regime to address the issues identified through the inquiry. This included the creation of a foreign trust register accessible by regulatory agencies, extending the information disclosure requirements at the registration phase and requiring filing of an annual return.

Additionally, the Shewan Report expedited the implementation of Phase 2 reforms. It also led to revising the AML/CFT legislation by introducing additional standards to identify and verify source of funds and source of wealth for all foreign trusts, and extending the scope of STR to cover attempted transactions. The information sharing arrangements between IR, NZPFIU and DIA in relation to foreign trusts disclosures were streamlined. The number of foreign trusts decreased by 75% after the commencement of the new disclosure requirements in 2016, from nearly 12 000 foreign trusts to just under 3 000 in 2020.

467. As set out in Box 7.3, new disclosure rules on foreign trusts require complete information of all parties to a trust to be included in the foreign trust register. The accuracy of the information on the New Zealand Foreign Trust register is verified through risk based reviews of TCSPs conducted by IR as part of their routine tax compliance duties. This may lead to audits of foreign trusts. A limited number of TCSPs represent the majority of registered New Zealand Foreign Trusts. The register is updated at the time of annual tax returns. Other issues may be identified through requests for information from international tax treaty partners.

468. There is no equivalent trust register for domestic express trusts. However, income-generating trusts are required to file tax returns with IR where information on trustees is provided and, in case of income distributions to beneficiaries, details of beneficiaries. However, there are limitations on the availability beneficial ownership information of express trusts if the trustee is not a professional service provider who is subject to CDD obligations or in situations where a trustee refrains from disclosing their status to a FI.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

469. New Zealand authorities can access basic and beneficial ownership information on legal persons from various sources. This includes the various registers of legal persons held by MBIE, reporting entities, the legal persons themselves and from other competent authorities.

470. MBIE maintains a record of each legal person in the relevant Register including basic shareholding information, with a history of updates. The availability of such information to the public free of charge facilitates timely access to basic information by reporting entities and other interested parties. Some information held by MBIE is available to LEAs but withheld from public access (e.g. information on limited partners). If foreign ownership is involved, it is not possible to obtain information from the Register beyond the ultimate holding company. These registers are publicly searchable online, and members of the public can also make specific requests for information to MBIE.

471. There is no centralized corporate beneficial ownership register in New Zealand. While basic shareholding information can be obtained mainly from the companies register, beneficial ownership information is not maintained since it is not a requirement at the registration time and thereafter as part of annual returns.

472. Basic and beneficial ownership information can be accessed from reporting entities if a legal person maintains a business relationship with a reporting entity. Reporting entities demonstrated a generally good understanding of beneficial ownership requirements, although implementation of such requirements varies across sectors and within sectors (see IO4). Such information can also be obtained from the legal persons themselves. However, share registers maintained by the legal persons include shareholders information on the assumption that all natural persons on the share register are the beneficial owners i.e. nominee shareholders are not recognized. Share registers do not include beneficial ownership information when the shareholder is a legal person.

473. Beneficial ownership information can be accessed from other competent authorities if a request is made for a proper purpose and an information exchange mechanism (MOU) is in place. Police, SFO, IR and FMA have extensive information-gathering powers. The effectiveness of this is subject to the availability of information. Case studies provided demonstrated the ability of these authorities to access beneficial ownership information. However, timeliness remains a challenge, as the authority must know which reporting entity holds the relevant CDD information.

474. The Registrar of Companies also has specific powers to require information on beneficial owners and controllers of companies and partnerships for specified law enforcement purposes. However, the Registrar has not used this power yet, as beneficial ownership information is not a requirement for the companies register, and no requests have been received from other agencies yet. Instead, other agencies have used other information-gathering powers available to them to access beneficial ownership information.

475. New Zealand issued a consultation paper in 2018 on enhancing the transparency of, and improving access to information on, beneficial ownership of New Zealand companies and limited partnerships. The paper examines different options of the requirements that need to be in place for New Zealand companies and limited

partnerships to hold and disclose information on beneficial owners. Other types of legal persons (e.g. incorporated societies, friendly societies, credit unions) are not included. They are considered less likely to be used as an attractive alternative to companies or the concept of beneficial ownership is difficult to apply in such structures. Trusts are captured by the proposed requirements of the paper only where the beneficial owners of corporate entities are persons who control a trust. Such a reform is expected to enhance the timely access of LEAs to beneficial ownership information of companies and limited partnerships. At the time of the onsite, no decision had been made on whether reforms would be introduced and what the reforms would be.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

476. In the absence of a trust register, identifying sources holding domestic trust beneficial ownership information is not easy and it is time consuming. Although it is expected that beneficial ownership information on express trusts generating taxable income is held by IR, it is unclear what proportion of the total number of express trusts in New Zealand are registered with IR.

477. Trust beneficial ownership information can be accessed from reporting entities to the extent that a trust maintains business relationships with a reporting entity and subject to identifying the reporting entity that keeps the relevant information. Police advise that identifying which lawyer or TCSP holds the beneficial ownership information can be a real challenge. Reporting entities from the various sectors met by the assessment team explained that the trust EDD process is burdensome and entails practical challenges in terms of time and resources assigned to identify the beneficial owners in the absence of a trust register that would otherwise facilitate the EDD process.

478. Such information can also be obtained from the trustees themselves, provided they keep accurate up-to-date records. The use of informal nominee trustees such as family members and strawmen could create an obstacle for the competent authorities to access the accurate beneficial ownership information.

479. In the same manner described above, LEAs have extensive information gathering powers. The effectiveness of these is subject to the availability of the required beneficial ownership information. Case examples were provided demonstrating the use of various methods by Police to uncover the use of trusts by offenders to shield their financial interest and the involvement of a lawyer and accountant in in creating structures to facilitate money laundering. However, LEAs must first identify which natural or legal persons holds the beneficial ownership information in order to exercise their respective powers.

480. The register of New Zealand Foreign Trusts maintained by IR provides timely access to beneficial ownership information of foreign trusts since it is accessible by Police and DIA. Relevant details of foreign trusts are also provided to tax treaty partners on request. IR reports a low number of requests from foreign partners, accounting for 47 information exchange requests in four years and a 100% success rate in providing beneficial ownership information.

Effectiveness, proportionality and dissuasiveness of sanctions

481. There is a range of sanctions applicable to violations of information requirements. However, not all of the sanctions powers have been exercised and it is unclear whether proportionate, dissuasive and effective sanctions have been imposed across all actors and types of legal persons and arrangements.

482. The Companies Act provides a number of powers and sanctions for persons who do not comply with information requirements. Generally, MBIE initiates investigations based on complaints received in relation to incorrect or false information on the register. Between 2015/16 and 2018/19, MBIE received 3 011 complaints and initiated 2 965 investigations (Table 7.2). In most cases, the information is rectified following a request for additional information under section 365 of the Companies Act. MBIE issued 2 039 notices between 2015/16 and 2018/19.

483. Failure to comply with such a request can also lead to a maximum fine of NZD 10 000 (section 373), but it is unclear whether a person has ever been fined for such a breach. Instead, removal of a company from the register is the most commonly used sanction. The process of removal from the Register involves a period of notice, which allows any objections to removal to be lodged and considered. Out of 757 removals initiated between 2015/16 and 2018/19 in relation to information violations, MBIE ultimately removed 269 companies from the register. The remaining would have had an objection against their removal or would have addressed the information violation. Companies may also be removed for failure to respond to a beneficial ownership notice, however the power to issue such a notice has not been used.

484. For the most serious cases, there are sanctions available under the Companies Act for companies that provide incorrect or false information to the Registrar and for falsification of records (sections 377, 379). These are punishable upon conviction with a maximum fine of NZD 200 000 or a prison term not exceeding 5 years. There are other sanctions applicable to directors, such as prohibition from being a director of company (section 383) or managing a company (section 382, 385). Prosecution is pursued for repeated and the most serious offending, after considering the sufficiency of evidence, the public interest, and the Solicitor General's Prosecution Guidelines 2013. New Zealand has convicted six individuals for breaching information requirements under the Companies Act. In most cases the convictions resulted in combined penalties, including those not related to information breaches. Penalties included community service, financial penalties and prison terms, with four individuals receiving prohibition orders from managing companies.

485. The use of the Registrar's powers to deregister companies appears to be an effective sanction to ensure that companies are complying with information requirements. However, there appears to be a lack of sanctions applied directly to individuals, with only six convictions between 2015 and 2019.

Table 7.2. Sanctions for breaches of the information requirements in the Companies Act

	2015 / 2016	2016 / 2017	2017 / 2018	2018 / 2019	Total
Complaints received relating to information kept on MBIE registers collected under the Companies Act	993	767	646	605	3 011
Investigations undertaken into complaints by MBIE	987	755	630	593	2 965
Requests for information issued under section 365 [31]	N/A	125	869	1 045	2 039
Removals of companies initiated for failure to respond to a section 365 request	41	106	300	310	757
Companies subsequently removed (section 316)	17	59	118	75	269
Prosecutions of individuals for breaching information requirements in the Companies Act (section 377)	2	1	1	2	6
Convictions for breaching information requirements (section 377)	2	1	1	2	6
Prohibition orders from managing companies for breaching information requirements (sections 382/385)	2	0	1	1	4

486. Companies are required to register their financial statements annually with MBIE. Where it is judged important for the integrity of the Register, failure to comply can result in MBIE infringement notices, both to directors and to companies. The infringement fee is NZD 7 000. Between 2016/17 and 2017/18, MBIE issued 149 notices.

487. There are also sanctions available for failing to comply with the information requirements for partners under the LP Act. As no information on the use of these powers were provided by New Zealand, the effectiveness of these sanctions cannot be assessed.

488. For trusts, there are proportionate and dissuasive sanctions available for trusts that are registered with IR and that breach information requirements. It is not known whether IR has exercised these powers, so the effectiveness of these sanctions cannot be assessed. For other trusts, there are some sanctions available under common law for breaches of fiduciary duties. However, the insufficient beneficial ownership requirements for trusts means that there are neither sufficient sanctions for failure to comply or sufficient legal liability for trustees.

489. There are measures available to IR in respect of New Zealand Foreign Trusts, if the New Zealand resident trustee fails to meet disclosure requirements by taxing the trust on its worldwide income. IR has not applied this measure due to high compliance to date.

490. There are a range of sanctioning powers under other pieces of legislation. For example, there is a range of proportionate and dissuasive sanctions for offences attached to such violations under the AML/CFT Act but no prosecutions have taken place. There are penalties attached to the offence of failure to comply with agencies information gathering powers. For example, failure to comply with FMA's information-

31 Section 365 request may be triggered in response to a complaint or come from another source (e.g. referral from a partner agency).

sharing power under section 25 of the FMA Act can result in a fine not exceeding NZD 300 000.

Overall Conclusions on IO.5

491. There is publicly available information on the creation and types of legal persons. In the absence of a trust register, there is no effective mechanism to identify domestic trusts in New Zealand. New Zealand authorities have developed a clear understanding of the risks of misuse of legal persons and legal arrangements and implemented several measures to mitigate those risks, including establishing a register of New Zealand Foreign Trusts and the Investigation and Enforcement Team in MBIE. However, a number of important gaps remain in the New Zealand framework that need to be addressed through effective measures. There are insufficient measures to ensure accurate and up-to-date beneficial ownership information of both legal persons, particularly companies and partnerships, and trusts. While this information may be available from reporting entities or the entity itself, this is contingent on competent authorities knowing where to find this information in the first place.

492. There are unmitigated risks associated with the use of nominee directors and shareholders. New Zealand has applied proportionate and dissuasive sanctions to companies through its ability to deregister companies for breaching information requirements. However, limited sanctions have been applied to individuals for breaches and it is unclear whether sanctions have been applied to breaches of information requirements for other legal persons and arrangements (such as partnerships and trusts).

New Zealand is rated as having a moderate level of effectiveness for IO.5.

7

Chapter 8. INTERNATIONAL CO-OPERATION

Key Findings and Recommended Actions

Key Findings

a) New Zealand demonstrates many characteristics of an effective system for international co-operation. It has a sound legal basis to provide and seek MLA and extradition. New Zealand authorities actively respond to formal international co-operation requests. They have received positive feedback from counterparts concerning the quality and timeliness of assistance provided.

b) The central authority for MLA, the CLO, has mechanisms in place to prioritise the increasing number of MLA requests and at present is able to ensure timely responses. Although the case management system and the statistics it produces are relatively basic, this is adequate in the context of the case load. Several competent authorities are involved in handling extradition requests and there is no clear authority with primary responsibility.

c) New Zealand authorities make MLA requests to the extent needed to build cases and are willing to pursue proceeds of crime located offshore. The number of outgoing requests has been increasing in recent years.

d) LEAs in New Zealand actively engage in various forms of direct international co-operation with counterparts. They are achieving good results through such co-operation. LEAs routinely seek and provide international co-operation for AML/CFT purposes, including through their network of liaison officers. The AML/CFT supervisors engage in close international co-operation with foreign regulators, particularly their Australian counterparts in respect of supervising reporting entities with Australian operations or ownership. New Zealand shares basic and beneficial ownership information of legal persons and arrangements with international counterparts.

Recommended Actions

a) New Zealand should review and strengthen the efficiency of its MLA and extradition regime. This may be done by exploring implementation of recommendations proposed by the Law Commission in its review of the Extradition Act and the MACMA and could including establishing a central authority to handle extradition requests.

b) New Zealand should maintain better statistics on MLA, extradition and exchanging basic and beneficial ownership information of legal persons and arrangements to facilitate effective case management and monitoring risk on an ongoing basis.

c) AML/CFT supervisors should continue to improve already close cross-border supervisory co-operation for AML/CFT purposes. In particular, RBNZ should continue to strengthen the co-operation with AUSTRAC which is the home regulator of the four major banks in New Zealand.

493. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40 and elements of R.9, 15, 24, 25 and 32.

Immediate Outcome 2 (International Co-operation)

494. Due to its open economy, New Zealand is exposed to transnational ML/TF risks. While not a major financial centre, it is an important regional remittance centre for the South Pacific, where New Zealand has strong economic and cultural ties. New Zealand co-operates with many jurisdictions, including Australia, which is its major partner for law enforcement and supervisory co-operation. New Zealand also engages actively in all areas of informal international co-operation. Competent authorities regularly seek forms of international co-operation and participate actively in various international AML/CFT fora and networks.

Providing constructive and timely mutual legal assistance and extradition

495. New Zealand generally provides MLA in a constructive and timely manner, and swiftly executes extradition requests. This is based on an analysis of the processes in place, interviews with relevant authorities, statistics on the provision of assistance, a review of case examples, and feedback from the FATF global network.[32]

496. New Zealand has a sound legal basis to provide and seek a range of MLA and extradition in relation to ML/TF and associated predicate offences. Its legal framework for MLA and extradition is set out in MACMA and the Extradition Act, which are broadly consistent with the FATF Recommendations. Between 2013 and 2016, the Law Commission, as referred by the New Zealand Government, conducted a review on these

32 In total, 14 jurisdictions provided feedback on their formal and informal international co-operation experience with New Zealand in recent years: Anguilla, Australia, Belgium, Canada, Germany, Hong Kong, China, India, Lebanon, Macao China, San Marino, Slovakia, Sweden, the United Kingdom and the United States of America.

two pieces of legislation and concluded that they should be replaced by more modern, simplified legislation as the current ones are complex and difficult to follow. The recommendations by the Law Commission were generally accepted by New Zealand and detailed review was ongoing.

Mutual legal assistance

497. The Attorney-General is designated by the MACMA as the central authority for MLA in New Zealand and the Attorney-General's powers under MACMA are largely delegated to the Solicitor-General. The Office of the Solicitor-General, i.e. the Crown Law Office, undertakes the legal work required for transmission and execution of MLA requests. There are 15 counsel in the criminal team of the CLO responsible for handling MLA requests.[33] The CLO maintains a website with key information for countries wishing to make a request to New Zealand.

498. CLO has mechanisms in place to ensure prioritisation and timely response to requests, albeit informal. All incoming MLA requests are first triaged by the manager of the criminal team based on urgency and a counsel is assigned to handle the request. The responsible counsel then prepares a memo on each request to seek views from the Deputy Solicitor-General on whether the request will be processed or refused. The criminal team meets regularly to monitor the progress and timeliness of pending requests. CLO has an internal guideline outlining how to deal with incoming and outgoing MLA requests, which requires acknowledgement of receipt be provided to the requesting jurisdictions within two weeks of receiving their requests. CLO is mindful of the relevant time frame for the requesting country and priority is given where the requesting country has indicated that the request is urgent (e.g. where the assets may be dissipated). CLO uses a spreadsheet for keeping records of all MLA requests rather than having a case management system for monitoring progress on requests.

Table 8.1. Incoming MLA Requests

	2016	2017	2018	2019	Total
MLA requests received	44	43	67	66	220
Outcome of requests received (at March 2020)					
MLA provided	25	29	39	33	126
Withdrawn by requesting countries	13	6	10	10	39
Refused by New Zealand	3	2	4	6	15
In progress	3	6	14	17	40

499. New Zealand has received on average over 50 MLA requests per year and the number of requests is increasing (see Table 8.1). While the spreadsheet used by Crown Law Office cannot accurately break down the requests received by offence (see R33), New Zealand indicated that there were around 35 ML-related MLA requests received between 2014 and 2019. During the same period, no TF-related request was received but there were several terrorism-related MLA requests received after the Christchurch attack (see IO9). Requests for assistance came most frequently from Australia, which accounted for approximately 16% of requests received in the past four years, and the remaining requests were from over 50 jurisdictions around the world.

500. On timeliness, case records of the 220 MLA requests received between 2016 and 2019 revealed that CLO usually wrote back to the requesting jurisdictions within one

[33] The team is also responsible for handling criminal appeal cases.

to four months, most of which were to request further information. New Zealand also indicated that the long processing time in some cases was mainly due to the lack of sufficient information provided by requesting jurisdictions and no response from requesting jurisdictions after New Zealand's written request for additional information. Feedback received from foreign jurisdictions was largely positive, with jurisdictions stating that responses by New Zealand to MLA requests were of good quality and provided in a timely manner.

501. Foreign restraining or forfeiture orders can be registered in New Zealand initially based on only a facsimile copy of the foreign order.[34] This reduces delays in waiting for the original of the order arriving by post. Once the Attorney-General's consent has been obtained, the CLO can apply for the registration of a foreign order on an ex parte basis. In the past five years, there was only one foreign restraint order registered in New Zealand. The order was subsequently lifted after a voluntary settlement and the assets were returned to the requesting jurisdiction without a forfeiture order being registered in New Zealand. New Zealand explained that assets could be restrained quickly and effectively using domestic powers under the CPRA (see IO8), which led to the low number of incoming MLA requests relating to assets recovery.

502. The mandatory and voluntary grounds for refusing to provide assistance are set out clearly in the MACMA and appear to be reasonable and justified. In practice, New Zealand occasionally refused requests between 2016 and 2019 (see Table 8.1) due to isolated reasons (e.g. double jeopardy). In addition, 39 requests received between 2016 and 2019 were withdrawn by the requesting jurisdictions. New Zealand explained that when assistance could not be provided (e.g. if the subject is not in New Zealand or refuses to have a voluntary interview), it would write back to the requesting jurisdictions such that the requests could be withdrawn. However, the assessment team noted that a small number of MLA requests in relation to search warrants were withdrawn by the requesting jurisdictions on the basis that the New Zealand authorities may be required to inform affected parties of the disclosure of the search warrant materials to the jurisdiction. This issue stemmed from case law in New Zealand. Feedback from the FATF global network supports that, in practice, it has not hindered the provision of MLA in respect of search warrants. New Zealand explained how they have adapted practice to accommodate the judgment on a case by case basis, but that the position requires legislative clarification. This is being progressed as part of the legislative amendments associated with New Zealand's accession to the Budapest Convention.

[34] Section 56(5) of MACMA

Box 8.1. Examples of handling incoming requests by New Zealand

The Czech Republic was investigating suspected fraud and money laundering by its nationals. In May 2017, the Czech Republic requested New Zealand to locate and interview the potential victims of fraud by a company in the Czech Republic that occurred in September 2016. CLO received the request from MFAT in May 2017. Since the request did not contain all the information necessary to assess and execute the request, CLO requested further information relating to these and other aspects of the request in a letter sent via MFAT on 29 June 2017. In August, CLO organised, via MFAT, to discuss the matter with an English-speaking liaison person in the Czech Republic. The liaison person provided the necessary information between August and September 2017, and the Deputy Solicitor-General agreed to provide the requested assistance in October 2017. New Zealand Police actioned the request, and CLO sent all requested information to the Czech Republic in November 2017 via MFAT.

Extradition

503. New Zealand's extradition procedures are laid out in the Extradition Act which governs the extradition of persons to and from New Zealand. A foreign jurisdiction is not required to have a treaty to request extradition from New Zealand. However, New Zealand's extradition regime is supported by four bilateral extradition treaties, 25 multilateral treaties with extradition provisions, the London Scheme for Extradition within the Commonwealth (covering more than 50 jurisdictions) and over 40 pre-existing extradition treaties entered by the United Kingdom before 1947.

504. The Extradition Act does not designate any central authority. MFAT is generally the contact point for all extradition inquiries, except for extradition requests from Australia and the United Kingdom, which follow the "backed-warrant procedure".

505. Under the standard procedure, extradition requests obtained from diplomatic channels (i.e. MFAT) are transmitted to the Minister of Justice. If the extradition request is supported, the Minister of Justice will initiate court proceedings with the assistance of the CLO and will notify the court to issue a warrant for arrest to be executed by the Police. The Court conducts an eligibility hearing to determine whether a person is eligible for surrender. Even if the Court considers a person is eligible for surrender, it is the Minister of Justice who makes the final decision on surrender. In cases of urgent requests, the Court can issue a provisional arrest warrant prior to the Minister of Justice receiving full supporting documentation from the requesting jurisdiction.

506. All extradition requests following the standard procedure are logged onto the same spreadsheet maintained by CLO for MLA requests. This is used for record keeping rather than to aid the counsels in the CLO who are responsible for monitoring the progress of requests. Extradition requests are generally prioritised on a case-by-case basis.

507. For extradition requests from Australia or the United Kingdom, the Extradition Act allows a streamlined process. Such requests come through the Police (i.e. are not

made to the Minister of Justice under the standard procedure), if a warrant for arrest of a person was issued in either of these two countries. The process is managed and assessed by New Zealand Police through its INTERPOL office, which uses a spreadsheet to record all extradition requests. Crown Solicitors in CLO are responsible for court proceedings in New Zealand. The District Court is allowed to make the surrender decision after an eligibility hearing without the need to refer the case to the Minister of Justice, although the Court may choose to do so. This "backed-warrant procedure" is generally a faster, more straightforward process than the "standard procedure".

508. Based on the case examples provided and feedback from the Global Network, extradition requests are generally swiftly considered and executed. However, the assessment team noted that the court proceeding of extradition can sometimes last for years. Between 2016 and 2019, New Zealand received 32 extradition requests in all criminal cases, most of which were handled through the "backed-warrant procedure" (i.e. requesting from Australia or the United Kingdom) and it appears in line with the risk profile of New Zealand. Only one incoming extradition requests related to ML[35] and no extradition request related to TF was received in the past four years. New Zealand had no record of refusing extradition requests, except for cases quashed in the court process. A few cases were discontinued due to various reasons (e.g. the individual was arrested in the requesting jurisdiction). Among those executed extradition requests, the average time to complete was around 8 to 9 months.

Table 8.2. Incoming Extradition Requests

	2016	2017	2018	2019	Total
Extradition request received					
Extradition requests received through standard procedure	0	5	0	1	6
Extradition requests received through backed-warrant procedure	3	8	6	9	26
Outcome of requests received (at March 2020)					
Request executed	1	8	3	4	16
Refused by New Zealand	0	0	0	0	0
In progress	1	2	3	5	11
Discontinued	1	3	0	1	5

509. New Zealand is able to extradite its own nationals pursuant to extradition requests and has not refused an extradition request solely on the grounds of nationality for at least the last fifteen years. Although dual criminality is a requirement for extradition, in assessing whether there is dual criminality, New Zealand authorities take into account the totality of the conduct. It does not matter whether, under the law of the extradition country and New Zealand, the acts or omissions are categorised or named differently or the constituent elements of the offence differ.

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

Mutual legal assistance

510. New Zealand authorities request MLA to the extent needed to build cases. Outgoing MLA requests are prepared and handled by CLO following similar procedures

35 Three more ML-related incoming extradition requests received in 2012 were still under the court process as of the on-site visit.

as incoming requests. Most requests originate from New Zealand Police and the remaining originate from other LEAs like SFO. CLO have provided detailed guidance for prosecuting agencies on how to make a request. During interviews, LEAs communicated their high level of understanding and commitment to requesting assistance when needed and the mechanisms in place are functioning effectively.

Table 8.3. Outgoing MLA Requests

	2016	2017	2018	2019	Total
MLA requests made by New Zealand	20	19	49	50	138
Outcome of requests made (at March 2020)					
Request executed	10	10	26	20	66
Withdrawn by New Zealand	5	3	7	3	18
Refused by requested country	3	2	1	0	6
In progress	0	4	15	27	46

511. As shown in Table 8.3, New Zealand is seeking more assistance from foreign jurisdictions to purse cases locally since 2018, although the authorities did not identify any specific reason for the increase. Similar to incoming requests, the spreadsheet used by CLO cannot break down the requests made by offence accurately (see R33). New Zealand noted that there were around 13 ML-related MLA made between 2014 and 2019, and a few terrorism-related MLA requests made after the Christchurch attack. Most of these requests were made to Australia and the United States of America.

512. As mentioned in IO.8, New Zealand demonstrated its willingness to pursue proceeds of crime located offshore when opportunities present. Between 2016 and 2019, New Zealand also made five asset restraint requests and two forfeiture requests to foreign jurisdictions, resulting in offshore assets worth NZD 8 615 000 being restrained (from the United Kingdom and Fiji) and NZD 1 432 600 forfeited. New Zealand has also repatriated proceeds of crime outside of the formal asset forfeiture process. In one case in 2017, New Zealand repatriated NZD 12 866 310 from Hong Kong, China as part of a settlement order. At the time of the onsite, New Zealand also had a large domestic restraint action underway that required funds to be repatriated to New Zealand from Russia.[36]

Extradition

513. Part 6 of the Extradition Act governs extradition to New Zealand. Similar to extradition from New Zealand, extradition under the standard procedure is processed by Minister of Justice and the CLO while those under the "backed-warrant procedure" (i.e. requests to Australia or the United Kingdom) are handled by the Police. Regardless of the requested jurisdictions, INTERPOL and Police Legal Services provide assistance to requesting LEAs or CLO to liaise with foreign counterparts throughout the extradition process. In determining whether to request for extradition, a number of factors are considered, including the seriousness of offence, likely sentencing, cost and location of individuals.

36 In April 2020 after the onsite, the New Zealand ARU restrained NZD 140 million worth of bank funds relating to this case.

Table 8.4. Outgoing extradition requests

	2016	2017	2018	2019	Total
Extradition request made					
Outgoing extradition requests through standard procedure	4	2	5	3	14
Outgoing extradition requests through backed-warrant procedure	7	12	6	4	29
Outcome of request made (at March 2020)					
Completed	7	11	6	2	26
Refused by other country	1	0	1	0	2
In progress / inactivated	3	3	4	5	15

514. Table 8.4 shows the number of extradition requests made by New Zealand between 2016 and 2019, which demonstrates that New Zealand's willingness to pursue individuals for being extradited back to the country. Only 4 out of the 43 cases related to ML and none related to TF or terrorism. Over half of these requests were made to Australia.

Box 8.2. Example of extradition

Operation Moa was the New Zealand end of an investigation into an Eastern European based organised crime group which moved drugs around the globe.

In late 2016, a group of Polish nationals travelled to New Zealand to import cocaine and launder the proceeds of crime. Between September and July 2017, they travelled between New Zealand and Poland and back, and attempted to remit sums of money.

In June 2018 and July 2018, two of the Polish nationals were arrested pursuant to INTERPOL Red notices in Germany and Venezuela respectively. New Zealand requested extradition of two of the Polish nationals from Venezuela and Germany. Both requests were approved and the two nationals were successfully extradited back to New Zealand in October 2019 (from Venezuela) and January 2019 (from Germany). The two individuals are now facing ML and drug charges in New Zealand.

Seeking and providing other forms of international co-operation for AML/CFT purposes

515. New Zealand engages actively in all areas of informal international co-operation and is achieving good results from successful cross-border co-operation. Competent authorities regularly seek forms of international co-operation, other than MLA or extradition, to exchange relevant information in an appropriate and timely manner with foreign counterparts. Competent authorities also participate actively in various international AML/CFT fora and networks. Informal co-operation is largely effective in exchanging information and supporting operational activity with foreign counterparts.

Exchange of Financial Intelligence & Law Enforcement Information

516. The NZPFIU co-operates well with foreign FIUs, both members and non-members of the Egmont Group. While NZPFIU can share information without the need

for formal information sharing arrangements, it has entered into 10 co-operation agreements with worldwide counterparts, including Australia and China. The Egmont Secure Web is used for information exchanges, along with other protected channels (e.g. face-to-face meetings through police liaison officer network). Between 2016 and 2019, NZPFIU responded to over 380 requests for information and made over 180 requests for information. It also disseminated over 500 intelligence reports to foreign FIUs or LEAs during the same period. Overall, NZPFIU has demonstrated that it actively provides assistance to foreign counterparts and makes spontaneous disclosures. Case examples also demonstrate a proactive approach by the NZPFIU to seek assistance internationally (see Box 8.3).

517. New Zealand Police maintain close ties and often work directly with foreign counterparts through the INTERPOL National Central Bureau (NCB). The Police regularly exchange information with foreign counterparts, and NCB receives approximately 25 000 emails per month relating to all forms of criminal activities. The Police have also developed co-operation through its police liaison officer network. Currently there are 15 police liaison officers deployed in major Asia-Pacific jurisdictions and international financial centres, and there is a plan for further expansion of the liaison officer network. The Police participates in various police-to-police networks, such as the Five Eyes Law Enforcement Group and Heads of FIU, Asset Recovery Interagency Network - Asia Pacific (ARIN-AP) and the Camden Asset Recovery Inter Agency Network (CARIN). The Police also hosts the Pacific Islands Chiefs of Police Secretariat and has entered into numerous MOUs and MOAs with foreign partners. The police liaison officer network and agreements entered are generally in line with New Zealand's geographical risk exposure identified in the NRA.

518. Customs maintains close ties with international customs organisations including those in the Border Five (New Zealand, Australia, Canada, the United Kingdom and the United States of America). Co-operation with foreign counterparts includes the exchange of information, creation of joint analytical products and conducting joint operational activities. Customs has a network of 12 overseas liaison officers deployed to various jurisdictions (e.g. the United States of America, Australia, China and Indonesia) and will increase to 14 in 2020.

519. IR conducts exchange of information with numerous tax treaty partners pursuant to 40 Double Tax Agreements, 19 Tax Information Exchange Agreements and the Multilateral Convention on Mutual Administrative Assistance in Tax Matters. IR actively responds to overseas requests for information and made spontaneous disclosures to foreign tax partners (Table 8.5).

Table 8.5. International Co-operation by Inland Revenue

	2016	2017	2018	2019
Requests for information				
Incoming	72	75	64	85
Outgoing	174	121	93	78
Spontaneous disclosure				
Incoming	26	17	19	18
Outgoing	29	28	31	12

520. SFO often assists overseas agencies in investigating fraud and corruption matters with a New Zealand connection. SFO from time to time shares information with overseas agencies through gateways provided in the *Serious Fraud Office Act 1990* (SFO

Act) (e.g. sections 36 and 51). SFO also deploys an officer as New Zealand's representative at the International Anti-Corruption Co-ordination Centre hosted by the National Crime Agency in London.

521. New Zealand provides a wide range of technical assistance and training to Pacific Island jurisdictions. LEAs provide direct support to investigative partners in the Pacific. For example, the ARU and SFO are regularly involved in supporting Pacific Island jurisdictions in relation to asset recovery, fraud, corruption, drug and ML investigations. They would also assist with TF if an investigation was required. The NZPFIU has developed a programme of assistance for Pacific Island jurisdictions in conjunction with the APG and the Asian Development Bank.

Box 8.3. Cases involving FIU/LEA and foreign counterparts

Case 1 – NZPFIU and NZ Police international co-operation

In 2019, the NZPFIU identified funds moving into New Zealand to the value of USD 11.85 million through the submission of an STR. The funds were sent to New Zealand by R who was resident in the United States. Police investigation identified that R's husband was subject to active crisminal investigation associated with corruption. In response to the investigation, the High Court granted a restraining order on the basis that the funds had entered New Zealand with the intention of concealing the illicit origin of the funds. R appealed the order on the basis that the Police should have sought a foreign generated order. The Court of Appeal dismissed the appeal and considered that the actions of the Police were appropriate in response to suspected international ML.

In the course of this investigation, Police conducted a large amount of international outreach. Five MLA requests were sent to overseas jurisdictions – one each to Panama, Switzerland, and Venezuela; and two to the Bahamas. Additionally, 13 Egmont requests were successfully made in order to reconstruct the travel movements of R and to establish evidence of banks accounts in her control. The case remained underway at the time of the onsite.

Case 2 – IR international co-operation

The tax authority in a foreign jurisdiction identified 11 individuals who, by using 45 local and 56 foreign companies, had been involved in a series of carousel schemes. They were attempting to obtain at least NZD 52 million in allegedly fraudulent VAT/GST refunds and rebates, of which NZD 5 million was an actual loss to that foreign jurisdiction. The tax authority in the foreign jurisdiction identified five third-party New Zealand companies and four purported New Zealand bank accounts, which were used in the carousel fraud. The New Zealand companies were unaware of their names being used to carry out VAT/GST fraud in the foreign jurisdiction. Similarly, bank details such as account numbers and branch locations provided to that treaty partner were also incorrect and did not exist.

As a result, the relevant tax authority in the foreign jurisdiction approached IR for assistance. They requested travel movements of the 11 individuals to and from New Zealand, copies of any Customs declaration and related documentation showing what goods were imported to and exported from New Zealand during the relevant period and affidavits from each of the New Zealand company directors and the banks' tax managers. All this information was provided to the relevant tax authority in the foreign jurisdiction to be used in a criminal case against the 11 individuals.

AML/CFT Supervisors

522. The supervisors engage in close international co-operation with their Australian counterparts (e.g. AUSTRAC and ASIC), in respect of the supervision of reporting entities which have Australian operations or ownerships. All supervisors participate in multilateral groups and fora (e.g. International Supervisors' Forum and informal supervisors' forum with Pacific jurisdictions).

523. RBNZ has been enhancing its international co-operation with foreign counterparts, in addition to intelligence sharing with AUSTRAC and engagement in multilateral for a, which has been ongoing since 2015. Since 2019, before conducting on-site inspections on registered banks, which are part of overseas banking groups, RBNZ has made request for supervisory information from home regulators. In November 2019, a representative from AUSTRAC attended the on-site inspection for an Australian-owned registered bank and RBNZ is intending to extend a similar invitation to attend the on-site inspections of other Australian-owned registered banks. A reciprocal arrangement for RBNZ representatives to attend on-site inspections undertaken by AUSTRAC when there is a nexus to New Zealand is also being considered. Given that the four largest banks in New Zealand are Australian-owned banks, co-operation with AUSTRAC should be strengthened further.

524. FMA regularly complies with requests from overseas regulators made under the IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information (IOSCO MMoU), bilateral MoUs and other co-operation agreements in relation to their investigations. For example, in 2018, the FMA co-operated with 36 requests made under the IOSCO MMoU. Some of these requests related to investigations of potential predicate offending by VASPs. The FMA is very involved with IOSCO, including currently co-chairing the Assessment Committee and as a member of the Committee on Enforcement and Exchange of Information.

525. DIA often co-operates with foreign counterparts particularly on AML/CFT supervisory matters relating to casinos and MVTS. There were also cases relating to DNFBP sectors (e.g. TCSPs and HVDs) and VASPs. For example, in 2019 DIA engaged in 22 co-operation cases, including requests for information on particular reporting entities, with foreign counterparts. Nine of these related to AUSTRAC.

Box 8.4. Co-operation provided by FMA and foreign counterparts

In 2018, FMA assisted the securities regulator in Australia with its investigation into a potential insider trading case and the securities regulator are signatories of the IOSCO multilateral MOU. FMA issued notices under sections 25 and 31 of the FMA Act to obtain information and to require witnesses and potential suspects to attend interviews, which FMA facilitated for investigators from the securities regulator in Australia.

526. Similar to LEAs, New Zealand's AML/CFT supervisors also provide assistance to Pacific Island jurisdictions, RBNZ provided technical assistance in one Pacific Island jurisdiction and hosted other overseas supervisors to share supervisory expertise. DIA is providing technical assistance focusing on casino supervision in one Pacific Island jurisdiction, which is part of APG's five-year Pacific AML/CFT Capacity Development Programme funded by New Zealand.

International exchange of basic and beneficial ownership information of legal persons and arrangements

527. New Zealand shares basic and beneficial ownership information of legal persons and arrangements with international counterparts. The Companies Register is a publicly searchable database maintained by MBIE, which includes information on the company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers, and a list of directors. Relevant authorities, such as the New Zealand Police, are able to access this information and share with their foreign counterparts.

528. Authorities such as the NZPFIU, the New Zealand Police and IR, have also responded to requests, including the use of non-coercive powers to obtain additional beneficial ownership information. For instance, the NZPFIU has shared relevant beneficial ownership information contained in the SARs (relating to both legal persons and arrangements with its foreign counterparts). Supervisory authorities seldom shared beneficial ownership information with their foreign counterparts, and usually these requests would be referred to the LEAs to process. MLA channels have been used when coercive measures are required, and production orders are used to obtain CDD information from reporting entities.

529. IR has shared beneficial ownership information to tax treaty partners relating to New Zealand Foreign Trusts (see IO5). IR reports a low number of requests from foreign partners, with 47 information exchange requests in four years and a 100% success rate in providing beneficial ownership information. However, there are no broader statistics on how often basic and beneficial ownership information is provided to foreign counterparties.

Box 8.5. Exchange of beneficial ownership information relating to New Zealand Foreign Trust

An overseas data leak showed a non-resident funnelling royalty income through a shell company in a low-tax jurisdiction and the company was owned by a New Zealand Foreign Trust. IR then received a request for assistance from another jurisdiction under its international tax treaty network. At the time of the leak, IR was already investigating the New Zealand trustee, so it expanded the investigation to obtain the information sought and provided it to the relevant jurisdiction. The information provided showed that the person in question was the settlor and beneficial owner of the New Zealand Foreign Trust. The jurisdiction successfully prosecuted the person for tax fraud.

Overall Conclusions on IO.2

530. Overall, New Zealand has many of the characteristics of an effective system in the area of international co-operation. New Zealand authorities provide MLA, extradition and exchange information in a constructive and timely manner to a large extent, and proactively seek international co-operation when required; only minor improvements are needed. This includes a holistic review of MACMA and the Extradition Act; keeping better statistics; and strengthening supervisory co-operation.

New Zealand is rated as having a high level of effectiveness for IO.2.

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2009.[37]

Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation which was not assessed in New Zealand's 3rd MER.

Criterion 1.1 - New Zealand has a three-tiered risk assessment system to identify and assess its ML/TF risks. The NRA assesses the risk as a function of threats, vulnerabilities and consequences and describes the scale and nature of the ML/TF risks faced by New Zealand at the national level. The supervisors (RBNZ, DIA and FMA) produce more specific assessments of the risks faced by each sector (SRAs). Reporting entities are required by the AML/CFT Act to produce their own assessments of the risks posed by their customers and the services provided to them.

The NRA and SRAs use a wide range of information, including analysis of information from the FIU and other LEAs, macro-economic information from domestic and international organisations, feedback of supervisors and inputs from the private sector.

TF risk was included in the first (2010) and second (2015) NRA. During 2018-19 these assessments were built on using a greater range of open source and classified material to form a comprehensive TF risk assessment module.

Criterion 1.2 - New Zealand has designated the National Co-ordination Committee (NCC) as the lead authority to co-ordinate actions to assess ML/TF risks (sections 150-152 of the AML/CFT Act). The AML/CFT Act casts specific responsibility on the NZ Police, MOJ, NZ Customs and the supervisors to assess risk.

Criterion 1.3 - New Zealand keeps its NRA and SRAs up-to-date. Two iterations of the NRA have been conducted in 2010 and 2013-15 with updates made to the second NRA in 2016, 2017 and 2019. A public version of the NRA was published in 2010, 2018 and updated in 2019.

The AML/CFT supervisors first published SRAs in 2011. During 2017-2018 each of the supervisors published new SRAs for their supervised sectors. DIA also published a further SRA for the newly captured DNFBP sectors in 2017 (Phase 2 entities). The DIA also updated both its SRAs in 2019. In this respect, there are a total of four SRAs across the three supervisors.

37. This report is available at www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationofnewzealand.html

The NRA includes recommendations for its review and updating within 18 months and for its reassessment every five years. However, reassessments and updates can be conducted earlier if events if the circumstances require it. There are no prescribed time frames to update SRAs, however, in practice updates are triggered by updates in the NRA.

Criterion 1.4 - New Zealand has mechanisms to provide information on the NRAs and SRAs to all relevant competent authorities and reporting entities. The NCC is mandated to facilitate the dissemination of information on ML/TF risks (section 152 of the AML/CFT Act). The current generation of the NRA is produced as a restricted document, which is distributed to relevant agencies. A public version is then published on Police's website and available to all reporting entities.[38]

Supervisors publish their SRA on websites and the FIU alerts the reporting entities when risk assessments are published. The supervisors and the FIU conduct frequent outreach and training on ML/TF risk and the findings of the NRA/SRAs.

Criterion 1.5 - New Zealand applies a risk-based approach for resource allocation and for implementing measures to prevent or mitigate ML/TF. The risk-based approach is evident from the budgetary resource allocation among various authorities following the second NRA in 2015 (as evident through Cabinet Papers in May 2017). This process, co-ordinated through the NCC, led to New Zealand's Phase 2 reforms to the AML/CFT Act. This provided for substantial funding for activity to mitigate the risks identified by the NRA and supplementary assessment of the DNFBP sectors' ML/TF risks. This included funding to the DIA for additional supervisory staff; funding to the Police for dedicated ML investigation teams and investment in the SFO for a new integrated case and evidence management system. The supervisors also use the SRAs as their basis for risk-based resource allocation.

Criterion 1.6 - New Zealand allows for regulatory and ministerial exemptions to modify the standard requirements of the AML/CFT Act in certain circumstances.

The New Zealand Governor-General has the power to make exemptions of classes of reporting entity and services through regulations (section 154 of the AML/CFT Act). Classes of reporting entity are exempted from all AML/CFT obligations in the *AML/CFT (Definitions) Regulations 2011*. Classes of reporting entities are exempted from AML/CFT obligations for certain services in the *AML/CFT (Exemptions) Regulations 2011*. These exemptions are granted only after taking into account multiple factors. These factors includes ML/TF risk but also include other factors such as the regulatory burden (section 154(3)). Accordingly, there is not an explicit requirement that there be proven low risk of ML/TF prior to granting of an exemption. While proven low ML/TF risk appears to be present in most exemptions, this was not demonstrated in all exemptions granted (e.g. certain historical and transitional exemptions in relation to special remittance facilities, providers of some family trusts and pawnbrokers (see R22)).

In addition, the Minister for Justice can exempt individual reporting entities from all, or some, AML/CFT obligations through a ministerial notice (section 157 of the AML/CFT Act).[39] The Minister has granted approximately 120 entities individual entities and has exempted 12 classes of services. The exemptions are granted after

38 www.police.govt.nz/sites/default/files/publications/fiu-nra-2019.pdf,

39 www.justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/info-for-businesses/ministerial-exemptions/decisions/

taking into account multiple factors, which includes ML/TF risk but also includes the regulatory burden (section 157(3)). These exemptions, however, appear to be on the basis of low risk of ML/TF and occur in strictly limited and justified circumstances.

Criterion 1.7

(a) Where New Zealand has identified higher risks, these are addressed through the AML/CFT Act. Reporting entities are required to apply EDD measures in identified scenarios of higher risk (sections 22 and 23 of the AML/CFT Act).

(b) Reporting entities are also required to take into account any applicable guidance material produced by the supervisors or the New Zealand Police relating to risk assessments (section 58 of the AML/CFT Act).

Criterion 1.8 - New Zealand permits reporting entities to conduct simplified CDD when dealing with certain customers (section 18 of the AML/CFT Act). This list includes customers which have the characteristics of a low ML/TF risk and others that are subject to other disclosure standards and controls by their supervisors. This includes government agencies, registered banks, licenced insurers and companies whose equity securities are listed in New Zealand (or overseas equivalent). These categories were assessed a low level of ML/TF risk during the legislative process for the AML/CFT Act and are consistent with the types of low-risk businesses included in the FATF Standards.

The requirement to conduct simplified CDD is not mandatory as a reporting entity *may* conduct simplified CDD in the circumstances listed in section 18(2). This implies that a reporting entity could instead, based on its assessment of ML/TF risk of the customer or transaction, undertake standard or EDD (see also R10.18).

Criterion 1.9 - Reporting entities are required to conduct ML/TF risk assessments (section 58 of the AML/CFT Act). The supervisors must ensure that reporting entities are implementing their ML/TF risk assessment obligations, as they are required to monitor reporting entities for compliance with the Act and investigate reporting entities and enforce compliance with the Act (section 131(b) and (d) of the AML/CFT Act). See analysis of R26 and R28 for more information.

Criterion 1.10 - Reporting entities are required to take appropriate steps to identify, assess and understand their ML/TF risks (section 58 of the AML/CFT Act). Reporting entities must:

a) document their risk assessment (section 58 of the AML/CFT Act).

b) consider customers, countries or geographic areas; and products, services, transactions or delivery channels in the risk assessment (section 58(2)).

c) keep their risk assessments up-to-date (section 58(3)(b)).

d) have mechanisms in place for reporting entities' risk assessment to be provided to competent authorities. Section 132(2) of the AML/CFT Act provides supervisors with the power to require production or access to all records, including risk assessments.

Criterion 1.11 - Reporting entities must:

a) have an AML/CFT programme that includes internal procedures, policies and controls to detect ML/TF and to manage and mitigate the risk (section 56(1) of the AML/CFT Act). There is no requirement however that the program be approved by senior management.

b) monitor its risk assessment and AML/CFT programme to identify any deficiencies and make the necessary changes (section 59(1)).

c) determine when EDD is required (section 57(1)(j)). Reporting entities' AML/CFT programme must be based on their risk assessment and it must set out how they will manage and mitigate ML/TF risk (section 57(1)(f)).

Criterion 1.12 - New Zealand permits reporting entities to carry out simplified CDD on a range of prescribed low risk customers (section 18 of the AML/CFT Act). There is no prohibition from carrying out simplified CDD on these customers where there is a suspicion of ML/TF. However, reporting entities must undertake EDD as soon as practicable after becoming aware that a suspicious activity must be reported (section 22A(2)). However, when a transaction is conducted outside the business relationship for an amount below the threshold value, there is no requirement to do CDD (see R10.18).

Weighting and Conclusion

New Zealand exempts many classes of reporting entities, which are not all strictly based on demonstrated low ML/TF risk. There is no explicit prohibition from carrying out simplified CDD where there is a suspicion of ML/TF. There is no requirement that reporting entities' AML/CFT programmes are approved by senior management. These are minor deficiencies.

Recommendation 1 is rated largely compliant.

Recommendation 2 – National Co-operation and Co-ordination

In its 3rd MER, New Zealand was rated compliant with these requirements. The agencies involved in New Zealand's AML/CFT regime have remained largely the same since then.

Criterion 2.1 - The MOJ leads the development of AML/CFT policies for New Zealand. It chairs the Oversight Committee, which is responsible for approving national AML/CFT policies. New Zealand's AML/CFT policies are set out in several policy and strategy documents developed by relevant agencies, including submissions to Cabinet. This includes a 2020 National AML/CFT Strategy, developed by the MOJ, which includes an action plan. Other key national policies have included New Zealand's Counter-Terrorism Strategy, All Government Response to Organised Crime, the Methamphetamine Action Plan which were informed by the NRAs.

Criterion 2.2 - The Minister of Justice is responsible for New Zealand's national AML/CFT policies. The MOJ is responsible for providing policy advice to the Government, evaluating the performance of the AML/CFT regime, advising the Government on legislative reform and administering relevant AML/CFT legislation (section 149 of the AML/CFT Act). MFAT is jointly responsible with the MOJ for the terrorism-related TFS regime and policy, and solely responsible for counter-proliferation TFS policy.

Criterion 2.3 - New Zealand has put in place a number of mechanisms to co-ordinate policy and operational issues related to AML/CFT and exchange information. The NCC, established under section 150 of the AML/CFT Act, comprises the MOJ, Customs, the supervisors, the New Zealand Police (including the FIU) and IR. The NCC is New Zealand's main AML/CFT co-ordinating body and meets monthly. An Oversight Committee comprising executive representatives from DIA, NZ Police, Customs, SFO,

FMA, RBNZ and MOJ meet every quarter. A Sector Supervisors' Forum comprising the three supervisors meets fortnightly to support co-ordination of operational matters and facilitate consistency among supervisors and information sharing. The MOJ and the FIU also attend.

Criterion 2.4 - New Zealand has co-operation and co-ordination mechanisms for CPF. An inter-agency Counter-Proliferation Forum, which includes a focus on PF, was established in 2018 and meets two to three times per year. The forum is multi-agency and multi-sector. The purpose of the forum is to connect interested agencies, to allow for information sharing and collaboration on counter-proliferation and CPF work. The forum includes representatives from agencies responsible for export controls (MFAT and Customs), movement of people (MBIE), scientific research (MBIE), finance (MOJ and the Police), as well as intelligence and defence agencies.

Criterion 2.5 - The *Privacy Act 1993* permits the sharing of information for law enforcement purposes (see R9). This is reinforced by specific provisions in the AML/CFT Act, the *Criminal Proceeds (Recovery) Act 2009* (CPRA) and the *Tax Administration Act 1994* (TA Act). Inter-agency MOUs are adopted where required (but usually are not). Privacy impact assessments are used by agencies to determine the impacts of proposed reforms on privacy, such as when New Zealand introduced the new AML/CFT regime in 2009. The New Zealand Privacy Commissioner has released guidance on situations where an entity has been asked by Police or a law enforcement agency to release personal information and when information can be shared.

Weighting and Conclusion

Recommendation 2 is rated Compliant.

Recommendation 3 – Money laundering offence

In its 3rd MER, New Zealand identified shortcomings that have been addressed by amendments to the Crimes Act 1961. The legislation required that the ML activity was committed for the purpose of concealing or helping someone else conceal the property, that not all designated offences qualified as predicate offences and self-laundering of proceeds was not covered.

Criterion 3.1 - New Zealand criminalises money laundering under s 243 of the *Crimes Act 1961*. The wording of s 243 closely follows the wording of Article 3(1)(b) of the Vienna Convention and Article 6(1)(a) of the Palermo Convention. The offence has the following main elements:

a) the defendant engaged in a money laundering transaction in respect of property that was the proceeds of an offence:

b) the defendant knew or believed that all or part of the property was the proceeds of an offence or was reckless as to whether all or part of the property was the proceeds of an offence.

A person engages in a money laundering transaction if, in concealing any property or by enabling any other person to conceal property, the person deals with property or assist the other person, directly or indirectly to deal with the property.

"Conceal" is defined to mean to conceal or disguise property, including by converting the property from one form to another, or to conceal or disguise the nature, source, location, disposition or ownership of property or any interest in property. The

shortcoming identified in the 2009 MER of requiring proof of intent to conceal has now been addressed through the enactment of subsection 243(4A) which states that the prosecution is not required to prove intent to conceal any property or intent to enable any person to conceal any property.

The Crimes Act includes a number of other offences that are also relevant to the criminalisation of money laundering. Under subsection 243(3) a person who obtains or has possession of property with intent to engage in a money laundering transaction also commits an offence. Section 246 criminalises the receiving of property that is stolen or obtained by another imprisonable offence, knowing or being reckless as to whether the property had been stolen or so obtained. The receiving offence is sufficiently broad to support prosecution of cases that would fall under the 'possession' or 'use' limbs of the Vienna and Palermo convention offences, given that receiving does not require transfer of ownership.

Criterion 3.2 - New Zealand introduced an all crimes approach to predicate offences in 2015. This addressed previous findings in New Zealand's 2009 MER that illicit arms trafficking offences did not qualify predicate offences for ML given their low penalties.

Criterion 3.3 - New Zealand does not apply a threshold for criminal offences to constitute predicate offences for money laundering.

Criterion 3.4 - Property is broadly defined in section 243 of the Crimes Act 1961 and covers real and personal property of any description.

Criterion 3.5 - Money laundering is a standalone offence in section 243 of the Crimes Act 1961. It is not necessary to that a person be convicted of a predicate offence to prove property is proceeds of crime. Subsection 243(5) also makes clear that is not necessary for the prosecution to prove that the defendant knew or believed the property was the proceeds of a particular offence or class of offence. The Court of Appeal has also found that it is not necessary for the prosecution to prove that a particular predicate offence had occurred, or that the person accused of money laundering had been involved in that offending (*R v Allison* [2005] 1 NZLR 721).

Criterion 3.6 - The definition of "offence" is section 243 of the Crimes Act includes any offence, wherever committed, that would be an offence in New Zealand if committed in New Zealand. This means that the proceeds of such offences are included within the scope of the money laundering offences in section 243. Section 245 of the Crimes Act narrows the scope of predicate offences by requiring that the act resulting in proceeds was also an offence where and when it was committed or was a New Zealand offence that had extraterritorial effect. This is consistent with criterion 3.6.

Criterion 3.7 - Money laundering is a standalone offence, and a person can be convicted of its regardless of whether they have, or have not, been convicted of a predicate offence. In cases of self-laundering, the courts have held that the laundering must follow a discrete antecedent offence (*R v Harris CA15/00 [2000]*). This has not prevented authorities from charging self-laundering but has guided how such charges are drafted to avoid duplicity.

Criterion 3.8 - Under the common law as applicable in New Zealand, *mens rea* (intent or knowledge) may be inferred from factual circumstances.

Criterion 3.9 - Money laundering is punishable by 7 years' imprisonment and the offence of obtaining or possessing property with intent to engage in money laundering is punishable by 5 years' imprisonment (sections 243(2) and (3) Crimes

Act). The offence of receiving property that is stolen or obtained from an imprisonable offence is punishable by up to 7 years' imprisonment depending on the value of the property, with the highest level of imprisonment apply for property in excess of NZD 1 000 (section 247 Crimes Act). Under section 39(1) of the Sentencing Act 2002, the courts may impose a fine instead of imprisonment. No fine is specified for money laundering, and fines have been rarely applied: for individuals, in low-level cases, and for a legal person at a higher level (NZD 102 400 for a money remitter providing services recklessly in 2006-2007, calculated from a starting point of 10 times the proceeds). Fines are determined by reference to provisions of the Sentencing Act 2002 (sections 7, 8, 9, 13, 39 and 40), taking into account the gravity of the offending in the particular case, including the degree of culpability of the offender, as well as the financial capacity of the offender (which may increase or decrease the amount). These penalties are proportionate and dissuasive, being comparable to penalties imposed for other serious offences, including predicate offences, under New Zealand law.

Criterion 3.10 - Criminal liability and sanctions for money laundering apply to legal persons. Section 2 of the Crimes Act 1961 includes a broad definition of "person" which extends to (among other things) bodies of persons, whether incorporated or not. Subsection 39(1) of the Sentencing Act 2002 permits the imposition of a fine on legal persons instead of imprisonment.

Criterion 3.11 - The Crimes Act 1961 criminalises the attempt to commit money laundering (sections 72 and 311), participating in money laundering (subsection 66(1)), conspiracy to commit money laundering (section 310), aiding and abetting and counselling (sections 66(1) and 311(2)) and contributing to the commission of money laundering by a group of persons acting with a common purpose (sections 66(2) and 310).

Weighting and Conclusion

Recommendation 3 is rated Compliant.

Recommendation 4 – Confiscation and provisional measures

In the previous ME, NZ was rated largely compliant as the forfeiture of proceeds and instrumentalities of crime did not cover all designated predicate offences (for example, illicit arms trafficking was not covered).

Criterion 4.1 - In 2009, New Zealand enacted the Criminal Proceeds (Recovery) Act 2009 which extended the scope of proceeds subject to forfeiture to the proceeds of any criminal offence of NZD 30 000 or more. The introduction of the all crimes approach to predicate offences in 2015 also addressed previous concerns about the ability of authorities to confiscate the proceeds of money laundering associated with illicit arms trafficking offences.

Additionally, in 2019 New Zealand amended the *Arms Act 1983* to introduce offences of importing and selling prohibited firearms, magazines and parts with penalties of 5 years' imprisonment. These changes addressed the specific shortcoming in relation to illicit arms trafficking offence.

New Zealand has in place legislative measures that enable the confiscation of the following:

(a) Property laundered - Laundered property is subject to a civil forfeiture regime under the CPRA. A court may issue an "assets forfeiture order" where it is satisfied on

the balance of probabilities that property is tainted property. "Tainted property" includes property that has been, wholly or partly, acquired from significant criminal activity or derived, directly or indirectly, from at least one activity that was a significant criminal activity. Property may be tainted property even if owned by a third party who did not commit the offence.

"Significant criminal activity" is defined as an activity that if proceeded against as a criminal offence would amount to offending: (a) that consists of, or includes, one or more offences punishable by a maximum term of imprisonment of 5 years or more; or (b) from which property, proceeds, or benefits of a value of NZD 30 000 or more have, directly or indirectly, been acquired or derived.

A separate, conviction-based forfeiture regime is established under section 32 of the *Misuse of Drugs Act 1979*, allowing courts, upon conviction, to make orders forfeiting money received from the offence and in the possession of the convicted person, as vehicles, aircraft, boats and other vessels in which the convicted person has an interest.

(b) Proceeds of (including income or other benefits derived from such proceeds, or instrumentalities used or intended for use in money laundering, or predicate offences - The proceeds of money laundering may be forfeited; such proceeds would be "tainted property" under the CPRA, due to the penalty for money laundering being 7 years' imprisonment. The proceeds of predicate offences with penalties of 5 years' imprisonment or more would similarly be "tainted property". In any event, the proceeds of any offence from which NZD 30 000 or more have been derived or acquired may be the subject of an asset forfeiture order.

The concept of "tainted property" extends to property directly or indirectly derived from an activity or activities, at least one of which is a significant criminal activity. This has been widely interpreted by the courts, see *Commissioner of Police v Ranga* [2013] NZHC 745, and may be used to forfeit income or other benefits derived from proceeds

A separate confiscation power exists for instrumentalities of crime under the Sentencing Act. A court may order the confiscation of instrumentalities where a person has been convicted of a "qualifying instrument forfeiture offence", defined in the Sentencing Act and CPRA as "an offence punishable by a maximum term of imprisonment of 5 years or more". Qualifying instrument forfeiture offences also include attempt, conspiracy, or being an accessory if the maximum term of imprisonment for that attempt, conspiracy, or activity is 5 years or more.

(c) Property that is the proceeds of, or used in, or intended or allocated for use in the financing of terrorism, terrorist acts or terrorist organisations, or - The offence of financing of terrorism under the Terrorism Suppression Act 2002 (TSA) is punishable by 14 years' imprisonment, therefore both the financing of terrorism and attempted financing of terrorism meet the threshold for significant criminal activity, the proceeds of which may be forfeited as well as threshold for qualifying instrument forfeiture offence.

In addition, under the TSA, the court can order the forfeiture of property subject to asset freezing obligations pursuant to counter-terrorism sanctions regimes. In considering such an order, the court must consider whether it is more appropriate for the property to remain subject to the freezing obligation or forfeited to the government.

(d) Property of corresponding value - Under the CPRA, the High Court may issue a "profit forfeiture order" for property up to the corresponding value of proceeds. Such an order allows for the forfeiture of untainted property to the Crown, where any person with an interest in the property has, on the balance of probabilities, unlawfully benefited from significant criminal activity.

Criterion 4.2

(a) Under the CPRA, competent authorities are able to identify and trace property that is subject to confiscation or is suspected of being the proceeds of crime through search warrants, production orders, examination orders and other relevant provisions that require disclosure of ownership and other relevant information. The Official Assignee can seek a warrant for the purposes of assessment and evaluation of any property that is subject to either restraint or forfeiture.

(b) Under the CPRA, competent authorities are able to restrain or freeze property that is subject to confiscation via restraining order relating to specific property, all or part of respondent's property or an instrument of crime. Competent authorities can also seek foreign restraining orders. The effect of a restraining order is that the property cannot be disposed of or dealt with other than as provided in the restraining order and it is put under the custody and control of the Official Assignee. In addition to asset freezing under the TSA (see Recommendation 6 below), the Prime Minister may direct the Official Assignee to take custody and control of property in New Zealand if the Prime Minister believes on reasonable grounds that the property is owned or controlled, directly or indirectly, by a designated terrorist entity (either UN or locally designated) or derived or generated from property of that kind.

(c) Under the CPRA, the court has wide powers to void an arrangement which has the intent of defeating, avoiding or impeding the operation of the CPRA or the forfeiture provisions of the Sentencing Act, to recognise effective control over the property as well as to set aside a disposition or dealing in respect of restrained property that contravenes a restraining order (including registered forfeiture orders).

(d) Authorities have a wide range of investigative powers outlined under legislation, including the CPRA and the Search and Surveillance Act 2012. This includes but is not limited to production orders, and examination orders.

Criterion 4.3 - The rights of bona fide third parties are protected under the CPRA and the TSA. The CPRA requires applications for restraining orders to identify the proposed property, the respondent (if any) and any other person to the knowledge of the applicant and that subsequent applications be served on the respondent and all third parties and interested parties. There is also a mechanism to allow a person (other than the respondent) who has an interest in the property covered by an application for a civil forfeiture order to apply to the court for relief.

Criterion 4.4 - The CPRA directs the Official Assignee to take into custody and control assets that are ordered to be restrained or forfeited by a Court. It also directs the Official Assignee to: dispose of confiscated assets (being both instruments of crime forfeited under the sentencing provisions of the Sentencing Act and assets confiscated under Asset Forfeiture Orders in civil cases), dispose of assets that have been restrained to meet a Profit Forfeiture Order (PFO) in civil cases as well as enforce PFOs where assets do not meet the amount specified to be repaid by the respondent. The Official Assignee has the statutory responsibility, and necessary powers, to preserve and manage property subject to a restraining order, and to administer property subject to a forfeiture order until it is disposed of.

Weighting and Conclusion

Recommendation 4 is rated Compliant.

Recommendation 5 – Terrorist financing offence

Criterion 5.1 - New Zealand criminalises terrorism financing under section 8 of the TSA.

Subsection 8(1) criminalises the provision or collection funds with the intention that they be used, or knowing that they are to be used, in full or in part, in order to carry out one or more acts of a kind that, if they were carried out, would be terrorist acts. Subsection 8(2A) criminalises the provision or collection of funds intending that they benefit, or knowing that they will benefit, an entity that the person knows is an entity that carries out, or participates in the carrying out of, one or more terrorist acts.

Section 5 of the TSA defines 'terrorist act' as one of three types of acts which relate to the offences in Article 2(1)(a) and Article 2(1)(b) of the TF Convention.

Subsections (2) and (3) implement the concepts set out in Article 2(1)(b) of the TF Convention, and extend the definition beyond intention to cause death or serious bodily injury to a civilian, to include intention: to a serious risk to the health or safety of a population; destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage; serious interference with, or serious disruption to, an infrastructure facility, if likely to endanger human life; and introduction or release of a disease-bearing organism, if likely to devastate the national economy of a country.

Terrorist acts in situations of armed conflict are covered by paragraph 5(1)(c) of the TSA, consistent with Article 2(1)(b) of the TF Convention.

Acts constituting offences against the treaties in the Annex to the TF Convention, as well as additional conventions relating to terrorism, are brought within the definition of "terrorist act" by paragraph 5(1)(b).

Criterion 5.2 - The analysis of New Zealand's terrorism financing offence as it relates to financing the carrying out of terrorist is set out under criterion 5.1.

The provision or collection of funds or other assets with the intention or knowledge they are to be used by a terrorist organisation or individual terrorist is criminalised by subsection 8(2A) of the TSA. The concepts of "terrorist organisation" and "terrorist entity" are both encompassed within the phrase "an entity that the person knows is an entity that carries out, or participates in the carrying out of, 1 or more terrorist acts". "Entity" is defined in the TSA as including natural and legal persons and arrangements, as well as unincorporated associations and organisations. Subsection 8(3) states expressly that in a prosecution for financing of terrorism, it is not necessary for the prosecutor to provide that the funds collected or provided were actually used, in full or in part, to carry out a terrorist act.

New Zealand's implementation of targeted financial sanctions pursuant to UNSC Resolutions 1267/1989, 1988 and 1373 also prohibit the making available of funds to designated terrorist entities under s 10 of the TSA (analysed under Recommendation 6).

Criterion 5.2bis - New Zealand has not enacted specific offences for individuals who travel to a state other than their state of residence for the purposes related to terrorist

acts or providing or receiving terrorist training.[40] However, the financing of terrorism offences in subsection 8(1) and 8(2A) of the TSA may be sufficiently broad to cover the financing of such acts where the financing is for the benefit of a terrorist entity or where there is sufficient proximity to a terrorist act. While the general terrorism financing offence may have some applicability, it is not clear that this is sufficient to cover all circumstances set out in 5.2*bis*.

Criterion 5.3 - Both the financing of terrorist acts in subsection 8(1) and the financing of terrorist entities offence in subsection 8(2A) cover the provision or collection of funds or other assets; section 4 of the TSA defines "funds" as assets of every kind, whether tangible or intangible, moveable or immoveable, however acquired, as well as legal instruments evidencing title to, or an interest in, assets. There are no limitations on the source of the funds that fall within the scope of the offences.

Criterion 5.4 - Subsection 8(3) of the TSA expressly states that it is not necessary to "prove that the funds collected or provided were actually used, in full or in part, to carry out a terrorist act". Subsection 8(1) also refers to "acts of a kind" that if they were carried out, would be terrorist acts, meaning that a link to specific terrorist act is not needed.

Criterion 5.5 - Under the common law in New Zealand, *mens rea* (intent or knowledge) may be inferred from factual circumstances.

Criterion 5.6 **-** Natural persons that commit terrorism financing offences under section 8 of the TSA are liable to imprisonment for 14 years. Offences against s 10 (targeted financial sanctions) are punishable by 7 years' imprisonment. These penalties are comparable to other serious offences under New Zealand law. Under subsection 39(1) of the Sentencing Act 2002, courts may impose fines instead of imprisonment. Fines are determined by reference to provisions of the Sentencing Act 2002 (sections 7, 8, 9, 13, 39 and 40), taking into account the gravity of the offending in the particular case, including the degree of culpability of the offender, as well as the financial capacity of the offender (which may increase or decrease the amount).

Criterion 5.7 - Criminal sanctions for terrorism financing are applicable to legal persons and are without prejudice to the criminal liability of natural persons. Under sections 7-10 and 40(1) of Sentencing Act a range of factors are taken into account in sentencing that go to proportionality.

Criterion 5.8 - The Crimes Act criminalises the attempt to commit terrorism financing (sections 72 and 311), participating as an accomplice in terrorism financing or attempted terrorism financing (section 66(1)), organising or directing others (sections 66(1) and 311(2)) and contributing to the commission of terrorism financing by a group of persons acting with a common purpose (section 66(2) and s 310).

Criterion 5.9 - New Zealand adopts an all crimes approach to predicate offences for money laundering under section 243 of the Crimes Act, which includes the offence of financing of terrorism.

Criterion 5.10 - The terrorism financing offences in the TSA have extraterritorial effect, including where committed by a New Zealand citizen, a stateless person ordinarily resident in New Zealand, on board an aircraft or ship required to be registered in New Zealand, or by another person in New Zealand who has not been

40 New Zealand has advised that legislation to being considered to create an express offence.

extradited. Section 17 of the TSA extends extraterritorial jurisdiction for terrorism financing offences to any act that is directed towards or resulted in one or more terrorist acts with a connection to New Zealand. There is no requirement for the offence of terrorism financing to occur in the same jurisdiction as the terrorist act, terrorist organisation or individual terrorist.

Weighting and Conclusion

It is not clear whether the general terrorism financing offence is sufficient to cover all circumstances set out in 5.2bis.

Recommendation 5 is rated Largely Compliant.

Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing

In its 3rd MER, New Zealand was rated partially compliant due to shortcomings that included the communication of designations, particularly to the DNFBP, money remitters and securities sectors not being satisfactorily organised, and insufficient practical guidance, particularly to the DNFBP and financial institutions, other than banks, on how to effectively implement the freezing obligations.

Criterion 6.1(a) - The Ministry of Foreign Affairs and Trade (MFAT) is the competent authority for proposing persons or entities to the UNSC Resolutions 1267/1989 and 1988 Committees for designation.

Criterion 6.1(b) - New Zealand has never proposed a designation pursuant to UNSC Resolutions 1267/1989 and 1988 on its own initiative. However, the New Zealand Counter Terrorism Committee has been identified as responsible for identifying targets for designation.

Criterion 6.1(c) - While New Zealand has never proposed a UNSC Resolution 1267/1989 or 1988 designation on its own initiative, authorities indicated that the same evidentiary standard ("reasonable grounds") would be applied when considering such a proposal as currently applies to UNSCR 1373 designations, and that this approach has been adopted for decisions about co-sponsorship of designations proposed by other UN Member States

Criterion 6.1(d) - New Zealand authorities have advised that they would follow the procedures and use the standard forms for listing if New Zealand were to propose a designation under UNSC Resolution 1267/1989 or 1988.

Criterion 6.1(e) - New Zealand authorities have advised that they would follow a similar process for the development of UNSCR 1267/1989 and 1988 designation proposals as used for designations under the TSA. This includes the preparation of a comprehensive statement of case to support the proposed designation.

Criterion 6.2(a) - New Zealand implements UNSCR 1373 through the TSA, which identifies the Prime Minister as the competent authority for interim designations (section 20 TSA) and final designations. The Prime Minister is required to consult the Attorney-General and Minister of Foreign Affairs (for interim designations) and the Attorney-General (for final designations).

However, TSA does not align with the specific criteria for designation as set forth in UNSCR1373 which sets out facilitation of terrorist acts as a standalone ground for implementation of TFS. The designation of persons and entities who facilitate the

commission of terrorist acts (e.g. by financing a terrorist entity without knowing the purposes to which the funds are to be put) is only covered by the power to designate "associated entities", and is therefore conditional on another entity that carried out or participated in those terrorist acts also being designated.

Criterion 6.2(b) - Under New Zealand's 'Terrorist Designations Process' published on the New Zealand Police website, the Terrorist Designation Working Group (TDWG) is responsible for identifying targets for designation pursuant to UNSCR 1373. The TDWG is chaired by the New Zealand Police and comprising the Department of Prime Minister and Cabinet (DPMC), the National Assessments Bureau, the New Zealand Defence Force, Crown Law, the MFAT and the New Zealand Security Intelligence Service. The TDWG makes recommendations to the Security and Intelligence Board, chaired by the DPMC Deputy Chief Executive National Security Group, which makes a final determination on whether to proceed with a recommendation to the Prime Minister.

Criterion 6.2(c) - MFAT conveys requests received from foreign partners to designate an entity pursuant to UNSCR 1373 to NZ Police and other members of the inter-agency TDWG. Consideration is then be given to a range of factors, including the scale of an entity's involvement in terrorist acts or support activity, connections to New Zealand and the likely impact of a designation in New Zealand, and the information available to support any statement of case for designation and the likely priority to be given to the request in light of available resources.

Criterion 6.2(d) - For final designation decisions, the Prime Minister must "believe on reasonable grounds that the entity has knowingly carried out, or has knowingly participated in the carrying out of, 1 or more terrorist acts" (section 22 TSA). Similarly, the Prime Minister must "believe on reasonable grounds" that "associated entities" knowingly facilitated one or more terrorist acts, or is acting on behalf of or at the direction of a terrorist entity or associated entity, or is owned or effectively controlled, directly or indirectly by a terrorist entity or associated entity. In making designation decisions the Prime Minister must, under administrative law, consider all relevant information, which may include classified information (section 30 TSA).While the Prime Minister is given a broad discretion about whether or not to list a person who meets the designation criteria, the Terrorist Designation Process indicates that the guiding consideration would be "whether designation of the relevant entity would effectively assist the suppression of terrorism".

The TSA also permits the Prime Minister to make interim designations for 30 days on the basis of having "good cause to suspect" that entity knowingly carried out, or has knowingly participated in the carrying out of, one or more terrorist acts.

Criterion 6.2(e) - New Zealand has never requested another country to give effect to freezing actions pursuant to UNSCR 1373. Nonetheless, authorities indicated they would provide a wide range of information, including the statement of case to support a designation, if they made such a request. Unclassified versions of statements of case are also available online for all designations.

Criterion 6.3(a) - The TDWG consideration of statements of case for possible designations is informed by information provided by the National Assessments Bureau and the Police National Intelligence Centre. Both are able to draw on a full range of information sources, including information collected by other agencies. MFAT also asks partner countries for views, and information, regarding possible designations.

Criterion 6.3(b) - Section 29 of the TSA states explicitly that a designation decision pursuant to UNSCR 1373 is not invalid just because the entity concerned was not notified or given a chance to comment before the designation decision. This permits designations to be made *ex parte* and designated persons and entities are not notified in advance.

Criterion 6.4 - Section 9 of the TSA makes it a criminal offence to deal with property of a designated terrorist entity. Section 10 makes it a criminal offence to make available, or cause to be made available, directly indirectly, property or any financial or related services to designated terrorist entities. The definition of "designated terrorist entity" automatically incorporates persons or entities designated pursuant to UNSC Resolution 1267/1989 and 1988, or UNSC Resolution 1373. Targeted financial sanctions are therefore immediately effective under the TSA upon designation. Assessors noted that the definition of "Al-Qaida entity" in the TSA is out of date as it refers to "association with Usama bin Laden" rather than ISIL/Al-Qaida, but authorities indicated that this has not created legal uncertainty.

Criterion 6.5(a) - The offence provisions under the TSA apply to all persons including legal persons and unincorporated bodies.

Criterion 6.5(b) - Freezing obligations under the TSA extend to all types of property whether controlled directly or indirectly, wholly or jointly owned, and whether derived or generated from other assets. Some property of persons or entities acting on behalf of, or at the direction of, designated persons or entities is captured by the concept of "indirect control", although this does not extend to *all* property of such persons, e.g. where the property of such persons is not controlled by the designated persons or entities named in relevant sanctions lists. For UNSCR 1373 sanctions, persons or entities acting on behalf of, or at the direction of, designated terrorists may, however, be designated as "associated entities" for UNSCR 1373 sanctions.

Criterion 6.5(c) - Under the TSA, it is a criminal offence to make available, or cause to be made available, directly indirectly, property or any financial or related services to or for the benefit of designated terrorist entities. This does not expressly extend to prohibiting making assets available to entities owned or controlled by designated entities (except for UNSCR 1373 where such entities may be listed). There is also is no express prohibition on making property available to persons acting on behalf of designated persons or entities, where the making available of property is not for the benefit of the designated person or entity named in relevant sanctions lists.

Criterion 6.5(d) - UNSCR 1373 designations must published in the official Gazette "as soon as practicable". Gazettal usually takes two days but can be expedited. A communications plan is created for designations which, in addition to gazettal, can include a Prime Ministerial press statement, fact sheets, diplomatic engagement and publication of the designations on the New Zealand Police web site. The FIU also notifies those reporting entities registered for goAML electronically, of changes in designations, usually within one working day of the designation. However, approximately 2 700 reporting entities (mostly DNFBPs) are not registered for goAML and therefore do not receive such communications.

The FIU undertakes targeted distribution to entities such as the Racing Industry Transition Agency, the NZ Association of Credit Unions, casinos, the NZ Law Society and the Real Estate Institute of NZ. While the New Zealand Police provides guidance in its "Suspicious Activity Reporting Guideline" on suspicious activity reports in sanctions cases (as a possible predicate to money laundering or terrorism financing),

the guidance not include information on how to fulfil *targeted financial sanctions* obligations arising under the TSA. During the on-site visit, RBNZ shared the high-level findings of a survey of sanctions measures implemented all registered banks in New Zealand with these banks and included examples of good practice.

Criterion 6.5(e) - The TSA requires anybody who is in possession or immediate control of property to file a suspicious property report as soon as practicable, if they suspect on reasonable grounds that property may be owned or controlled, directly or indirectly, by a designated terrorist entity or derived or generated from such property. This applies to all persons, not just reporting entities. Further, reporting entities are required to submit a suspicious activity report (SAR) in circumstances where the reporting entity has reasonable grounds to suspect it may be relevant to the enforcement of the TSA, which would include the reporting of attempted transactions in contravention of the TSA.

Criterion 6.5(f) - Third parties may apply to the High Court for relief under the TSA. Relief includes declaring that the third party's interest is no longer subject to the prohibition on dealing under section 9, directing that the third party's interest not be included in any forfeiture order or, where forfeiture has occurred, direct the Crown to transfer the interest (or pay an equal amount) to the third party. Where property has been brought under the control of the Official Assignee, a third party may apply to the Prime Minister for relief. Persons who hold assets that act in purported compliance with the TSA (e.g. by freezing the assets and submitting a suspicious property report) are protected from civil, criminal or disciplinary proceedings.

Criterion 6.6(a) - The New Zealand Police web page concerning UNSC Resolution 1267/1989 and 1988 designations includes information on how to apply for delisting, either through the MFAT or directly to the Ombudsperson to the ISIL (Da'esh) and Al-Qaida Sanctions Committee. The page does not include information on applying to the UN Focal Point for Delisting (relevant to UNSC Resolution 1988 sanctions).

Criterion 6.6(b) - The New Zealand Police web page concerning UNSCR 1373 designations under the TSA include information on how to apply to the Prime Minister for revocation of a designation. The TSA requires that an application be on the basis that the designation should not stand because the entity no longer meets the designation criteria. While the Prime Minister *may* take any relevant information into account, the TSA establishes no grounds for the Prime Minister when deciding whether to revoke a designation. However, Standard Operating Procedures adopted in 2019 state that "the TDWG [in advising the Prime Minister on a revocation decision] consider it appropriate that the primary focus be on whether the grounds for revocation have been made out in any revocation application or recommendation".

Criterion 6.6(c) - It is expressly stated that nothing in the TSA prevents a person from bringing any judicial review proceedings in relation to designations under the Act. Judicial review of refusals to de-list persons or entities under UNSCR 1373 may, however, be ineffective due to the Prime Minister's broad legal discretion to maintain a designation even where the designation criteria are no longer met.

Criterion 6.6(d) - The New Zealand Police web page on UNSC Resolution 1267/1989 and 1988 designations includes information for New Zealand citizens, residents or organisations to submit delisting requests through the MFAT. There is no information about the UN Focal Point for De-listings in relation to UNSC Resolution 1988.

Criterion 6.6(e) - The New Zealand Police web page on UNSC Resolution 1267/1989 and 1988 designations includes information for New Zealand citizens, residents or organisations to submit delisting requests through the Ministry of Foreign Affairs and Trade. There is also information on how to apply directly to the Ombudsperson to the UNSC Resolution 1267/1989 Committee.

Criterion 6.6(f) - New Zealand has not published any procedures or guidance for persons whose assets have been frozen as a result of a false positive or other inadvertent freezing action.

Criterion 6.6(g) - The same communication channels used for new designations are used for de-listings, which reach the approximately 60 per cent of reporting entities registered for goAML. Unfreezing is automatic upon delisting. The "Advisory on Obligations to Suppress Terrorism under the TSA" does not include guidance on what to do when an entity is delisted.

Criterion 6.7 - The TSA includes broadly worded exception to prohibitions on dealing with the property of designated terrorist entities, or making property available to designated terrorist entities, which expressly extends to dealing "to satisfy the essential human needs of" a designated individual or their dependent. This does not comply with the requirement under UNSC Resolution 1452 and successor resolutions for such dealings only to be permitted where there is a prior licence or authorisation by authorities and, for UNSC Resolution 1267/1989 and 1988 designations, prior notification to the UNSC.

Section 11 of the TSA gives the Prime Minister a broad power to authorise dealings with frozen property. There are no criteria specified in the TSA for the Prime Minister to take into account when deciding whether to grant an authorisation. This means that there is no requirement that an authorisation relate to basic expenses or extraordinary expenses as defined in UNSC Resolution 1452, nor is there any requirement to notify the relevant UNSC Committee of proposed authorisations for basic expenses or to seek the Committee's approval of authorisations for extraordinary expenses. It is possible that New Zealand courts may read down section 11 in accordance with UNSC Resolution 1452 given it is intended to implement an international obligation, but this has not yet been tested.

A Prime Ministerial direction to the Official Assignee to take control of the property of designated terrorist entities may be subject to conditions, including to permit access to funds for basic expenses. However, this power does not include a requirement to comply with relevant UNSC Resolutions, including the notice and approval requirements.

Weighting and Conclusion

New Zealand has a strong and comprehensive legislative framework to give immediate effect to designations pursuant to UNSC Resolutions 1267/1989 and 1988, and by the Prime Minister pursuant to UNSCR 1373. However, this does not extend to all property owned or controlled by persons acting on behalf of, or at the direction of, UNSCR 1267/1989 and 1988 designated entities. There are also technical shortcomings when it comes to authorising dealings with frozen property or making assets available to designated terrorist entities, particularly "essential human needs" exception and the lack of any express requirement for authorised dealings with frozen funds under the TSA to comply with UNSC Resolution 1452 and successor resolutions. In New Zealand's context this is relatively minor: New Zealand has a relatively low counter-terrorism financing sanctions exposure, no resident designated individuals

at the time of the onsite visit,[41] and there has been no judicial consideration to date of the scope of the "essential human needs" which would need to be proved by a defendant. Therefore, a lower weighting has been given to this shortcoming for New Zealand, but it should be rectified to close any potential gap. Further the competent authority for UNSCR 1373 designations (the Prime Minister) is not required to take the designation criteria into account when considering delisting requests, which may make judicial review of such decisions ineffective – a minor shortcoming.

Recommendation 6 is rated Largely Compliant.

Recommendation 7 – Targeted financial sanctions related to proliferation

This is a new Recommendation.

Criterion 7.1 - New Zealand implements UNSC sanctions in relation to Iran and the Democratic People's Republic of Korea through regulations made under the *United Nations Act 1946*.

The *United Nations (Iran—Joint Comprehensive Plan of Action) Regulations 2016* (Iran Regulations) define "designated person" as an individual or entity designated by or under paragraph 6(c) of Annex B to UNSC Resolution 2231, meaning that any designations have immediate legal effect in New Zealand.

The *United Nations Sanctions (Democratic People's Republic of Korea) Regulations 2017* (DPRK Regulations) define "designated person" by reference to persons designated under OP8(d) of UNSC Resolution 1718 and a list of successor resolutions. This means that designations are immediately effective in New Zealand upon adoption by the UNSC.

Criterion 7.2(a) - The prohibition on dealing with assets of designated persons under clause 29 of the Iran Regulations and clause 44 of the DPRK Regulations apply to all persons. Section 29 of the *Interpretation Act 1999* defines "person" as including legal persons and unincorporated bodies. The asset freezing obligations under the DPRK Regulations include coverage of the requirements of OP 32 of UNSC Resolution 2270.

Criterion 7.2(b) - Property is broadly defined in both the Iran and DPRK Regulations to include everything that is "capable of being owned", including real or personal property, and tangible or intangible property. The definitions are broad enough to cover jointly owned property. The prohibitions on dealing with property of designated persons extends to property owned or controlled, directly or indirectly by a designated person. The Iran Regulations extend the prohibition on dealing to property of an "agent of a designated person" which is defined broadly, and in line with UNSC Resolution 2231 obligations. Under DPRK Regulations, any person determined by the Secretary of Foreign Affairs and trade to be acting on behalf of, or at the direction of, a designated person is also a designated person whose assets fall within the prohibition on dealing

Criterion 7.2(c) - Clause 30 of the Iran Regulations and clause 45 of the DPRK Regulations prohibit the sending, transfer or delivery, or causing the sending, transfer or delivery, of property to or for the benefit of a designated person without the Minister of Foreign Affairs' consent.

41 On 27 August 2020, the Prime Minister designated the individual responsible for the March 15 2019 attacks in Christchurch under the TSA: www.beehive.govt.nz/release/march-15-offender-designated-terrorist-entity. The individual is in custody serving a sentence of imprisonment for life without parole.

Criterion 7.2(d) - At the time of the onsite visit, New Zealand authorities did not have a mechanism in place to communicate changes in Iran and DPRK designations to reporting entities, beyond providing a link to the relevant UN web site listing individuals and entities While the New Zealand Police provides guidance in its "Suspicious Activity Reporting Guideline" on suspicious activity reports in sanctions cases (as a possible predicate to money laundering or terrorism financing), the guidance does not include information on how to comply with targeted financial sanctions obligations.

Criterion 7.2(e) - While reporting entities may be required to file SARs in relation to suspected sanctions offences, there is no obligation to report assets frozen under, or other action taken to comply with, targeted financial sanctions under the Iran and DPRK Regulations.

Criterion 7.2(f) - There is no legislation that protects the rights of bona fide third parties in the Iran Regulations or the DPRK Regulations.

Criterion 7.3 - There are no mechanisms for monitoring or ensuring compliance by financial institutions and DNFBPs with Iran or DPRK Regulations. Contraventions of the targeted financial sanctions obligations in the Iran and DPRK Regulations are punishable by a fine of NZD 10 000 or 12 months' imprisonment, for individuals, and a fine of NZD 100 000 for bodies corporate.

Criterion 7.4(a) - The MFAT DPRK and Iran sanctions web pages include links to the relevant UNSC Sanctions Committees' web pages. However, there is no information provided on how to apply for delisting, either through MFAT or to the UN Focal Point on Delisting.

Criterion 7.4(b) - Authorities indicated that they would provide *ad hoc* advice if approached by a person whose assets had been inadvertently frozen due to a "false positive" match. However, the possibility of seeking such advice has not been publicised.

Criterion 7.4(c) - Clause 31 of the Iran Regulations and clause 46 of the DPRK Regulations allow the Minister of Foreign Affairs to consent to an activity that would otherwise contravene targeted financial sanctions. The consent may only be granted if the Minister is satisfied that the requirements of relevant UNSC resolutions are met, including any requirement to notify the relevant UNSC Sanctions Committee and receive their decision.

Criterion 7.4(d) - At the time of the onsite visit, New Zealand authorities did not have a mechanism in place to communicate changes in Iran and DPRK designations to reporting entities, beyond providing a link to the relevant UN website. New Zealand has not produced any guidance on what to do in the case of delisting.

Criterion 7.5(a) - The Iran Regulations permit the addition to frozen accounts of interest or other earnings due on those accounts, or payments due under contracts that arose prior to the accounts becoming subject to freezing, in accordance with the relevant resolutions. Regulation 31(4) and 31(5) of the Iran Regulations mirror the wording of UNSC Resolution 2231 closely. While the DPRK Regulations do not expressly permit the addition to frozen accounts of interest or other earnings to frozen accounts, the wording of the Regulations is consistent with UNSC Resolution 1718 and successor.

Criterion 7.5(b) - The Minister of Foreign Affairs' power in clause 31 of the Iran Regulations to consent to activities otherwise prohibited by the targeted financial

provisions expressly requires consideration of the purposes set out in UNSC Resolution 2231 and compliance with any UNSC notice and decision requirements.

Weighting and Conclusion

The Iran and DPRK Regulations closely follow the wording UNSC Resolution 2231 and 1718 (and successor resolutions) and provides a strong legislative framework for the immediate implementation of TFS obligations under the resolutions. However, as at the time of the on-site visit, there was no mechanism for communicating new designations or changes in designations to reporting entities. The guidance available for Iran and DPRK sanctions is high level and is focused on the obligation to file SARs. It does not provide assistance regarding the implementation of targeted financial sanctions or unfreezing of assets in the case of delisting. There is a lack of guidance on how to apply for delisting, and the procedures to resolve false positives have not been publicised. There is also no specific obligation to report freezing actions taken under the Iran and DPRK Regulations. Taking into account New Zealand's risk and context, these are moderate shortcomings.

Recommendation 7 is rated Partly Compliant.

Recommendation 8 – Non-profit organisations

In its 3rd round MER, SRVIII was rated partially compliant, noting several shortcomings.

Criterion 8.1(a) - New Zealand has a large and diverse NPO sector comprising approximately 114 000 entities. Of these, New Zealand identifies a subset of both registered charities and other NPOs as likely falling within the FATF definition. New Zealand's 2019 NRA identified NPOs that "send funds to counterpart or 'correspondent' NPOs located in, or close to, countries where terrorists operate are vulnerable to exploitation". However, as part of the 2017 Regional Risk Assessment on NPOs and Terrorism Financing (which included a number of ASEAN jurisdictions together with New Zealand and Australia), New Zealand identified the overall TF risk associated with its NPO sector as low.

Criterion 8.1(b) - New Zealand assessed the ML/TF risks of its NPO sector in its 2019 NRA as one of 16 "vulnerable channels". The 2019 NRA identified charities as being at greatest risk of abuse for TF, particularly those that operate overseas (approximately 1 500 charities totalling NZD 3.8 billion in 2018) or that are non-resident charities (approximately 200-400). Authorities have assessed the major geographical risks for New Zealand charities, and have highlighted the limited knowledge of AML/CFT within the sector, particularly smaller and less sophisticated entities.

Criterion 8.1(c) - The *Charities Act 2005* is New Zealand's legislative framework for the regulation of registered charities. The legislation is administered by the charities regulator (DIA Charities Services), and includes some TF specific measures such as prohibiting designated terrorist entities or persons convicted of relevant offences under the TSA from serving as a charitable trustee.

Other NPOs have an incentive to apply to Inland Revenue for approval as a donee organisation.

New Zealand has reviewed the *Incorporated Societies Act 1908* and is in the process of reviewing the Charities Act 2005, which may have some impact on mitigating the terrorism financing risk of higher risk NPOs. These reviews however, do not focus on those NPOs identified as vulnerable to abuse for TF, nor has the proportionality or the effectiveness of regulatory actions available to addressing the TF risk been considered.

Criterion 8.1(d) - New Zealand has undertaken a number of assessments of its NPO sector's vulnerability to TF, including as a participant in the 2017 [Asia-Pacific] Regional Risk Assessment of NPOs and Terrorism Financing, and as part of its 2018 and 2019 NRAs.

Criterion 8.2(a) - The Charities Act, administered by DIA Charities Services, contains a range of measures to promote accountability, integrity and public confidence in the administration and management of registered charities (some 27 000 entities out of 114 000 NPOs). The policy of promoting public trust and confidence in the charitable sector (among other things) is expressly set out in the Charities Act.

Relevant measures under the Charities Act include requirements for registered charities to submit annual returns where their annual income NZD 1 000 or greater, with increasing requirements for larger charities. A public online charities register lists all current and previously registered charities, including summaries of each charity's purpose, activities, sectors, countries that the charity operates in, past and present officers, copies of annual returns and financial statements.

The Chief Executive of the DIA is empowered to inquire into charitable entities and persons who may have breached the Charities Act or committed a serious wrongdoing in connection with a charitable entity.

For other NPOs, donee organisations that send the majority of their funds overseas must apply to Inland Revenue and be added to the list of donee organisations in Schedule 32 of the *Income Tax Act 2007*. This involves a high level of initial and ongoing scrutiny by Inland Revenue. A small subset of non-charity NPOs (approximately 2 000), and tax-exempt non-resident charities (approximately 300), which have been identified in the 2019 NRA as possibly presenting some risk of abuse for TF, are primarily subject to policies to combat tax evasion rather than other goals.

Criterion 8.2(b) - DIA Charities Services has published information on its web site to assist charities in protecting against terrorism financing and money laundering outlining the nature of the risks (including common and less common typologies), providing information on ways to reduce the risk, and assisting charities to understand and comply with legal requirements in relation to TF. Direct engagement with the sector has included a workshop to explore risk factors (as part of the 2019 NRA, and a free webinar on terrorism financing in September 2019 for NPOs that carry out some of their purposes of overseas, as part of a broader series of webinars. The webinars were promoted through a newsletter sent to over 57 000 recipients and a targeted email sent to all registered charities that indicated they operated overseas.

Criterion 8.2(c) - As noted in 8.2(b), New Zealand authorities have conducted a free webinar on terrorism financing covering: what terrorism financing is; what New Zealand's international obligations are and why they matter; how not-for-profit organisations can be abused to raise and move funds for terrorist purposes, particularly overseas terrorism; and how to stop TF, what organisations should watch out for, and how doing this helps all not-for-profit organisations. There has been one such event to date and the process appears to be more focused on education than

development and refinement of best practices, but DIA Charities Services is planning further work.

Criterion 8.2(d) - The DIA Charities Services guidance on protecting against terrorism and money laundering includes a range of suggested ways to reduce TF vulnerability, including the use of the formal financial system to transfer funds within New Zealand or overseas.

Criterion 8.3 - DIA Charities Services supervises and monitors registered charities through the annual return and other reporting obligations set out above under criterion 8.2(a) and through Charities Services' power to inquire into charitable entities and other persons. The reporting obligations for charities are generally comprehensive but have not taken into account identified factors affecting vulnerability to TF when determining (for example) levels of reporting to the regulator; instead, obligations scale with the operating expenditure of the charity.

The power for the DIA to inquire into charities and other persons may be triggered by "serious wrongdoing in connection with a charity" which includes any suspected contravention of the TSA. Such inquiries may look into a range of matters, including the activities of the charity and the management and administration of the charity

Beyond registered charities, other categories of NPOs identified as being of moderate risk of abuse for TF including foreign charities, overseas donee organisations and charitable trusts, are not subject to risk-based monitoring or supervision.

Criterion 8.4(a) - Charities Services primarily monitors charities through annual returns, which must be provided within six months of the end of the charity's financial year. The registration process and annual returns include information about charities' countries of operation, which is relevant to TF risk

Charities Services also responds to information provided by other agencies, and complaints about serious wrongdoing within charities. Other NPOs assessed as at moderate risk of abuse for TF are not subject to risk-based supervision or monitoring.

Criterion 8.4(b) - Available sanctions for registered charities include: formal letters of expectation, warnings, monitoring, deregistration, disqualification of officers and entities, and prosecutions for offences where relevant. Overseas donee organisations may lose this status in response to wrongdoing. There do not appear to be relevant powers to impose sanctions in relation to other moderate-risk NPOs, i.e. non-charity NPOs (approximately 2 000), and tax-exempt non-resident charities.

Criterion 8.5(a) - DIA Charities Services is expressly permitted to share registration information about registered charities for the purposes of administering Inland Revenue (taxation) legislation. DIA Charities Services may also disclose information or documents to any person to assist in detecting or prosecuting offences against any law, but such information is not admissible as evidence. There are also exceptions in the Privacy Act permitting the sharing of information with the Police where criminal activity is suspected. The FIU may share SARs and reports with Charities Services.

Criterion 8.5(b) - DIA Charities Services has an eight-member team of investigators, including two accountants that work with other agencies (including the Police) as required. The team includes members with background in law enforcement and criminal intelligence. NPOs outside the registered charities cohort, which have been identified as presenting a moderate vulnerability of abuse for TF, would be subject to investigation by the Police.

Criterion 8.5(c) - DIA Charities Services maintains a broad range of financial and programmatic information on registered charities and has powers under the Charities Act, to require the production of further documents or information reasonably necessary to Charities Services carrying out its functions. Information held by DIA Charities Services and the Companies Office can be made readily available to the Police for any criminal investigation of TF.

Under other legislation governing legal persons and arrangements, such as Incorporated Societies Act 1908 and the Charitable Trusts Act 1957, regulators focus is more on investigating compliance with the requirements of these Acts rather than broader wrongdoing by the NPO.

Criterion 8.5(d) - Section 139 of the AML/CFT Act gives the Police, Customs and any AML/CFT supervisor a broad power (subject to privacy protections) to share information to any other agency or regulator for law enforcement purposes. This would include sharing TF related information with NPO regulators.

Criterion 8.6 - DIA Charities Services is actively engaged with international counterparts and is the contact point for sharing information about registered charities in New Zealand.

IR is able to exchange information on charitable trusts and approved donee organisations with other jurisdictions under relevant international exchange instruments that allow information received by tax administrations to be shared for non-tax purposes.

The Companies Office is the contact point for international sharing of information about other forms of incorporated NPOs, such as incorporated associations.

Weighting and Conclusion

New Zealand has identified that its NPO sector is at low risk of TF. Those NPOs identified as being at highest risk of abuse for TF, namely registered charities, are subject to a comprehensive regulatory and supervisory framework. Outreach on TF issues to the NPO sector has commenced and further work in developing and refining best practices is planned although not yet complete. Some NPOs other than registered charities have been identified as a moderate risk, and there is little in the way of risk-based monitoring or supervision. Given the overall low risk of New Zealand's NPO sector, this is a minor shortcoming. New Zealand has yet to review the adequacy of its laws and regulations for NPOs to address identified TF risks although a general review of the legislation focused on modernisation may have some impacts.

Recommendation 8 is rated Largely Compliant.

Recommendation 9 – Financial institution secrecy laws

In its 3rd MER, New Zealand was rated compliant with these requirements. The FATF requirements have not changed since then, although New Zealand has introduced new laws.

Criterion 9.1 - There are no FI secrecy laws that inhibit the implementation of AML/CFT measures in New Zealand. The *Privacy Act 1993* regulates the disclosure and sharing of personal information to protect the privacy of individuals. Section 7(4) provides that an action is not a breach of the Privacy Act if that action is authorized or required by the AML/CFT Act. The Privacy Act also permits the use and disclosure

of the information by both public and private sector agencies for law enforcement purposes (Privacy Principles 10 (1)(c)(i), 10(2) and 11(e)(i)).

a) *Access to information by competent authorities:* Competent authorities have statutory powers to request information from reporting entities (see R27, 29 and 31). Sections 132 and 143 of the AML/CFT Act set out the information gathering powers for the supervisors and the NZPFIU. Sections 70-78 of the Search and Surveillance Act and section 25 of the FMA Act set out additional powers.

b) *Sharing of information between competent authorities:* Competent authorities are not prevented from using information that was collected for one purpose for another purpose if sharing is necessary for law enforcement purposes (Privacy Principle 10(1)(c)(i)). This includes personal information (Privacy Principle 11(e)). These general provisions are supported by specific information-sharing powers in sections 46-48, 137-140 and 143 of the AML/CFT Act, section 59 of the FMA Act and section 36 of the SFO Act. For the SFO, there are restrictions on further disclosure or use of such information (sections 41 and 42 of the SFO Act). Such restrictions do not appear to cause potential impediment to the information sharing process with other government agencies. IR can also to share tax information on reporting entities (sections 18D-18J, section 23 of Schedule 7 of the TA Act).

c) *Sharing of information between FIs:* There are no FI secrecy laws that restrict the sharing of information between FIs where this is required by R13, 16 or 17. Sharing of information between reporting entities is not covered by the AML/CFT Act, although there is a power under the AML/CFT Act to make information-sharing regulations (sections 139(2) and 139A). No regulations have been made to date. The general information-sharing principles set out in Privacy Principles 10 and 11 also apply to private sector bodies.

Weighting and Conclusion

Recommendation 9 is rated Compliant.

Recommendation 10 – Customer due diligence

New Zealand was rated non-compliant with these requirements in the 3rd round MER. There were numerous deficiencies, particularly in relation to the lack of requirements to obtain information on the ultimate beneficiaries of transactions, to conduct ongoing and EDD and to ensure the CDD is done based on reliable documents from an independent source. The MER identified additional issues in relation to circumstances in which CDD had to be performed and the CDD threshold for wire transfers.

In 2009, New Zealand amended its AML/CFT legislation and addressed most of the deficiencies identified by the time of its second follow-up report in 2013. This recommendation was re-rated to largely compliant. Since then, the FATF requirements for CDD have substantially changed.

Criterion 10.1 - The use of anonymous accounts or accounts in fictitious names is prohibited (section 38(1) of the AML/CFT Act).

Criterion 10.2 - FIs are required by the AML/CFT Act to undertake CDD measures as follows:

a) Reporting entities must conduct CDD when establishing business relations (sections 14(1)(a), 18(1)(a) and 22(1)(a) of the AML/CFT Act);

b) Reporting entities must conduct CDD when carrying out occasional transactions above a threshold of NZD 10 000, whether or not the transaction is carried out in a single operation or several operations that appear to be linked (sections 14(1)(b), 18(1)(b) and 22(1)(b) of the AML/CFT Act; clause 10 of the AML/CFT (Definitions) Regulations 2011). This is below the applicable threshold in the FATF Recommendations of USD / EUR 15 000. Clauses 11-15 of the AML/CFT (Definitions) Regulations 2011 also define a number of other transactions to be occasional transactions. All of these have a threshold lower than USD/EUR 15 000;

c) Reporting entities must conduct CDD on wire transfers in the circumstances covered by R16 (section 22(3), 27 and 28 of AML/CFT Act and clause 13A of the AML/CFT (Definitions) Regulations));

d) There is no explicit requirement that CDD be conducted in all situations where there is suspicion of ML/TF. Reporting entities must conduct EDD in situations where a customer seeks to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose; or when a reporting entity considers that the level of risk involved is such that EDD should apply to a particular situation (sections 22(1)(c)(d)). Reporting entities must also conduct EDD as soon as practicable after becoming aware that a suspicious activity must be reported (section 22A(2)). However, when a transaction is conducted outside the business relationship for an amount below the threshold value, there is no requirement to do CDD.

e) There is no explicit requirement in the AML/CFT Act that CDD be conducted where there are doubts about the veracity or adequacy of previously obtained customer identification data. Instead, reporting entities are not required to obtain or verify information previously obtained and verified, unless there are reasonable doubts about the veracity or adequacy of the information (section 11(4)).

Criterion 10.3 - Reporting entities are required to identify their customers as part of the CDD process (sections 11, 15 and 23 of the AML/CFT Act) and verify that customer's identity using reliable, independent source documents, data or information (sections 13, 16 and 24 of the AML/CFT Act). The definition of customer is broad and can include any natural person, legal person or legal arrangement and includes permanent and occasional customers.

Criterion 10.4 - Reporting entities are required to conduct CDD on any person acting on behalf of a customer in establishing a business relationship and when carrying out an occasional transaction (sections 11(1)(c) and 19 of AML/CFT Act). Reporting entities must verify the identity information and the person's authority to act on behalf of the customer (sections 16(1)(c), 20 and 24(1)(a)).

Criterion 10.5 - Reporting entities are required to conduct CDD on any beneficial owner of a customer (section 11(1)(b) of AML/CFT Act) and take reasonable steps to verify the beneficial owner's identity (section 16(1)(b) or 24(1)(a)) using reliable, independent source documents, data or information (section 13).

The AML/CFT Act definition of beneficial owner does not include the term "ultimate" when describing ownership and control (section 5). However, the non-binding Beneficial Owner Guidelines issued by the supervisors, clearly address situations of ultimate ownership and control.

Criterion 10.6 - Reporting entities are required to obtain information as to the nature and purpose of the proposed business relationship (sections 17(a), 21 and 25 of the AML/CFT Act).

Criterion 10.7 - Reporting entities are required to conduct ongoing due diligence on the business relationship, including:

a) ensuring that the business relationship and the transactions relating to that business relationship are consistent with the reporting entity's knowledge of the customer, its business and risk, including source of funds for ongoing monitoring for customer relationships which require EDD (section 31(2) of the AML/CFT Act).

b) ensuring that reporting entities regularly review the customer's account activity, transaction behaviour and any customer information obtained under through the CDD process or it otherwise holds (section 31(4)). For situations where EDD is triggered, reporting entities are required to update CDD information. However, there is no explicit requirement to verify the new information and to keep updated records for customer relationships where EDD is not triggered.

Criterion 10.8 - For customers that are legal persons or legal arrangements, there is no explicit requirement for reporting entities to understand the nature of their customer's business and its ownership and control structure. Nonetheless, reporting entities are required to obtain information on the nature and purpose of the proposed business relationship between the customer and the reporting entity (section 17(a) of the AML/CFT Act) and the nature of the respondent's business specifically in correspondent banking relationships (section 29(2)(a)). Understanding the ownership and control structure is also covered in the non-binding Beneficial Ownership Guideline issued by the supervisors.

Criterion 10.9 - For customers that are legal persons and arrangements, reporting entities must identify the customer and verify its identity as follows:

a) Reporting entities must obtain and verify the customer's name and company identifier number (sections 15 and 16 of the AML/CFT Act). There is no explicit requirement to identify and verify their legal form and proof of existence; however, this is achieved as part of the verification of the company identifier number.

b) There is no explicit requirement for the reporting entities to identify the powers that regulate and bind the legal person or arrangement. Reporting entities are required to identify persons having a senior management position in the legal person or arrangement only when they meet the definition of a beneficial owner (see R10.10).

c) Reporting entities must obtain and verify the customer's address or registered office (section 15 of the AML/CFT Act).

Criterion 10.10 - As set out in R10.5, reporting entities are required to identify and take reasonable measures to verify the identity of beneficial owners of legal persons. Reporting entities must collect information about legal persons as follows:

a) the identity of the natural person who has a controlling ownership interest in a legal person, which is defined as an individual who owns more than 25% of the customer (section 5 of the AML/CFT Act; clause 5 of the AML/CFT (Definitions) Regulations).

b) the identity of the natural person(s) (if any) exercising control of the legal person through other means (section 5 of the AML/CFT Act). As noted in R10.8, the supervisors have released non-binding Guidelines setting out how reporting entities should identify the natural person exercising control.

c) There is no explicit requirement to identify individuals holding senior management positions when no natural person can be identified under (a) or (b). The non-binding Guidelines clarify that individuals holding senior management positions should be identified.

Criterion 10.11 - As set out in R10.5, reporting entities are required to identify and take reasonable measures to verify the identity of beneficial owners of legal arrangements. They must collect information about legal arrangements as follows:

a) For trusts, reporting entities are required to identify and take reasonable measures to verify the identity of beneficial owners of legal arrangements (sections 11(b) and 16 of the AML/CFT Act). The definition of beneficial owner in section 5 of the AML/CFT Act broadly refers to a person who has effective control, although it does not explicitly set out that reporting entities must identity the settlor, trustee or protector. The non-binding Guidelines from the supervisors clarify this point. The AML/CFT Act also requires reporting entities to collect the name and the date of birth of each beneficiary of the trust (section 23(2)(a)). Alternately, if the trust is a discretionary trust or a charitable trust or a trust that has more than 10 beneficiaries, they must obtain a description of each class or type of beneficiary and, if a charitable trust, the objects of the trust (section 23(2)(b). Trusts are also subject to EDD requirements which includes identifying and verifying the source of funds and wealth (section 23(1)(a) and 24(1)(b).

b) The requirements described in (a) extend to any other 'vehicle for holding personal assets' (section 22(1)(a)).

Criterion 10.12 - Other than the general CDD requirements on customers and beneficial owners, there are no explicit CDD requirements stipulated in relation to the beneficiaries of life insurance and other investment related insurance policies.

Criterion 10.13 - There is no explicit requirement for reporting entities to include the beneficiary of a life insurance policy as a risk factor in determining whether EDD measures are applicable.

Criterion 10.14 - Reporting entities are required to verify the identity of customers and beneficial owners prior to establishing a business relationship or conducting an occasional activity of transaction (sections 16(2), 20(2) and 24(2) of the AML/CFT Act). Verification of identity may be completed after the business relationship has been established if:

a) verification of identity is completed as soon as is practicable once the business relationship has been established; and

b) it is essential not to interrupt normal business practice;

c) ML/TF risks are effectively managed through procedures of transaction limitations and account monitoring (sections 16(3) and 24(3)).

There are no provisions for deferring identify verification for occasional transactions.

Criterion 10.15 - If verification occurs after the establishment of the business relationship, reporting entities are required to adopt appropriate risk management procedures (sections 16(3), 20(3) and 24(3) of the AML/CFT Act). If the reporting entity is an FI, this is mandated to be transaction limitations and account monitoring.

Criterion 10.16 - Reporting entities are required to apply CDD requirements to existing customers on the basis of materiality and risk if there is a material change in the nature of purpose of the business relationship or the reporting entity considers that it has insufficient information about the customer (section 14(1)(c) of the AML/CFT Act). It does not specify that the reporting entity must take into account whether and when CDD measures were last undertaken or the adequacy of data obtained. The ongoing CDD obligations do however require reporting entities to regularly review any customer information obtained under relevant CDD provisions (section 31(4)(b)).

Criterion 10.17 - Reporting entities are required to perform EDD where the ML/TF risks are higher and in a number of other specific circumstances (section 22(1) of the AML/CFT Act). This includes a business relationship with a customer who is a trust or a customer seeking to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose. A non-exhaustive range of risk factors is set out in section 58(2). The range of EDD measures set out in sections 23-25 however are insufficiently broad.

Criterion 10.18 - New Zealand permits reporting entities to undertake simplified CDD for a range of customer types set out in section 18(2) of the AML/CFT Act. The customer types are consistent with the types of low-risk businesses included in the FATF Standards (see R1.8 and R1.12).

Where simplified CDD is permissible, reporting entities are only required to obtain information on the nature and purpose of the business relationship (section 21) and identify and verify the identity and authority of the person acting on behalf of the customer (sections (19 and 20).

While it is not mandatory that reporting entities undertake simplified CDD for the customer types set out in section 18(2), there is no explicit requirement to refrain from applying simplified CDD measures where there is a suspicion of ML/TF or in situations posing higher ML/TF risk. However, reporting entities must undertake EDD as soon as practicable after becoming aware that a suspicious activity must be reported (section 22A(2)). However, when a transaction is conducted outside the business relationship for an amount below the threshold value, there is no requirement to do CDD (see R10.2(d)).

The Identity Verification Code of Practice 2013 sets out suggested best practice for the verification of natural persons that reporting entities have assessed to be low to medium risk.

Criterion 10.19 - Where a reporting entity is unable to conduct CDD, the reporting entity is required to refrain from establishing the customer relationship, terminate any existing business relationship with the customer, refrain from carrying out an occasional transaction or activity with or for the customer, and consider whether to make a SAR (section 37 of AML/CFT Act).

Criterion 10.20 - There is no requirement permitting a reporting entity to not pursue CDD where it may tip off the customer.

Weighting and Conclusion

There are a range of decencies with New Zealand's arrangements for CDD. This includes issues with the definition of beneficial owner and insufficient requirements relating to existing customers and EDD. New Zealand also lacks requirements to understand the nature of customers' business and identify the powers that regulate and bind legal persons and arrangements, permitting reporting entities to not purse CDD where it may tip off the customer and in relation to beneficiaries of life insurance policies and updating CDD information. Due to the limited risks in New Zealand, the issues relating to life insurance are given minimal weighting.

Recommendation 10 is rated Largely Compliant.

Recommendation 11 – Record-keeping

New Zealand was rated largely compliant with these requirements in the 3rd round MER due to the absence of an explicit requirement for institutions to retain business correspondence other than those required for the purpose of enabling reconstructions of transactions. Since then, New Zealand has introduced the AML/CFT Act.

Criterion 11.1 - Reporting entities must keep all necessary records on transactions, both domestic and international, for at least five years following completion of the transaction (section 49 of the AML/CFT Act).

Criterion 11.2 - Reporting entities must keep all necessary records collected through the CDD process, account files, business correspondence and the results of any analysis undertaken (sections 50(1) and 51(1) of the AML/CFT Act). They must retain CDD records for at least five years following the occasional transaction or termination of the business relationship (section 50(3 of the AML/CFT Act). However, there is no retention period specified for the account files, business correspondence and written findings.

Criterion 11.3 - Reporting entities must keep transaction records that are sufficient to permit reconstruction for at least 5 years after the completion of the transaction (section 49(1) of the AML/CFT Act).

Criterion 11.4 - As set out in R27, 29 and 31, there are sufficient requirements/powers in the AML/CFT Act to ensure availability of CDD and transaction records to the domestic competent authorities. For example, supervisors may, on notice, require the production of, or access to, all records, documents or information relevant to supervision and the monitoring of reporting entities for compliance (sections 132(1) and 132(2)(a) of the AML/CFT Act). The NZPFIU and the New Zealand Police can also order the production of records that is relevant to the analysis of information received under the AML/CFT Act (section 143). Records must

be kept in written form in English or in a form to make them readily available, which implies that these records must be made available swiftly (section 52).

Weighting and Conclusion

There is no retention period specified for reporting entities to keep account files, business correspondence and written findings.

Recommendation 11 is rated Largely Compliant.

Recommendation 12 – Politically exposed persons

New Zealand was rated non-compliant with these requirements in the 3rd MER due to the absence of any AML/CFT legislative measures regarding the establishment and maintenance of customer relationships with PEPs. Since then, New Zealand introduced the AML/CFT Act in 2009, which includes PEP requirements. New Zealand's 2nd Follow-Up Report found that these changes largely addressed the deficiencies. Since then, the FATF requirements for PEPs have changed.

Criterion 12.1 - A PEP is defined in section 5 of the AML/CFT Act to only include foreign PEPs. The definition of foreign PEP excludes important political party officials and restricts the time frame for holding a prominent public function to any time within the past 12 months rather than basing it on an assessment of risk. Regarding the CDD requirements, reporting entities are required to:

a) put in place adequate and effective procedures, policies, and controls to determine when EDD is required (section 57(1)(j). They must also take reasonable steps to determine whether a customer or beneficial owner is a PEP as soon as practicable after establishing a business relationship or conducting an occasional transaction or activity (section 26(1) of the AML/CFT Act).

b) obtain senior management approval to continue a business relationship with a PEP after its establishment (section 26(2)(a)). There are no requirements however to obtain such approval before establishing a new business relationship with a PEP.

c) take reasonable steps to verify the source of that wealth or those funds (sections 26(2) and (3)). Reporting entities are only required to obtain source of wealth *or* funds, rather than source of wealth *and* funds.

d) conduct enhanced ongoing monitoring on that relationship (section 31(2)).

Criterion 12.2 - New Zealand does not extend its PEP requirements to include domestic PEPs or PEPs from international organisations.

Criterion 12.3 - Regarding foreign PEPs, the definition of PEP extends to include immediate family members and individuals with a close relationship with the PEP (section 5 of the AML/CFT Act). This does not extend to domestic PEPs or PEPs from international organisations.

Criterion 12.4 - There are no explicit requirements in the AML/CFT Act for determining whether beneficiaries, or beneficial owners of beneficiaries, of life insurance policies are PEPs. However, as outlined in R12.1, there are requirements to take reasonable steps as soon as practicable after establishing a business relationship or conducting an occasional transaction or activity to determine whether the customer or any beneficial owner is a PEP and to conduct EDD in such situations.

Weighting and Conclusion

The definition of PEP has several issues, including its lack of coverage of domestic and international organization PEPs. There is no explicit requirement to obtain senior management approval before establishing a new business relationship with a PEP or obtain source of wealth and funds regarding a PEP. Due to the limited risks, the issues relating to life insurance are given minimal weighting.

Recommendation 12 is rated Partially Compliant.

Recommendation 13 – Correspondent banking

New Zealand was rated non-compliant with these requirements in its 3rd MER due to the absence of any AML/CFT legislative measures concerning the establishment of cross-border correspondent banking relationships. Since then, New Zealand introduced the AML/CFT Act in 2009, which includes correspondent banking and shell bank requirements. New Zealand's 2nd Follow-Up Report found that these changes had largely addressed the deficiencies.

Criterion 13.1 - In relation to cross-border correspondent banking and other similar relationships, FIs must conduct EDD (section 29(1) of the AML/CFT Act) and do the following:

a) gather sufficient information about the respondent to understand fully the nature of the respondent's business and determine from publicly available information the reputation of the respondent and whether, and to what extent, the respondent is supervised for AML/CFT purposes, including whether the respondent has been subject to a ML/TF investigation or regulatory action (section 29(2)(a)-(b));

b) assess the respondent's AML/CFT controls (section 29(2)(c));

c) obtain approval from the senior management before establishing a new correspondent banking relationship (section 29(2)(d)); and

d) document the respective AML/CFT responsibilities of the correspondent and the respondent (section 29(2)(e)).

There are no explicit requirements that apply correspondent banking rules to non-bank institutions (e.g. securities firms) that undertake activities similar to correspondent banking activities.

Criterion 13.2 - For "payable-through accounts", the correspondent FI must satisfy themselves that the respondent has:

a) verified the identity of, and conducts ongoing monitoring in respect of, customers that have direct access to the accounts of the correspondent bank, and

b) is able to provide to the correspondent, on request, the relevant CDD documents, data, or information CDD (section 29(2)(f)).

Criterion 13.3 - Reporting entities must not establish or continue a business relationship with, or allow an occasional transaction or activity to be conducted through it by, a shell bank or a FI that has a correspondent banking relationship with a shell bank (section 39(1) of the AML/CFT Act).

Weighting and Conclusion

It is not clear whether New Zealand's correspondent banking rules apply to non-bank relationships with similar characteristics.

Recommendation 13 is rated Largely Compliant.

Recommendation 14 – Money or value transfer services

New Zealand was rated non-compliant with these requirements in its 3rd MER. In particular, New Zealand did not have a designated supervisor of MVTS providers nor did it monitor MTVS providers for compliance. Since then, the FSP Act commenced operation and New Zealand introduced the AML/CFT Act in 2009 and the FMA Act in 2011. These Acts create an MVTS registration scheme. This Recommendation was re-rated to largely compliant in New Zealand's second follow-up report. The FATF requirements for MVTS have also changed.

Criterion 14.1 - Natural or legal persons that provide MVTS are required to be registered on the FSPR (section(5)(1)(f) and 13 of the FSP Act). A person may be ineligible for registering if they meet a disqualifying criterion, such as being bankrupt or convicted of certain offences, including ML/TF offences (section 14).

Criterion 14.2 - Proportionate and dissuasive sanctions apply to persons who provide MTVS without being registered. Every individual who provides MVTS without being registered can be convicted and sentenced to 12 months jail or a fine of up to NZD 100 000, or both. Legal persons are liable for a fine of up to NZD 300 000 (sections 11(2) and 12(2) FSP Act).

The administration of the FSPR and enforcement of the requirement to register is split between several different agencies. The FSP Act is administered by MBIE. MBIE maintains and administers the FSPR and ensures that entities registered on the FSPR comply with registration requirements.

The FMA is then mandated to monitor compliance with the FSP Act requirements (section 9(1)(c) of the FMA Act). In practice, the FMA focuses on identifying businesses which are misusing their FSPR registration to mislead the public. The FMA can issue warnings (e.g. that a MVTS is unregistered) and mandate that the person displays this warning (section 49 of the FMA Act).

The DIA is then the main supervisor for MVTS providers' broader AML/CFT obligations. While the DIA does not enforce FSPR registration requirements, it can refer cases of unregistered MVTS providers it identifies to the FMA for enforcement.

There is little evidence that FMA, DIA and MBIE are taking action to identify natural or legal persons that carry out MVTS without registration, and there is no evidence of a co-ordinated process between FMA, MBIE and DIA to identify such entities.

Criterion 14.3 - MVTS providers are captured as reporting entities under section 5 of the AM/CFT Act. DIA is the main supervisor of MVTS providers (section 130(1)(d) of the AML/CFT Act). There are seven MVTS providers that are licensed by the FMA to provide other financial services and therefore are subject to AML/CFT supervision by the FMA in line with section 130(2)(a) of the AML/CFT Act.

Criterion 14.4 - There is no specific requirement for MVTS agents to be registered or licensed. If such agents carry out financial services as their business, they would be captured under the registration requirements of the FSP Act. However, agents that do

not conduct financial services in their ordinary course of business are not covered under the requirements of the FSP Act.

Nor are MVTS providers required to maintain a current list of their agents that is accessible by competent authorities. Using its powers under section 132 of the AML/CFT Act, DIA can request MVTS providers to provide information on their agents and sub-agents. This does not, however, require that the MVTS provider *maintains* such a list.

***Criterion* 14.5** - MVTS providers are not required in the AML/CFT Act to include agents in their AML/CFT programmes. They are required to set out the procedures for their agents to conduct CDD on its behalf (sections 34 and 57(1)(k) of the AML/CFT Act), but this does not apply the full scope of the MVTS provider's AML/CFT programme to the agent. MVTS providers are also not required to monitor their agents' compliance with their programme, although they do have a general obligation to monitor and manage compliance with their own programme (section 57(1)(l)).

Weighting and Conclusion

MVTS providers are captured as financial service providers and therefore are subject to registration requirements, but there are several deficiencies. Minimal action is taken to identify unregistered MVTS providers. There are insufficient requirements for MVTS agents to be licensed or registered. There are no requirements for maintaining an updated list of agents accessible by competent authorities. These are important deficiencies in light of the ML/TF risk posed by the MVTS sector to New Zealand.

Recommendation 14 is rated Partially Compliant.

Recommendation 15 – New technologies

New Zealand was rated non-compliant with these requirements in its 3rd MER because it did not implement adequate AML/CFT measures relating to the ML/TF threats regarding new or developing technologies, including non-face-to-face business relationships or transactions. Since then, New Zealand introduced the AML/CFT Act in 2009. In New Zealand's 2nd Follow-Up Report, this Recommendation was re-rated to largely compliant. The FATF requirements on new technologies have also changed.

Criterion 15.1 - New Zealand assessed new payment technologies as a high priority vulnerability in the 2018 and 2019 NRA. The 2019 NRA included a detailed vulnerability assessment of the availability and impact of abuse of new payment technologies. The assessment covered stored value instruments, internet-based payment services, mobile payments, alternative banking platforms and virtual assets. In addition, the SRAs issued by DIA, FMA and RBNZ in 2017, 2018 and 2019 all assessed the ML/TF risks posed by new technologies in their specific sectors.

Reporting entities have an over-arching obligation to conduct ML/TF risk assessments with regard to their business, products and delivery methods (section 58(2) of the AML/CFT Act) and have an AML/CFT programme which prevents the use of products for ML/TF (for example, through the misuse of technology) (section 57(i)). This is not however a sufficiently explicit requirement for reporting entities to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Criterion 15.2

(a) Reporting entities must undertake an assessment of the ML/TF risks they may reasonably expect to face in the course of their business before conducting CDD or establishing an AML/CFT programme (section 58 of the AML/CFT Act). This is not however a sufficiently explicit requirement for reporting entities to undertake risk assessments of new products, business practices or technologies prior to the launch or use of such products, practices and technologies.

(b) When dealing with new or developing technologies or products that might favour anonymity however, reporting entities must undertake EDD (section 22(5) of the AML/CFT Act) and take additional measures to mitigate and manage the ML/TF risk (section 30). This is not however a sufficiently explicit obligation for reporting entities to take appropriate measures to manage and mitigate the risks relating to new products, practices and technologies.

Criterion 15.3

(a) Virtual assets were included in both the 2018 and 2019 NRAs, within the ML/TF vulnerability analysis of modern payment technologies. The NRA identified ML/TF vulnerabilities associated with virtual assets and noted that formal virtual currency exchanges have a small presence in New Zealand. The NRA concluded that virtual assets are one of the most vulnerable new payment technologies that present a dynamic ML/TF risk. The usage was thought to have a relatively low value but the misuse of virtual assets have been observed in a number of Police investigations.

DIA's Phase 1 SRA issued in 2018 included virtual currencies under the ML/TF risk assessment of payment service providers sectors which was rated medium-high. DIA's Financial Institutions SRA issued in December 2019 specifically assessed VASPs as their own sector which was assigned an overall high risk rating. This reflected the vulnerabilities of the sector which include ease of access, anonymity and beneficial ownership issues, exposure to cross-border payments and prior association with organised crime. This SRA assessed in greater detail the specific risks of different types of VASPs and the services they offer.

(b) New Zealand is developing its risk-based approach to respond to the risks posed by virtual assets and VASPs. New Zealand has not specifically covered VASPs under the AML/CFT Act, as they are largely covered under the definition of FI (see below). DIA and FMA are the AML/CFT supervisors for VASPs (see R15.6) and established a working group in 2017 to develop the supervisory approach to VASPs. As the lead supervisor, the DIA has reviewed the known reporting entity VASPs in 2019 to identify VASPs of high ML/TF risk to prioritise for supervisory engagement. In March 2020, DIA released VASP-specific AML/CFT guidance.

(c) The AML/CFT Act includes the five types of VASP as businesses that are offering services for transferring money or value, investing, administering or managing funds or participating in securities issues and the provision of financial services related to those issues. The Act however does not however extend to virtual asset wallet providers which only provide safekeeping and/or administration of virtual assets but do not also facilitate exchanges or transfers. The covered VASPs have the same AML/CFT obligations as other reporting entities, including the requirements to take appropriate steps to identify, assess, manage and mitigate their ML/TF risks. The minor deficiency noted in R1.11 applies here.

Criterion 15.4

(a) VASPs are required to register on the FSPR if they provide services that are captured by the financial service definition under the FSPR Act (see R26). The FSP Act

applies to VASPs when they are ordinarily resident or have a place of business in New Zealand, regardless of where the financial service is provided (section 8A of the FSP Act) and applies to natural and legal persons (section 3). VASPs providing services in relation to virtual assets that qualify as 'financial products' are subject to additional licensing obligations under the FMC Act. VASPs registered outside of New Zealand may also be considered to be reporting entities under the AML/CFT Act if the entity is actively and directly advertising or soliciting business from persons in New Zealand.

(b) VASPs that are captured as FIs are subject to the same vetting and qualification requirements as other FIs under the FMC Act and FSP Act (see R26.3). The analysis under R26.3, and the relevant deficiencies noted, are applicable here.

Criterion 15.5 - New Zealand takes action to identify VASPs that require registration or licensing, although it is not clear yet whether this is sufficient to ensure all unregistered VASPs can be captured. DIA and FMA have directly communicated with entities outlining their capture as financial services providers and reporting entities. They have also identified VASPs through open source searches, information provided by other agencies, other forms of intelligence and SARs. DIA has released information on how VASPs are covered in New Zealand.

Proportionate and dissuasive sanctions apply to persons who carry out VASP activities without being registered. Every individual who is liable on conviction to a term of imprisonment for up to 12 months or a fine of up to NZD 100 000, or both. In the case of a person who is not an individual, that person is liable for a fine of up to NZD 300 000 (sections 11(2) and 12(2) of the FSP Act). The FMA, which enforces the FSPR to some extent (see R14.2), has additional powers under the FMA Act. The FMA can issue warnings and mandate that the person displays this warning (section 49 of the FMA Act).

Criterion 15.6

(a) DIA is the lead supervisor for VASPs. The FMA is responsible for the part of the sector where VASPs carry out activities within its remit (such as initial coin offerings). VASPs are subject to regulation and risk-based supervision in the same manner as the DIA and FMA supervise the rest of their reporting populations (see R26). As VASPs are newly supervised in New Zealand, the supervisors are developing their risk-based approach for supervision for VASPs. For DIA, they are categorized among the entities prioritized for supervisory engagement, due to the high ML/TF risk, with an initial focus of guidance and outreach.

(b) FMA and DIA have sufficient powers to supervise and monitor the compliance of VASPs, including the authority to conduct inspections, compel the production of information and impose a range of disciplinary and financial sanctions. The deficiencies regarding the range of sanctions noted in R27.4 is relevant here. While there are powers to withdraw, restrict or suspend the VASP's license or registration, as discussed in the analysis under R27 it is unclear whether DIA or FMA would have this power for breaches of the AML/CFT Act.

Criterion 15.7 - DIA has issued guidelines for VASPs to assist the sector in understanding the applicable compliance obligations under AML/CFT Act. The guidelines refer VASPs to DIA's 2019 SRA and covers key AML/CFT compliance aspects, such as captured VASP activities, territorial scope, relevant supervisor and AML/CFT obligations. Other general guidance issued for FIs are also relevant to them (see R34). DIA has engaged with VASPs through phone calls, emails and face-to-face

meetings. The FMA has also released guidance to VASPs under its purview, which provides information particularly focused on initial coin offerings.

Criterion 15.8

(a) VASPs are subject to a range of proportionate and dissuasive criminal, civil and administrative sanctions in the same manner applicable to FIs for breaches of their AML/CFT obligations (see R35.1).

(b) Civil and criminal sanctions set out in the AML/CFT Act can only apply to reporting entities, but not their directors and senior management (see R35.2).

Criterion 15.9

Most VASPs are reporting entities under the AML/CFT Act. Therefore, the analysis on R10-R21 applies here, with the following qualifications:

(a) As set out in R10.1(b), the occasional transaction threshold for CDD by reporting entities is NZD 10 000 (section 10 of the AML/CFT (Definitions) Regulation 2011). This is above the USD/EUR 1 000 threshold value required for VASPs. Some transactions have a lower threshold value consistent with the FATF Standards. For example, CDD thresholds for occasional wire transfer transactions is NZD 1 000 (section 13A of the AML/CFT (Definitions) Regulation 2011). There is no threshold value explicitly defined for virtual asset transactions.

(b)(i)-(ii) As reporting entities under the AML/CFT Act, VASPs are required to comply with sections 27 and 28 of the Act when acting as ordering, intermediary or beneficiary institutions in a wire transfer transaction. The analysis in R16.1 to R16.4 applies here. As the definition of wire transfer in sectifon 5 of the AML/CFT Act only includes transfers of 'money', the wire transfer requirements for VASPs do not apply for transactions between virtual assets. There also are no provisions to mandate that all virtual asset transfers be treated as cross-border wire transfers and that information is made available to the beneficiary VASP or FI immediately and securely.

(b)(iii) With respect to monitoring the availability of information, the conclusions made under R16.8, 16.11 and 16.13 are applicable here. With respect to taking freezing actions and prohibiting dealing with designated persons and entities, the analysis under R16.18 is applicable here as well.

(b)(iv) The same analysis included in R15.9(b)(i)-(iii) also applies to virtual asset transfers by FIs.

Criterion 15.10

New Zealand communicates updates to relevant sanctions lists to VASPs in the same way as to other reporting entities. The shortcomings with respect to the provision of guidance to reporting entities, monitoring reporting entities for compliance with UNSC Iran and DPRK sanctions, and requiring reporting of assets frozen under UNSC Iran and DPRK sanctions similarly apply to VASPs.

Criterion 15.11

FMA and DIA are able to exchange information internationally, including information held by their supervised VASPs, and co-operate with counterparts (sections 131(e) and 132(2) of the AML/CFT Act). LEAs are also able to share information relating to virtual assets. The analysis and conclusions made under R40 are applicable here.

Weighting and Conclusion

There are no explicit requirements for reporting entities to undertake risk assessments of new products, business practices or technologies and to do so prior to the launch or use of such products, practices and technologies. Nor is there an explicit requirement for reporting entities to take appropriate measures to manage and mitigate the risks relating to new products, practices and technologies. New Zealand covers most VASPs as reporting entities, apart from some wallet providers, but has not introduced the VASP-specific requirements for CDD and wire transfers. The deficiencies in R6, 10-21, 26-27 and 37-40 also apply to VASPs. The deficiencies in relation to VASPs are given less weight as the sector is not materially important for New Zealand.

Recommendation 15 is rated largely compliant.

Recommendation 16 – Wire transfers

In its 3rd MER, New Zealand was rated non-compliant with these requirements, as it did not have sufficient requirements in relation to the information accompanying wire transfers. Since then, New Zealand introduced the AML/CFT Act in 2009. This recommendation was re-rated to largely compliant in New Zealand's 2nd Follow-Up Report. The FATF requirements on wire transfers have also changed.

Criterion 16.1 - The following rules apply to all wire transfers of more than NZD 1 000 (section 5A of the AML/CFT (Definitions) Regulations 2011). This is below the FATF requirement of USD/EUR 1 000. All cross-border wire transfer of more than NZD 1 000 must be accompanied by:

a) the required and accurate originator information (name; account number; and address, official personal document number, customer ID number or date and place of birth) (sections 27(1), 27(4) and 28 of the AML/CFT Act),

b) the required beneficiary information (name and account number) (section 27A). The information obtained by the reporting entity must accompany the wire transfer (section 27(4)).

The AML/CFT Act excludes credit and debit card transactions from the definition of wire transfer if the credit or debit card number accompanies the transaction, even though credit or debit cards may, in theory, be used as a payment system to effect a person-to-person wire transfer (section 5).

Criterion 16.2 - There is no explicit requirement in the Act relating to batch transfers. Therefore, the requirements in sections 27 and 28 of the AML/CFT Act also apply in cases where numerous individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries.

Criterion 16.3 - For wire transfers with a value of less than NZD 1 000, New Zealand does not mandate that they are accompanied by the required originator and beneficiary information.

Criterion 16.4 - As there is not a requirement to collect the required originator and beneficiary information in the circumstances outlined in R16.3, there is not a requirement to verify this information where there is a suspicion of ML/TF. However, some of the required originator information (e.g. the name of the originator where they are the customer) would be collected and verified under CDD requirements (see R10.2, 10.3 and 10.16).

Criterion 16.5 and 16.6 - For domestic wire transfers, the same requirements as set out in R16.1 apply. Alternatively, FIs may also identify the originator by obtaining just the originator's account number if they are able to provide the rest of the required originator information within 3 working days of the beneficiary institution making a request (section 27(2) of the AML/CFT Act). This is consistent with the FATF Standard.

Although the Act does not also require that the information be made within 3 working days of a request by a competent authority, the fact that the FI is obliged to do this for beneficiary institutions means that the information must be available if requested by a competent authority. Competent authorities and law enforcement are able to access this information by virtue of the powers granted under the AML/CFT Act and other Acts (see R27 and R31). However, these requirements do not apply to domestic wire transfers of less than NZD 1 000.

Criterion 16.7 - The ordering and beneficiary reporting entities are required to retain most information on originator and the beneficiary for five years (sections 49 and 50 of the AML/CFT Act). These requirements however do not ensure that full beneficiary information is maintained by the ordering institution. In particular, there is no requirement to keep the beneficiary's account number or a unique transaction reference number.

Criterion 16.8 - Reporting entities are prohibited from carrying out occasional transactions or continuing business relationships if CDD, including on wire transfers cannot be carried out (section 37 of the AML/CFT Act). For wire transfers equal to or above NZD 1 000, verification of the originator's identity must also be carried out before the wire transfer is ordered (section 28). This effectively prohibits wire transfers where R16.1 to 16.7 cannot be met for originators for occasional transactions and within business relationships. However, there is no explicit requirement to stop executing a wire transfer if it lacks the required beneficiary information. There are also no requirements to prevent a wire transfer below the threshold limit if it does not include the required originator or beneficiary information.

Criterion 16.9 - For cross-border wire transfers, any information about the originator obtained by an intermediary institution must be provided by that intermediary institution to the beneficiary institution as soon as practicable (section 27(6) of the AML/CFT Act). This obligation does not however include the collected beneficiary information, nor does it mandate that the originator information be retained with a wire transfer, just that the information be provided as soon as practicable.

Criterion 16.10 - There are no explicit requirements for intermediary institutions to retain records for at least five years where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer. However, reporting entities have a general obligation to maintain transaction records for 5 years (section 49 of the AML/CFT Act). The limitations identified in the analysis of R16.7 also apply to intermediary FIs.

Criterion 16.11 - There are no explicit requirements on intermediary institutions to take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack required originator information or required beneficiary information.

Criterion 16.12 - There are no explicit requirements on intermediary institutions to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

Criterion 16.13 - There are no explicit requirements that beneficiary institutions take reasonable measures, which may include post-event or real time monitoring, to identify international wire transfers that lack required originator or beneficiary information.

Criterion 16.14 - There are no explicit requirements that beneficiary institutions verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information, for wire transfers of USD/EUR 1 000 or more.

However, if the beneficiary to a wire transfer transaction is a customer with an established relationship with the reporting entity, the reporting entity would have previously conducted customer identification and verification in accordance with the CDD requirements of the AML/CFT Act (see R10).

Any transaction that occurs outside of a business relationship and involves the receipt of a wire transfer by a beneficiary institution for an amount of more than NZD 1 000, is defined to be an occasional transaction (clause 13A of the AML/CFT (Definitions) Regulations). Reporting entities are therefore required to conduct CDD procedures as outlined in R10.

The information obtained through the CDD process must be retained in line with sections 49 and 50 of the Act (see R11).

Criterion 16.15 - Beneficiary institutions must use effective risk-based procedures for handling wire transfers that are not accompanied by all the required information and consider whether the wire transfers constitute a suspicious activity (section 27(5) of the AML/CFT Act). The non-binding Wire Transfer Guideline from the supervisors clarifies that the procedures should assist beneficiary institutions to determine when to accept, reject or suspend a wire transfer and what further action to be taken.

Criterion 16.16 - The requirements of sections 27 and 28 of the AML/CFT Act in relation to wire transfers are applicable to all reporting entities when they act as ordering, intermediary or beneficiary institutions. This includes MVTS providers.

Criterion 16.17 - There are no specific legal requirements for MVTS providers either to review ordering and beneficiary information to decide whether to file a SAR or to ensure that a SAR is filed in any country affected and make transaction information available to the FIU.

Criterion 16.18 - All natural and legal persons in New Zealand, including reporting entities, are required to take freezing action and comply with prohibitions from conducting transactions with designated persons and entities when conducting wire transfers (see R6).

Weighting and Conclusion

While New Zealand has a legislative framework for wire transfers, there are a range of deficiencies. There are no requirements relating to wire transfers less than NZD 1 000, full beneficiary information does not need to be maintained and there is no prohibition on executing wire transfers where the wire transfer rules cannot be complied with. There are also no explicit requirements relating for intermediary and

beneficiary institutions to carry out a range of actions to ensure the wire transfer rules are complied with.

Recommendation 16 is rated partially compliant.

Recommendation 17 – Reliance on third parties

New Zealand was rated non-compliant with these requirements in its 3rd MER, as there were insufficient obligations imposed on the reporting entity seeking to rely on a third party. Since then, New Zealand introduced the AML/CFT Act in 2009. New Zealand's 2nd Follow-Up Report found that these changes appeared to have partly address the deficiencies. The FATF requirements on reliance have also changed.

Criterion 17.1 - New Zealand permits reporting entities to rely on third parties to conduct the CDD in two circumstances under the AML/CFT Act (i) reliance on a member of a designated business group (DBG) (section 32 and (ii) reliance on another reporting entity (section 33).

A DBG allows groups of entities that meet certain criteria to share some compliance responsibilities and rely on one another for CDD purposes (section 32). Each member of the group must be related to each other and agree to be a member of the DBG (section 5). The reporting entity that relies on another retains ultimate responsibility for the CDD measures (sections 32(2) and 33(3)).

Section 33 permits reliance on another reporting entity or a person who is resident in a country with sufficient AML/CFT systems and measures in place and who is supervised or regulated for AML/CFT purposes. The reporting entity that relies on another retains ultimate responsibility for the CDD measures (sections 33(2)).

Regarding the specific FATF requirements for both types of reliance:

a) Reporting entities are required to obtain immediately the necessary identification information (sections 32(1)(a)(i) and 33(2)(c)(i)). Verification information must be provided as soon as practicable after a request by a reporting entity (with a maximum limit of five days after a request) (sections 32(a)(ii) and 33(2)(c)(ii)).

b) For section 33 reliance, the reporting entity must ensure that that the third party is a reporting entity (if based in New Zealand) or supervised or regulated for AML/CFT purposes (if based overseas) (section 33(2(a)). The third party is also required to conduct CDD to the standards in the AML/CFT Act (whether they are based in New Zealand or not) (section 33(2)(c)). But this does not require reporting entities to satisfy themselves that the third party has measures in place for compliance with record-keeping requirements specifically. Similar requirements apply for DBG reliance under section 32 (due to the definition of DBG in section 5 of the AML/CFT Act), although overseas-based DBG members are not specifically required to conduct CDD to the standards in the AML/CFT Act. In addition, non-reporting entities may be part of a DBG if they are part of a joint venture.

Criterion 17.2 - While there are no explicit requirements in the AML/CFT Act that reporting entities should have regard to information available on the level of country risk when determining in which countries a third party that meets the conditions can be based, they must be based in a country which has 'sufficient' AML/CFT systems and measures in place (sections 5 and 33(2)(a)(ii)).

Reporting entities also have a general obligation to have regard to risk factors, including the countries the deals with, as part of their over-arching risk assessment (section 58).

Criterion 17.3 - New Zealand does not have a policy of permitting reporting entities that are part of the same financial group to rely on each other (other than the DBG requirements set out in R17.1). Accordingly this criteria is not applicable to New Zealand.

Weighting and Conclusion

Reporting entities are permitted to rely on third parties to conduct the CDD procedures required under the AML/CFT Act. Reporting entities may rely on a non-reporting entity in certain DBGs. For overseas-based third parties, there are insufficient requirements for reporting entities to have regard to the level of country risk.

Recommendation 17 is rated largely compliant.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

New Zealand was rated non-compliant with these requirements in its 3rd MER, as FIs were not required to have internal controls or ensure that foreign branches and subsidiaries observe appropriate AML/CFT standards. Since then, New Zealand introduced the AML/CFT Act in 2009. New Zealand's 2nd Follow-Up Report found that these changes appeared to have addressed some of the deficiencies. The FATF requirements have also changed.

Criterion 18.1 - Reporting entities are required to establish and implement a written AML/CFT programme, which includes internal procedures, policies and controls to detect and manage its ML/TF risk (sections 56(1) and 57 of the AML/CFT Act). The reporting entity must conduct the risk assessment prior to establishing its AML/CFT programme and include consideration of the nature, size and complexity of the business (section 58). The programme must include requirements for:

a) the appointment of a compliance officer (section 56(3)). However, the officer does not have to be at the management level, as section 56(4) only mandates that the compliance officer report to a senior manager;

b) vetting procedures for senior managers, the compliance officer and other AML/CFT staff (section 57(1)(a)). The AML/CFT Program Guideline, which reporting entities must have regard to under section 57(2), clarifies that vetting of employees should be of a high standard;

c) an employee training programme (section 57(1)(b)). Although there is explicit no requirement for training to be ongoing, the AML/CFT Program Guideline clarifies that the AML/CFT Program should document the scope and nature of training, frequency, delivery methods, and completion dates and rates.

d) an independent audit function to test the system at least every two years (sections 59 and 59B).

Criterion 18.2 - There is no specific requirement for financial groups to implement group-wide programs against ML/TF applicable and appropriate to all branches and subsidiaries.

In addition to the analysis of R18.1 above (which applies here), the following applies specifically to branches and subsidiaries. There are no specific requirements for:

a) reporting entities to implement group wide policies and procedures for sharing information for the purpose CDD and ML/TF risk management;

b) the provision, at a group level, compliance, audit and/or AML/CFT function, of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purpose and from the group level functions to the branches and subsidiaries; and

c) the adequate safeguards on confidentiality and the use of information exchanged, including safeguards to prevent tipping-off.

The AML/CFT Act permits sharing of certain information and the adoption of shared AML/CFT programmes among members of the same DBG (see R17). The formation of DBGs however are not mandatory for financial groups. Subsidiaries are not able to share information with their parent if they do not form a DBG together.

Criterion 18.3 - Reporting entities are required to ensure that their foreign branches and majority-owned subsidiaries apply AML/CFT measures equivalent with the AML/CFT Act, where the minimum AML/CFT requirements of the host country are less strict than those of the New Zealand, to the extent that host country laws and regulations permit (section 61(1) of the AML/CFT Act). If the host country does not permit the proper implementation of AML/CFT measures equivalent with New Zealand, reporting entities are required to apply appropriate additional measures to manage the ML/TF risks, and inform their home supervisors (section 61(2)).

Weighting and Conclusion

There are requirements for FIs to implement risk-based AML/CFT programs. However, there are no requirements for the compliance officer to be appointed at a management level. There is no requirement for financial groups to implement group-wide programs against ML/TF applicable and appropriate to all branches and subsidiaries.

Recommendation 18 is rated Partially Compliant.

Recommendation 19 – Higher-risk countries

New Zealand was rated non compliant with these requirements in its 3rd MER, as there were insufficient obligations regarding higher-risk countries. Since then, New Zealand introduced the AML/CFT Act in 2009. This Recommendation was re-rated to largely compliant in New Zealand's 2nd Follow-Up Report. The FATF requirements have also changed.

Criterion 19.1 - Reporting entities must conduct EDD when establishing business relationships or conducting an occasional transaction with a non-resident customer from a country that has insufficient AML/CFT systems or measures in place (section 22(1)(a)(b) of the AML/CFT Act) and when a reporting entity considers that the level of risk involved is such that EDD should apply to a particular situation (section 22(1)(d)). This is insufficient to apply broadly to business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF. Nonetheless, the AML/CFT supervisors issued a non-binding Guideline, which refers to FATF's lists of high risk and non-co-operative jurisdictions. The MOJ

and Police also issue a statement following each FATF plenary advising of changes to the FATF list of high-risk and non-co-operative jurisdictions.

The range of EDD measures set out in sections 23 to 25 of the AML/CFT Act are also insufficient (see R10.17).

Criterion 19.2 - The New Zealand Governor-General has the power to make regulations prohibiting or regulating the entering into of transactions or business relationships between a reporting entity and any other person (section 155 of the AML/CFT Act). This can include any transactions and business relationships with a specified overseas country. New Zealand can also make regulations mandating EDD requirements (section 153) and has prohibited the establishment of branches and subsidiaries in relation to DPRK specifically (clause 43 of the DPRK Regulations).

Criterion 19.3 - The MOJ and Police issue a statement following each FATF plenary advising of changes to the FATF list of high-risk and non-co-operative jurisdictions. The supervisors also have issued a "Countries Assessment Guideline", which refers reporting entities to FATF's lists of high risk and non-co-operative jurisdictions and FATF Mutual Evaluation reports. DIA and RBNZ also inform their reporting entities of changes to the FATF's lists of high risk and non-co-operative jurisdictions and the FIU also publishes the updated list on its website.

Weighting and Conclusion

There are insufficient requirements for reporting entities to apply EDD, proportionate to the risks, to customers and transactions involving countries for which this is called for by the FATF. The range of EDD measures are insufficient.

Recommendation 19 is rated Partially Compliant.

Recommendation 20 – Reporting of suspicious transaction

In its last MER, New Zealand was rated largely compliant. Deficiencies related to the lack of power to report STRs related to a sufficiently broad range of offences in the designated predicate offence category of illicit arms trafficking and to effectiveness issue – obligations to report FT-related STRs were not fully understood by FIs.

Criterion 20.1 - Under the AML/CFT Act a reporting entity is required to report suspicious activity. Suspicious activity is defined under the AML/CFT Act and covers activity where the reporting entity has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing.

The legislation also outlines the information that must be included in the suspicious activity report, including the requirement to report, as soon as practicable but no later than 3 working days after the reporting entity forms its suspicions. The period for reporting begins when a reporting entity becomes aware of reasonable grounds objectively justifying a suspicion of a reportable transaction.

Criterion 20.2 - Suspicious transactions reporting is covered explicitly under the AML/CFT Act which makes references to prospective transactions, propositions of service, requests and inquiries, thus incorporating attempted transactions. The reporting obligations do not prescribe any limitations on the monetary threshold.

Weighting and Conclusion

New Zealand has a legislative framework to report suspicious activity/transactions.

Recommendation 20 is rated Compliant.

Recommendation 21 – Tipping-off and confidentiality

In its last MER, New Zealand was rated largely compliant as the tipping off provision were not applied to one aspect of the reporting obligation (the obligation to report SPRs which relate to the terrorist-related property of designated persons/entities).

Criterion 21.1 - The AML/CFT Act provides for the protection of persons who disclose or supply information in any suspicious activity report (SAR) or information in connection with any suspicious activity report from civil, criminal or disciplinary proceedings in respect of the disclosure or supply of information or consequences following from it. However, the protection does not apply if the information was disclosed or supplied in bad faith or was disclosed in breach of legal privilege.

Criterion 21.2 - The AML/CFT Act prohibits a reporting entity from disclosing any SAR, any information which will identify, or is reasonably likely to identify, any person who handled a transaction subject to the SAR, or who made or prepared the SAR, or any information that discloses, or is reasonably likely to disclose, the existence of a suspicious activity report. As the list of exceptions under the Act, covers another member of a designated business group of which the reporting entity is a member, the tipping-off provisions would not inhibit information sharing under Recommendation 18.

Weighting and Conclusion

Recommendation 21 is rated Compliant.

Recommendation 22 – DNFBPs: Customer due diligence

In its 3rd MER, New Zealand was rated non-compliant with these recommendations as there were deficiencies regarding CDD thresholds and insufficient coverage of DNFBP sectors. Since then, New Zealand introduced the AML/CFT Act in 2009. New Zealand's 2nd Follow-Up Report found that these changes appeared to have partly addressed the deficiencies. The FATF requirements have also changed. The AML/CFT Act was substantially amended in 2017 to expand its coverage of DNFBP sectors.

The AML/CFT Act covers casinos, law firms, conveyancing practitioners, incorporated conveyancing firms, accounting practices, real estate agents and TCSPs (who are defined as DNFBPs in the AML/CFT Act) and DPMS as a type of HVDs (sections 5 and 6 of the AML/CFT Act). Notaries in New Zealand do not carry out any of the activities set out in criteria 22.1(d). The Act sufficiently covers each category of DNFBPs with the following exceptions in relation to TCSPs and DPMS.

A person acting as a secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons is not captured by the definition of TCSP. Persons solely acting as trustees of family trusts are also exempt from CDD obligations (section 20 of the AML/CFT (Definitions) Regulations 2011). It is unclear what the basis is for this exemption for (see R1.6).

Various types of DPMS are excluded from the Act, including persons engaged in the buying or selling of precious metals or precious stones for industrial purposes (section 5 of the AML/CFT Act) and pawnbrokers (section 31 of the AML/CFT (Definitions) Regulation 2011). Pawnbrokers have a separate regulatory regime under the *Secondhand Dealers and Pawnbrokers Act 2004*, which includes CDD

requirements. It is unclear what the basis is for the exemptions for DPMS involved with industrial purposes (see R1.6),

Criterion 22.1 - DNFBPs are required to comply with the CDD requirements set out in R10 as follows:

a) Casinos must conduct CDD on cash and non-cash (e.g. casino chips) transactions of more than NZD 6 000 that occur outside of a business relationship (section 11 of the AML/CFT (Definitions) Regulation 2011; sections 5 and 14(1)(b) of the AML/CFT Act). Customers that have a business relationship with a casino are subject to CDD requirements regardless of their transaction value. Remote interactive gambling and ship-based casinos are prohibited in New Zealand (sections 9(2) and 10 of the Gambling Act 2003).

b) Real estate agents must conduct CDD on their customers' real estate transactions (sections 5 and 14 of the AML/CFT Act). A customer is specifically defined to include the estate agent's client and excludes any other person involved in the transaction who is not their client except a person who conducts an occasional transaction (section 5B of the AML/CFT (Definitions) Regulations 2011). This is not consistent with the FATF standard, which requires CDD be conducted on both the purchasers and the vendors of the property in all circumstances.

c) DPMS must conduct CDD on cash transactions of NZD 10 000 or more (section 5AB of the AML/CFT (Definitions) Regulations 2011; sections 5 and 14 of the AML/CFT Act). However, DPMS are exempt from a range of other obligations under the AML/CFT Act, including EDD requirements (section 6(4) of the AML/CFT Act). Pawnbrokers, who may also be DPMS, have CDD obligations for any article acquired, including requirements to identify the person from whom an article is received and verifying their identity (sections 42 and 43 of the Secondhand Dealers and Pawnbrokers Act). However, these requirements do not extend to a purchaser of an item, nor does it extend to the full CDD requirements in the AML/CFT Act.

d) Lawyers and accountants are required to conduct CDD when establishing a business relationship with a new customer and where a customer seeks to conduct an occasional transaction or activity (sections 5 and 14 of the AML/CFT Act).

e) TCSPs are required to conduct CDD when establishing a business relationship with a new customer and where a customer seeks to conduct an occasional transaction or activity (sections 5 and 14 of the AML/CFT Act).

The deficiencies identified under R10 also apply to DNFBPs.

Criterion 22.2 - DNFBPs are subject to the same record keeping requirements as all reporting entities. The deficiencies identified under R11 also apply to DNFBPs. As a type of HVD, DPMS must keep CDD records under section 50 of the AML/CFT Act (see R11.2). They are however exempt from the record-keeping requirements in section 49 of the AML/CFT Act (see R11.1 and R11.3). Pawnbrokers which are DPMS must also keep records of the CDD information collected under R22.1 for three years after transaction (section 44 of the Secondhand Dealers and Pawnbrokers Act). This does not meet the five year standard required by R11.

Criterion 22.3 - DNFBPs have the same PEPs requirements as all reporting entities. Therefore, the conclusions made in the R12 analysis apply here as well. DPMS which are HVDs or pawnbrokers do not have PEP requirements.

Criterion 22.4 - DNFBPs are subject to the same requirements of the AML/CFT Act in relation to new technologies as all reporting entities. Therefore, the conclusions made in R15.1 and R15.2 apply here as well. DPMS which are HVDs or pawnbrokers do not have relevant requirements.

Criterion 22.5 - DNFBPs are subject to the requirements of the AML/CFT Act in relation to reliance as all reporting entities. Therefore, the conclusions made in R17 apply here as well.

Weighting and Conclusion

Casinos, real estate agents, law firms, conveyancers, accounting practices, and TCSPs are subject to the requirements of the AML/CFT Act in the same manner as all reporting entities. There are scope issues with the definition of TCSPs and DPMS. The CDD requirements for real estate agents and DPMS do not meet the FATF Standards. The record-keeping requirements for DPMS do not meet the FATF Standards and DPMS do not have PEP and new technology requirements. The deficiencies identified in R10, R11, R12, R15 and R17 also apply here.

Recommendation 22 is rated partially compliant.

Recommendation 23 – DNFBPs: Other measures

In its 3rd MER, New Zealand was rated non-compliant with these requirements, as there was insufficient coverage of DNFBP sectors and a lack of obligations to have AML/CFT procedures. Since then, New Zealand introduced the AML/CFT Act in 2009. New Zealand's 2nd Follow-Up Report found that these changes appeared to have partly address the deficiencies. The FATF requirements have also changed. The AML/CFT Act was substantially amended in 2017 to expand its coverage of DNFBP sectors.

The scope issues regarding TCSPs and DPMS apply here (see R22).

Criterion 23.1 - DNFBPs are subject to the same SAR reporting requirements in the AML/CFT Act as other reporting entities. Therefore, the conclusions made in R20 apply here as well. DPMS which are HVDs only have a voluntary SAR reporting obligation. DPMS which are pawnbrokers have an additional obligation to report stolen goods to the Police (section 39 of the Secondhand Dealers and Pawnbrokers Act).

Criterion 23.2 - DNFBPs are subject to the same requirements for internal control and foreign branch and subsidiaries in the AML/CFT Act as all reporting entities. Therefore, the conclusions made in R18 apply here as well.[42] DPMS which are HVDs are only required to audit their AML/CFT compliance when requested by a supervisor (section 6(d)(ii)(I)). DPMS which are pawnbrokers do not have R18 requirements.

Criterion 23.3 - DNFBPs are subject to the same requirements for high-risk countries in the AML/CFT Act as all reporting entities. Therefore, the conclusions made in R19

42 The FATF currently has a project underway to clarify the application of R18 to DNFBPs. This analysis has considered that all of R18 applies to DNFBPs.

apply here as well. DPMS which are HVDs or pawnbrokers do not have relevant requirements.

Criterion 23.4 - DNFBPs are subject to the same requirements for tipping-off and confidentiality and subsidiaries in the AML/CFT Act as all reporting entities. Therefore, the conclusions made in R21 apply here as well. There are not equivalent tipping-off requirements for pawnbrokers and their reporting requirement.

Weighting and Conclusion

DNFBPs are subject the same requirements in the AML/CFT Act as all reporting entities. There are scope issues with the definition of TCSPs and DPMS. DPMS do not have sufficient obligations regarding the obligations in R18, R19, R21 and R22. The deficiencies identified in R18 and R19 also apply here.

Recommendation 23 is rated Partially Compliant.

Recommendation 24 – Transparency and beneficial ownership of legal persons

New Zealand was rated partially compliant with these requirements in its 3rd MER due to the inability of competent authorities to have access in a timely fashion to adequate, accurate and current information on the beneficial ownership and control of legal persons. New Zealand's 2nd follow-up report found that New Zealand had not yet reached a level of largely compliant. Since then, New Zealand has applied AML/CFT requirements to a wider range of DNFBPs. The FATF requirements have significantly changed as well.

Criterion 24.1 - New Zealand has mechanisms in place that identify and describe the different types, forms and basic features of these legal persons. MBIE oversees the rules, institutions and practices that legal persons in New Zealand and administers the various registers of legal persons. MBIE's website provides authoritative information on the various types of business structures available in New Zealand and the incorporation and registration process of each type.

Legal persons created in New Zealand consist of companies (limited liability, co-operative, unlimited liability), limited partnerships, incorporated charitable trusts, incorporated societies, building societies, credit unions and industrial and provident societies (see Table 1.2 in Chapter 1). The incorporation process and the basic features for these entities are set out in the *Companies Act 1993, Limited Partnerships Act 2008* (LP Act), *Incorporated Societies Act 1908* (IS Act), *Friendly Societies and Credit Unions Act 1982* (FSCU Act), *Building Societies Act 1965* (BS Act), *Charitable Trusts Act 1957* (CT Act) and the *Industrial and Provident Societies Act 1908* (IPS Act) respectively.

In addition, there are bespoke legal persons created by Parliament. These are unique entities that are created by statute and generally are not registered, although some of them may appear on certain MBIE registers. New Zealand however has not identified these entities as high risk nor have they featured in ML/TF investigations.

As set out in R24.3, there are processes for recording basic information on legal persons created in New Zealand. For companies and limited partnerships, there are no specific requirements for obtaining and recording beneficial ownership information, although the Registrar of Companies can request this (sections 365A to 365H of the Companies Act; sections 78A to 78H of the LP Act) (see R24.6).

Criterion 24.2 - New Zealand's 2019 NRA analysed the ML/TF risks of legal persons (in particular, companies, limited partnerships and incorporated societies). The NRA assigned legal persons an overall rating of high vulnerability, with limited liability companies identified as the most vulnerable to ML/TF. They are attractive to criminals because they are readily available, relatively easy to set up and there is a limited liability on the shareholder. Limited liability partnerships were also identified as vulnerable to ML, as only the general partner is disclosed on the public register which can obscure the visibility of ownership. Building societies, co-operatives and credit unions were identified as highly vulnerable to cash laundering in the RBNZ SRA. There are domestic and international aspects in the analysis.

Criterion 24.3 - Legal persons must be registered with MBIE under their respective legislation.

Companies are required to register under section 12 of the Companies Act. All of the necessary information is publicly available, including company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers and a list of directors (Schedule 1 of the *Companies Act 1993 Regulations 1994*).

Limited partnerships must also register with MBIE (section 52 of the LP Act) and provide similar information as to companies (regulation 4 of the *Limited Partnerships Regulations 2008*). While the register is required to be publicly available (section 55 of the LP Act), information on limited partners is not publicly available (section 115 of the LP Act). The basic regulating powers of limited partnerships, contained in its partnership agreement, are also not publicly available.

Incorporated societies are incorporated under sections 7-8 of the IS Act. The publicly available register provides information on the status, address and filings, but does not necessarily include information on officers. Incorporated charitable trusts are registered under section 10 of the CT Act with MBIE. The register includes information on the incorporated charitable trust's status, address and amendments to trust deeds. While it does not contain information on the trustees, a separate Charities Register provides additional information including the names of trustees and officers.

Building societies are incorporated and registered under sections 13-15 of the BS Act. MBIE's publicly available register includes information on the building society's status, officers, and filings (including trust deeds and amendments). Similarly, credit unions are incorporated under the FSCU Act with MBIE. The publicly available register includes information on status, address and filings (including trust deeds and amendments). Industrial and provident societies are established under the IPS Act (Annex 95). MBIE's public register includes information on status, address and filings (including trust deeds and amendments).

Criterion 24.4 - Companies and limited partnerships are required to ensure that the information set out in R24.3 is maintained (sections 94B, 159 and 214 of the Companies Act; sections 59 and 76 of the LP Act). Companies must also maintain a share register in New Zealand at its registered office with the name and address of shareholders and the number of shares (sections 86 and 189 of the Company Act). Companies must notify the Registrar of changes to the location of the share register within 10 days (section 189(4)). Limited partnerships must keep information on the names and addresses of current and past partners at their registered office (section

74 of the LP Act). There are no requirements for limited partnerships to maintain records of proof of their incorporation or certificate of registration.

Incorporated societies must keep a register of its members containing the members' names, addresses, and the dates when they became members (section 22 of the IS Act). Incorporated charitable trusts do not have members or shareholders but must notify the Registrar of changes to the board's name, trust deed or registered office (sections 16 and 25 of the CT Act).

Building societies must maintain a register including the names and addresses of members, which by default must be kept at the societies' registered office (Part 7 of the BS Act). Every credit union is to maintain an indexed register of members (section 130 of the FSCU Act). Every industrial and provident society is required to maintain a register of members (section 8(1)(v) of the IPS Act). Incorporated societies, incorporated charitable trusts, building societies, credit unions and industrial and provident societies do not have specific requirements to maintain the information set out in R24.3. However, obligations to inform MBIE of changes to this information mitigate this to some extent (R24.5).

Criterion 24.5 - Companies must notify the Register of changes to holding company information, directors or their details, alteration of the constitution, the place for maintaining records, registered office or address for service (sections 94B, 159, 32, 189 and 193 of the Companies Act). Failure to do so is an offence. Companies must submit an annual return to the Registrar in (section 214) and failure to do so is an offence by each director of the company (section 214(10)). Directors also have a duty to take reasonable steps to ensure that the share register is properly kept (section 94) and the failure to do so is an offence (sections 373(2)).

Limited partnerships must submit annual returns (sections 76 and 112 of the LP Act). Failure to comply with is requirement is an offence by every general partner (section 76 of LP Act). This potentially year-long delay in updating information is not sufficient to keep information up-to-date.

Changes to an incorporated society's name, registered office and rules must be notified to the Registrar (sections 11A, 18(2) and 21 of the IS Act). Societies must also send the list of names and address of members if requested by the Registrar (section 22), but there is not a general obligation to keep this information up-to-date. There are also no penalties for failing to inform the Registrar, except for changes of the names of societies (section 11A). Incorporated charitable trusts must update the Registrar on changes to the board's registered name, trust deed or rules and registered office (sections 16 and 23 of the CT Act). Failure to do so is an offence (section 23(3)).

Building societies must inform the Registrar of changes to their rules and name within 14 days and failure to do so is an offence (sections 19 and 23 of the BS Act). Credit unions must file an annual return (section 127 of the FSCU Act) and advise the Registrar of changes to rules, name and address (sections 5, 106B and 147). Failure to comply is an offence (section 153 of the FSCU Act). Industrial and provident societies are required to file an annual return (section 8(1)(iv) of the IPS Act) and advise the Registrar of changes to rules, name and registered address (sections 5A, 7 and 8(a)(i) of the IPS Act). There are no legal penalties for failing to keep this information updated. Building societies, credit unions and industrial and provident societies also do not have a specific obligation to keep their registers of members up-to-date.

Criterion 24.6 - There is no general requirement for companies, limited partnerships and other legal persons to hold information on their beneficial ownership. As outlined below, some beneficial ownership information is collected through various mechanisms:

a) The Registrar of Companies has the power, for law enforcement purposes, to request information on the beneficial ownership and control of companies and limited partnerships (sections 365A to 365H of the Companies Act; sections 78A to 78H of the LP Act). This however does not create a general requirement for companies and limited partnerships to *hold* this information.

b) For listed companies, anyone who has a substantial holding in a listed company is required to release a substantial holder notice (section 276 and 277 of the FMC Act). A substantial holding is a relevant interest (including a beneficial interest) in 5%or more of a class of quoted products with voting rights. Listed companies are required to disclose all substantial shareholders in their annual report (section 293 FMC Act).

c) As set out in R10, 11, and 22, reporting entities under the AML/CFT Act are required to conduct CDD on beneficial owners of customers and keep records. Therefore, beneficial ownership information where a reporting entity undertaken CDD on the legal person which is its customer. This information is accessible to supervisors and LEAs (see R27 and 31).

Criterion 24.7 - As set out R24.6, there are no general requirements for companies and limited partnerships to maintain information on their beneficial owners. Beneficial ownership information obtained by reporting entities through CDD is subject to ongoing review. However, there is no explicit requirement to verify the new information and to keep updated records for customer relationships where EDD is not triggered (see R10.7).

For listed companies, a substantial product holder must release a substantial product holder notice if their holdings changes by more than 1% (section 277 of the FMC Act).

Criterion 24.8 - New Zealand has measures in place to ensure that legal persons co-operate with competent authorities to some extent.

a) Companies must have at least one of its directors live in New Zealand or in Australia (if also a director of a body corporate that is incorporated in Australia) (section 10(d) of the Companies Act). All limited partnerships must have at least one general partner that is a New Zealand-registered company or a natural person who lives in New Zealand or Australia (if also director of a company incorporated in Australia). The resident director/partner requirements extend to Australia, on the basis of the close co-operation that exists between the countries. While the *Trans-Tasman Proceedings Act 2010* enables any specified judgements in New Zealand to be enforced in Australia, there do not appear to be any other arrangements to ensure that New Zealand companies and partnerships who meet the residency requirement through an Australian resident director or partner co-operate with New Zealand competent authorities. The residency requirements can also be sidestepped using nominee requirements (see R24.12). There are no equivalent requirements for other legal persons, such as incorporated or mutual societies, however these legal persons are typically domestically focused.

b) While New Zealand places AML/CFT obligations on all DNFBPs, there is no explicit requirement that a DNFBP is authorized by the company and accountable to competent authorities for providing basic information and available beneficial ownership information and giving further assistance to the authorities.

c) As outlined in R24.6, the Registrar may also require a company or limited partnership provide beneficial ownership information.

Criterion 24.9 - There is no general obligation for legal persons (or their representatives) to maintain information and records for at least five years after the date on which the company is dissolved. For companies, liquidators must retain the accounts and records of a company for one year after completion of the liquidation (section 256 of the Companies Act).[43] The same requirement is applicable to limited partnerships (section 92 of the LP Act).

Reporting entities under the AML/CFT Act are required to keep CDD records about customers for five years after the end of the relationship (section 50 of AML/CFT Act). Liquidators who are reporting entities may collect some of this information through the CDD process in some circumstances. However, if a reporting entity is liquidated, there is no requirement for the retention of any records unless the High Court orders their retention (section 53 of the AML/CFT Act).

Criterion 24.10 - Competent authorities, including LEAs, have powers to obtain timely access to the basic and beneficial ownership information on legal persons that is available. The registers for companies and limited partnerships, incorporated societies, building societies and credit unions maintained by the Companies Office are open to the public and online. Certain information is withheld from the register (e.g. names of limited partners), but this information can be requested by competent authorities.

As mentioned in R24.6, the Registrar has the power to obtain information on the beneficial ownership and control of companies. The supervisors and the NZPFIU can request basic and beneficial ownership information from reporting entities (sections 132 and 143 of the AML/CFT Act). If the information is not provided, the supervisors and the NZ Police may also compel the production of the information by search warrant (sections 117 and 118 of the AML/CFT Act; sections 99 and 100 of the Search and Surveillance Act). IR also has extensive powers to request information for revenue purposes (Part 3 of the TA Act). See also the analysis in R27 and R31.

These powers, however, are useful only to the extent to which the information is collected and available in the first place (see R24.7).

Criterion 24.11 - Although not expressly prohibited or regulated in New Zealand, New Zealand has addressed the ML/TF risks of bearer shares. As the name of each shareholder is required to be registered on a company's share registry, as well as the name of the transferee for each transfer of shares, companies are effectively prohibited from issuing bearer shares (sections 35 to 40 and 84 to 87 of the Companies Act).

New Zealand however has not addressed the ML/TF risks of bearer share warrants, as they are not expressly prohibited or regulated in New Zealand. Where a company

43 Section 256 has been amended to extend this to 6 years (section 40 of the *Insolvency Practitioners Regulation (Amendments) Act 2019*). This amendment came into effect in September 2020

issues products that are convertible into shares, they must provide this to the Registrar (section 49 of the Companies Act). However, this notice does not include information as to the holders of these products. In practice however, New Zealand authorities are not aware of any bearer share warrants that exist.

Criterion 24.12 - New Zealand permits nominee directors and shareholders. There is no explicit requirement for nominee shareholders and directors to disclose their status and the identity of their nominator to the company and to the Registrar, and to include such information on the relevant register. However, New Zealand applies the following mechanisms that partially ensure that they are not misused:

a) Under the AML/CFT Act, New Zealand explicitly regulates DNFBPs which carry out the activity of acting as, or arranging for a person to act as, a nominee director or nominee shareholder in relation to legal persons or legal arrangements. In situations where the DNFBP is acting as the nominee shareholder or nominee director, it has the obligation to conduct CDD as per the requirements of the AML/CFT Act. In such situations, identification and verification information, including beneficial ownership information, must be available with the DNFBP. These measures however do not extend to nominees that are not captured as DNFBPs under the AML/CFT Act (for example, a person who acts as a nominee director or shareholder and they are not a business).

b) Nominee directors have the same duties as ordinary directors, including acting in good faith and in what they believe to be the best interests of the company (section 131 of the Companies Act). This imposes upon them a duty of care (section 137). Although not explicit, a person who appoints and directs a nominee director would also likely be treated as a director under New Zealand law and be subject to the same duties (due to the definition of director in section 126). However, these obligations will not identify a director who is a nominating director.

c) Reporting entities must also conduct EDD when they identify a company with nominee shareholders (section 22(1) of the AML/CFT Act). However, the reporting entity will need to identify that the company has nominee shareholders in the first place. Reporting entities may also identify nominees as part of their beneficial ownership obligations in the CDD process.

Criterion 24.13 - There are a range of sanctions for legal or natural persons that fail to comply with the basic and beneficial ownership requirements detailed above. Not all of these are sufficiently dissuasive.

For breaches under the Companies Act, failing to maintain a share register can result in a company or director being liable to a fine of up to NZD 10 000 (sections 87(4), 373 and 374). Providing incorrect or false information to the Registrar is an offence and can result in a fine of up to NZD 200 000 or a prison term not exceeding 5 years (section 377). Failing to give notice of a change in ultimate holding company (section 94B(3)), failing to advise a change of directors (section 159(3)), failing to comply with a beneficial ownership notice (sections 365F-365G) and failing to provide an annual return (section 214(10) are all offences. If the board of a company fails to comply with these provisions, every director of the company commits an offence and can be liable for a fine of up to NZD 10 000. These are not sufficiently dissuasive. Companies can also be deregistered for intentionally providing inaccurate information, for failing to respond to a beneficial ownership notice and for failing in a persistent or serious way

to comply with the Act (section 318) and directors may be disqualified for committing an offence under the Act (section 383(1)(b)).

Similar sanctions apply to breaches of the LP Act. Failure to comply with the requirement to maintain lists of both general and special partners Act is an offence and each partner can be liable to a fine of up to NZD 10 000 (section 74 of the LP Act). These are not sufficiently dissuasive. Limited partnerships must also be deregistered if a partner provides inaccurate information or fails to comply with the Act in a persistent or serious way (section 98A).

There are insufficiently dissuasive sanctions for some of the breaches under the IS Act and the CT Act. For example, if a society carries on its operations without having a registered office, the fine applicable to each officer and member of the society is one shilling a day (section 23 of the IS Act). A similar penalty applies for breach of the information requirement for incorporated charitable trusts (section 12 of the CT Act).

Under the BS Act, the provision of false information is an offence for which a person is liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding NZD 1 000 or to both (section 133). Under the FSCU Act, the penalty for providing false or misleading information is fine not exceeding NZD 750 (with an additional NZD 50 fine for each additional week). These are not sufficiently dissuasive.

Significant sanctions apply to breaches of obligations in the AML/CFT Act (see R35). For example, failing to comply with record-keeping requirements is a civil liability act (section 78(e) of the AML/CFT Act). On conviction, an individual can be liable to fine of up to NZD 200 000, and a body corporate can be liable to a fine of up to NZD 2 million (section 90(3)(a)(b) of the AML/CFT Act). These are sufficiently proportionate and dissuasive.

Failing to comply with the information-gathering powers in sections 143-143B of the TA Act can lead to criminal penalties, including fines (of up to NZD 25 000 for a first offence, or NZD 50 000 for repeat offences) or imprisonment of up to five years. These are sufficiently proportionate and dissuasive.

Criterion 24.14 - New Zealand can rapidly provide international co-operation in relation to basic ownership and the beneficial ownership information it has available:

a) New Zealand can facilitate access to basic information held on its relevant registers. Foreign competent authorities can freely access basic information via the online registries which are publicly available.

b) Authorities can exchange information through a variety of channels, including MLA and police-to-police assistance (see R37 and R40). MBIE typically respond to law enforcement requests for information within 1 to 2 days for simple requests and 7-14 days for more complex requests involving multiple companies and data items. IR is able to provide international co-operation regarding beneficial ownership through a wide range of tax treaties (see section 17B of the TA Act). The supervisors also are empowered to co-operate international counterparts (section 131 of the AML/CFT Act). The deficiencies noted in R37 apply here.

Criterion 24.15 - While competent authorities in New Zealand monitor the assistance they receive from foreign counterparts (see R37), they do not specifically differentiate requests for basic and beneficial ownership information in their case monitoring. IR regularly provides feedback to other tax authorities from which assistance was

received as a standard step in the exchange of information process. The NZPFIU does not formally monitor the quality of assistance received from other countries in response to its requests for assistance in locating beneficial owners residing abroad. FMA has a process to monitor the quality of assistance received from foreign counterparts and provide feedback. Formal feedback is provided through the annual IOSCO Monitoring Group Survey.

Weighing and Conclusion

At incorporation, there are no specific requirements for obtaining and recording beneficial ownership information beyond the immediate shareholders (including ultimate natural persons who own the legal person or those who exert control through means other than ownership). For limited partnerships where general partners are not natural persons, there are no specific requirements to obtain information on the ultimate natural persons. There are no requirements for limited partnerships to maintain records of proof of their incorporation or certificate of registration.

There are insufficient requirements for companies to take reasonable measures to obtain and hold up-to-date beneficial ownership information and keep sufficient records. Fines prescribed for violations for some information requirements (e.g. in relation to incorporated societies and charitable trusts) are not proportionate and insufficiently dissuasive. There are insufficient requirements to mitigate the risks posed by bearer share warrants and nominee shareholders and directors.

Recommendation 24 is rated partially compliant.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

New Zealand was rated non-compliant with these requirements in its 3rd MER because there were no requirements to obtain, verify and retain adequate, accurate and current information on beneficial ownership and control of trusts. New Zealand's 2nd follow-up report found that New Zealand had not yet reached a level of largely compliant. Since then, New Zealand has applied AML/CFT requirements to a wider range of DNFBPs. The FATF requirements have significantly changed as well.

New Zealand is a common law country. Trusts are governed through a combination of common law and legislation (*Trustee Act 1956* and *Perpetuities Act 1964*). New Zealand has introduced new legislation (*Trusts Act 2019*) to replace the Trustee Act and Perpetuities Act, however the new Act did not commence until January 2021. Therefore, the Trusts Act 2019 is not used as basis for arriving at New Zealand's level of compliance under this Recommendation, but is referenced in footnotes as appropriate.

Criterion 25.1

(a) There is not an explicit statutory requirement for all trustees to obtain and hold adequate, accurate and current information on the identity of the settlor, the trustees, the protector and the beneficiaries or class of beneficiaries and any other natural

person exercising ultimate effective control.[44] New Zealand does not have a register of domestic trusts but has registers on certain types of trusts.

Under common law, trustees have fiduciary duties to understand the terms of a domestic trust (*The Taumarunui Museum Trust v Ruapehu District Council* (HC) 31/08/06). Connected to this are obligations for trustees to consider the settlor's intentions when exercising discretion (*Clement v Lucas* [2017] NZHC 3278) and to identify all classes of beneficiaries before making a distribution (*Re Hay's Settlement trusts* [1982] 1 WLR 202 (Ch)). While this may mean that some information regarding the parties to a trust is collected by the trustee, this does not meet the FATF Standard that adequate, accurate and current information about all relevant parties to a trust is held and maintained by the trustee. In particular, there are no explicit obligations for identifying ultimate beneficial ownership and control of parties which are legal persons.

Where a trustee is acting in a professional capacity as a business, they will have obligations under the AML/CFT Act as a DNFBP. They are required to conduct CDD, apply EDD, ongoing monitoring, and record keeping measures (see R22). The AML/CFT supervisors have released non-binding Guidelines on CDD for trusts, which states that the beneficial owners for a trust include the trustee and any other individual who has effective control over the trust, specific trust property, or with the power to amend the trust's deeds, or remove or appoint trustees (see also R10). This might include a protector or special trustee (if there are any), or one or more of the beneficiaries of the trust. However, trusts are subject to EDD in line with sections 23 and 24 of the AML/CFT Act which explicitly require that reporting entities obtain and verify the identity of each beneficiary of the trust and the source of funds. While such requirements are applicable to professional trustees to obtain and hold adequate, accurate and current beneficial ownership, it does not capture those domestic trusts not created by reporting entities.

In addition, if the trust derives taxable income or makes a taxable distribution to a beneficiary, it must register and file a tax return with IR (section 59(3) of the TA Act) This includes providing the name of each beneficiary, date of birth, address and other details (Forms IR6 and IR6B).

For New Zealand Foreign Trusts, there are more extensive rules as part of the registration and disclosure process under sections 59B-59D of the TA Act. New Zealand resident trustees of foreign trusts must register with IR and provide the trust deed and details of each connected person (including settlors, trustees, protectors, appointers, parents or guardians and beneficiaries) to the trust (sections 59B-D of the TA Act). If the trust has a resident settlor but not a resident trustee, the settlor must provide this information (section 59).

(b) There are no specific provisions for trustees to hold basic information on other regulated agents and service providers including investment advisors, accountants and tax advisors.[45] Professional trustees which are DNFBPs apply CDD measures on

44 The Trusts Act 2019 places extensive requirements on trustees to hold documents and maintain information on the trust.

45 There are requirements in the Trusts Act 2019 for trustees to keep records of any written contracts entered into during that trustee's trusteeship, and any accounting records and financial statements prepared during that trustee's trusteeship. Such records are expected to include information on accountants and any other service providers with whom the trust engaged in a contract.

other regulated agents and service providers in the course of dealing with them as customers.

(c) Records of customer identification and verification of identity obtained by professional trustees in the course of their dealings with trusts as customers are subject to record keeping requirements under section 50 of the AML/CFT Act. Such records must be kept for at least 5 years after the end of the business relationship (see R11). For trusts that generate income, trustees must keep certain records for a period of 7 years after the end of the income year (section 22(2) of the TA Act).

Criterion 25.2 - There is no general obligation for trustees to keep the information referred to in R25.1 accurate and up-to-date.[46] Professional trustees which are DNFBPs must conduct ongoing CDD to ensure that the business relationship and the transactions are consistent with their knowledge about the customer and the customer's business and risk profile, and to identify any ground for reporting suspicious activity (section 31 of the AML/CFT Act) (see R10).

For trusts that are deriving taxable income or making taxable distributions to beneficiaries, the annual tax returns to IR must include up-to-date information on beneficiaries and trustees (section 22 of the TA Act).

For foreign trusts, the trustee is required to inform IR within 30 days of any changes to the information provided at the time of the foreign trust registration (sections 59(B)(5) and 59(C)(2) of the TA Act).

Criterion 25.3 - There are no explicit requirements for trustees to disclose their status to reporting entities when forming a business relationship or carrying out an occasional transaction above the threshold. Reporting entities, however, must conduct CDD on their customers, beneficial owners of customers and any person acting on behalf of a customer (see R10). Reporting entities are also required to obtain information as to the nature and purpose of the proposed relationship as part of the CDD measures and determine whether the customer should be subject to EDD.

Criterion 25.4 - There is nothing in New Zealand trust law to prevent trustees of a trust from providing competent authorities with information relating to the trust. Public and private sector agencies can disclose information for law enforcement purposes under Privacy Principle 10(1)(c)(i) and Privacy Principle 11(e)(i) of the Privacy Act.

For reporting entities, they must obtain information on the beneficial ownership and assets of trusts to be held or managed under a business relationship (see sections 11, 15-17 and 22-24 of the AML/CFT Act). If the trustees do not provide the required information, the reporting entity cannot lawfully have a business relationship with the trustees (section 37). While privileged communications are exempt from disclosure under the AML/CFT Act, the term is defined narrowly in section 42 to mean communication between two lawyers or a lawyer and its client and would not apply to documents such as trust deeds.

Criterion 25.5 - Competent authorities can obtain relevant information held by trustees, and other parties, including reporting entities, regarding trusts created in, or operating in, New Zealand. This includes information on beneficial ownership, residence of the trustee and any assets held or managed by a reporting entity. The

46 Each of the trustees is required under section 45 of the Trust Act 2019 to keep, so far as is reasonable, the trust deed and any other document that contains terms of the trust and any variations made to the trust deed or trust.

supervisors and the NZPFIU have information-gathering powers under the AML/CFT Act. Search warrant powers are also available to LEAs under the Search and Surveillance Act and the section 101 of the CPRA. IR has broad information gathering powers under section 17B of TA Act for tax purposes. See R27 and R31 for further information.

However, these powers are contingent on this information being available in the first place. As set out in R25.1, there are not uniform obligations for trustees to collect and hold identity information, including information on beneficial owners.

Criterion 25.6 - The authorities may exchange information on trusts with foreign counterparts based on the procedures outlined under R37 and R40. The NZPFIU may also share information, including beneficial ownership, with foreign counterparts as part of its respective functions (sections 142(ka) and 143 of the AML/CFT Act), as can the AML/CFT supervisors (section 132 AML/CFT Act). Information on New Zealand Foreign Trusts held by IR is shared with the NZPFIU and the DIA (section 28 of the TA Act) and with international partners. There is no information-sharing agreement between IR and the other supervisors (RBNZ and FMA). For domestic trusts, there is not a domestic register of trusts that can be accessed by local or foreign authorities. Instead, trust information will need to be accessed either from trustees or from reporting entities using competent authorities' information-gathering powers (see R27 and R32).

Criterion 25.7 - Under the AML/CFT Act, failure to comply with CDD or record-keeping requirements is subject to a range of criminal and administrative sanctions (see R35). For trusts that derive taxable income and are registered with IR, proportionate and dissuasive sanctions apply for failures to keep sufficient records and provide information to IR. Penalties range from NZD 4 000 for a first offence to 50 000 for multiple offences where a person knowingly commits the offence (sections 143 and 143A of the TA Act). Similar penalties for failure to comply with the rules on New Zealand Foreign Trusts.

Breaches of trustees' fiduciary duties may give rise to claims by the beneficiary and legal liability of the trustee based on these claims, including removal of the trustee and claims for losses. These remedies are only available to beneficiaries and not competent authorities. In the most extreme cases, a trustee who acts dishonestly and contrary to the terms of the trust commits the offence of criminal breach of trust and is liable to imprisonment for up to 7 years (section 229 of the *Crimes Act 1961*). A beneficiary may also apply to the court to review an act, omission or decision of a trustee (section 68 of the Trustee Act 1956). However, in the absence of a sufficient obligations to collect beneficial ownership or general trust information (see R25.1), there are neither sufficient sanctions for failure to comply or sufficient legal liability for trustees.

Criterion 25.8 - There is a wide range of sanctions imposed against persons failing to grant the competent authorities timely access to trust related information, provided that this information is available in the first place (see R25.1).

For trustees who are reporting entities, it is an offence to wilfully obstruct a supervisor in the exercise of their powers or performance of their functions (section 102 of the AML/CFT Act). An individual person who is convicted of an offence is liable to, either or both, imprisonment of up to 3 months and a fine of up to NZD 10 000. A body corporate or partnership is liable to a fine of up to NZD 50 000. Reporting entities can also be liable for civil liability acts for failing to keep records as required

by the Act (see section 78). The maximum amount of a pecuniary penalty in the case of an individual is NZD 200 000, in the case of a body corporate or partnership is NZD 2 million. Sanctions under the AML/CFT Act are both proportionate and dissuasive

A person who obstructs IR in carrying out their duties under the TA Act commits an offence and is liable the first time the person is convicted of that type of offence, to a fine not exceeding NZD 25 000 and a fine not exceeding NZD 50 000 for future offences (section 143H).

Under the Search and Surveillance Act, failure to comply with a production order is an offence for which a person is liable on conviction to imprisonment for a term not exceeding one year in the case of an individual and a fine not exceeding NZD 4 000 in the case of a corporate body. See also R35.

Weighting and Conclusion

The requirements to obtain and hold adequate, accurate and current information on the identity of the settlor, the trustees, the protector and the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control over the trust are not mandated on all types of trustees. There are no specific provisions for trustees to hold basic information on other regulated agents and service providers including investment advisors, accountants and tax advisors. The requirements to keep accurate and up-to-date information on the trust are not mandated on all types of trustees. There are no explicit requirements for trustees to disclose their status to reporting entities when forming a business relationship or carrying out an occasional transaction. Sanctions and liability on trustees are insufficient.

Recommendation 25 is rated Partially Compliant.

Recommendation 26 – Regulation and supervision of financial institutions

In its 3rd MER, New Zealand was rated non-compliant with these requirements mainly because (i) other than registered banks, no category of FI was subject to any regulation and supervision for compliance with AML/CFT requirements; and (ii) there was no designated competent authority to ensure the compliance of FIs (other than registered banks) with AML/CFT requirements. Since then, New Zealand has made legislative amendments to bring all financial sectors under AML/CFT regulatory regime. New Zealand's 2nd Follow-Up Report found that these changes appeared to have largely addressed the deficiencies. The FATF requirements have also changed.

Criterion 26.1 - RBNZ, FMA, and DIA are the three AML/CFT supervisors for financial sectors in New Zealand. RBNZ supervises registered banks; life insurers; and NBDTs. FMA supervises derivatives issuers; brokers and custodians; equity crowd-funding platforms; financial advisers; MIS managers; peer-to-peer lending providers; DIMS providers; licensed supervisors (formally known as securities trustees); and issuers of securities. DIA supervises the remaining FIs, including MVTS providers; currency exchange, payment; non-bank non-deposit taking lending; non-bank credit card; stored value instruments; financial leasing; tax pooling; factoring; payroll remittance; debt collection; cash transport; and safe deposit boxes (section 130 of the AML/CFT Act).

No agency in New Zealand has a mandate to supervise for implementation of TFS obligations.

Criterion 26.2 - There is no general licencing or registration regime under the AML/CFT Act. Instead, FIs are registered and licenced as follows.

Core Principles FIs in New Zealand include registered banks; life insurers; MIS managers; brokers and custodians; equity crowd-funding platforms; DIMS providers; financial advisers; issuers of debt, equity or derivatives; and licensed supervisors. All Core Principles FIs are required to be licensed in New Zealand as well as being registered on the FSPR except for wholesale MIS managers, wholesale DIMS providers, wholesale derivative issuers, debt and equity issuers (where issuing securities in the ordinary course of their business) and brokers and custodians, which are only required to be registered on the FSPR (Part 5 of the Reserve Bank Act; Part 2 of the IPS Act; Part 6 of the FMC Act; Part 2 of the *Financial Markets Supervisors Act 2011* (FMS Act); Part 2 and 3 of the *Financial Advisors Act 2008* (FA Act); Part 2 of the FSP Act).

NBDTs and peer to peer lending providers are required to be licensed and registered on the FSPR (section 11 of the NBDT Act; section the 390 of FMC Act and clause 184 of the *Financial Markets Conduct Regulations 2014*; Part 2 of the FSP Act). Other FIs, including money changers and MVTS providers, are required to be registered on the FSPR (Part 2 of the FSP Act), except for providers of tax pooling, factoring, payroll remittance, debt collection, cash transport and safety deposit boxes. These FIs do not have any licensing or registration requirements.

The Reserve Bank Act does not have specific provisions that prohibit the establishment of shell banks in New Zealand. In practice, shell banks are prohibited from being established or operated in New Zealand through the implementation of RBNZ's licencing regime and Statements of Principles.

Criterion 26.3 - BNZ conducts ongoing checks of fitness and propriety (e.g. criminal record checks and home regulator checks) for chief executive officers, directors, senior managers and persons having significant interest of registered banks (Part C and M of Statements of Principles, sections 73-73B of the RBNZ Act); directors and senior officers of NBDTs (section 15 of the NBDT Act); and directors or relevant officers of licensed life insurers (sections 34-43 of the IPS Act). For NBDTs and life insurers, the suitability checks tests do not extend to shareholders or controllers.

FMA assesses FMC-licensed FIs, including retail derivatives issuers; equity crowd-funding platforms; retail MIS managers; peer to peer lending providers and DIMS providers, on an ongoing basis against the eligibility criteria, which include fit and proper tests on directors, senior managers and controllers (i.e. beneficial owners) of the licensed FIs (section 396 of the FMC Act and section 189 of the FMC Regulations). Directors, senior managers and controllers of licensed supervisors are also subject to similar fit and proper enforced by FMA (section 16 of the FMS Act; sections 4 and 6 of *Financial Markets Supervisors Regulations 2014*).

For FIs that are registered on the FSPR, the Registrar of Companies and FMA have procedures (including annual confirmation) in place to ensure these FIs are continuously qualified to be registered on the FSPR. FIs are disqualified if their controlling owners, directors or senior managers have been convicted of a crime involving dishonesty or ML/TF in New Zealand or overseas (Part 2 of the FSP Act). However, section 14 of the FSP Act defines controlling owner as any person beneficially owns 50% or more of a financial service provider. The 50% threshold appears large and is inconsistent with relevant thresholds adopted in other legislations (e.g. the RBNZ Act and FMC Regulations).

The FIs that are not required to be licensed or registered in New Zealand are not subject to any market entry requirements (see R26.2).

Criterion 26.4

(a) New Zealand was subject to IMF's Financial Sector Assessment Programme in 2016. Regarding Basel Committee on Banking Supervision Principles (BCPs), New Zealand was rated materially non-compliant on six AML/CFT-related BCPs and rated largely compliant for BCPs relating to consolidated group supervision. Regarding International Association of Insurance Supervisors Principles, New Zealand was rated as partly observing six relevant principles, including Principle 23 on group-wide supervision. While the IMF did not conduct a full detailed assessment of New Zealand's securities regulation in 2016 due to the then nascent regulatory regime for securities, it conducted a review on some relevant principles in form of technical notes. The IMF's technical notes, supplemented by FMA's self-assessment, suggest that the relevant IOSCO Principles and Responsibilities are broadly implemented. Updates provided by RBNZ indicated that some progress had been made to follow up the recommendations made by IMF, e.g. to undertake reviews on RBNZ Act and IPS Act.

(b) For all other FIs, including MVTS providers and money changers, they are regulated and subject to supervision to ensure compliance with the AML/CFT Act.

Criterion 26.5 - RBNZ, FMA and DIA adopt a risk-based approach to conduct their AML/CFT supervision on FIs.

RBNZ conducted SRAs in 2011 and 2017 to assess the ML/TF risks of the three financial sectors under its AML/CFT supervision. Registered banks are subject to more intensive supervision as it was assessed as high risk, while life insurers are only subject to limited on-site inspections due to their low level of risk. RBNZ determines the frequency and intensity of on-site and off-site AML/CFT supervision of individual institutions based on its AML/CFT Risk Assessment Model, which utilises a range of data sources, and their compliance history.

FMA also conducted SRAs in 2011 and 2017 to assess the ML/TF risk of the nine financial sectors under its AML/CFT supervision. Similar to RBNZ, FMA assesses the ML/TF risks of individual FIs and assigns risk ratings using a red flag model. FMA supervised FIs are selected for on-site inspections or desk-based reviews on a risk-based approach, which also determines the frequency and intensity.

DIA conducted four SRAs in 2011, 2017-18 and 2019, which included the financial sectors under DIA's AML/CFT supervision. DIA uses an Entity Risk Model, which combines analysis of FIs' annual reports and compliance history, to construct the risk profile of each supervised FI. DIA determines the frequency and intensity of on-site and off-site AML/CFT supervision of individual institutions based on its Entity Risk Model.

Criterion 26.6 - FIs are required to submit annual reports on their risk assessments and AML/CFT programme to their relevant supervisors (section 60 of the AML/CFT Act). The reports enable the supervisors to make a judgement about the risk of non-compliance of a particular FI and are used in assessing risk. RBNZ, FMA and DIA update the risk profiles of individual FIs every year when the annual report data is received. In case of any major events (e.g. negative news received from internal or external sources) or developments in the management and operations of the FIs or their groups, case examples indicate that AML/CFT supervisors will adjust their

supervisory approach in response, albeit a review of the ML/TF risk profile of the FI does not always occur.

Weighting and Conclusion

Some shortcomings were identified in the market entry: (a) RBNZ does not extend the fit and proper test to shareholders or controllers of NBDTs and life insurers; (b) some core principle FIs are only required to be registered on the FSPR without a need to be licensed; (c) providers of factoring, tax pooling, payroll remittance, debt collection, cash transport and safety deposit boxes are not required to be licensed or registered in New Zealand, and hence they are not subject to any market entry requirements and (d) the fit and proper test only applies to controlling owner of FIs with beneficial ownership equal to or more than 50% under the FSPR registration regime. Also, Core Principles FIs are not regulated and supervised fully in line with the Core Principles that are relevant to AML/CFT, no agency has a mandate for supervision of FIs for implementation of TFS obligations and the supervisors do not always review the assessment of a FI's ML/TF risk profile when there is a major event or development.

Recommendation 26 is rated Partially Compliant.

Recommendation 27 – Powers of supervisors

In its 3rd MER, New Zealand was rated non-compliant with these requirements mainly because other than RBNZ's powers in relation to registered banks, there was no supervisor with any powers to monitor and ensure compliance with AML/CFT requirements and the RBNZ's role in relation to registered banks' compliance was very limited. Since then, New Zealand has made legislative amendments to empower relevant supervisors. New Zealand's 2nd Follow-Up Report found that these changes appeared to have largely addressed the deficiencies. The FATF requirements have also changed.

Criterion 27.1 - RBNZ, FMA and DIA have powers to supervise and ensure compliance by their respective FIs with AML/CFT requirements. This includes powers to require the production of documents, conduct onsite inspections, provide guidance, co-operate and share information, and initiate and act on requests from overseas counterparts (section 132 of the AML/CFT Act; Part 5 of the RBNZ Act; Part 3 of the FMA Act; Part 8 of the FMC Act).

Criterion 27.2 - RBNZ, FMA and DIA have the authority to conduct inspections of their respective FIs at any time with or without a court order (sections 117-118 and 133 of the AML/CFT Act; section 66E of the RBNZ Act; sections 51-52 of the NBDT Act; sections 130 and 132 of the ISP Act; section 29 of the FMA Act).

Criterion 27.3 - RBNZ, FMA and DIA are authorised to compel production of any records, documents, or information relevant to their monitoring the compliance of their respective FIs with the AML/CFT Act without the need for a court order (section 132(a) of the AML/CFT Act; section 93 of the RBNZ Act; section 47 of the NBDT Act; section 121 of the ISP Act; section 25 of the FMA Act).

Criterion 27.4 - RBNZ, FMA and DIA are empowered to impose a range of disciplinary and financial sanctions on their respective FIs if the FIs fails to comply with requirements in the AML/CFT Act. For example, supervisors can order a reporting entity to undertake an audit of its AML/CFT programmes (section 59(2) of the AML/CFT Act). Supervisors can bring civil proceedings against a reporting entity if it fails to comply with the AML/CFT requirements set out in Part 2 of the AML/CFT Act

(sections 78 and 79). This includes powers to issue a formal warning (section 80); accept an enforceable undertaking (section 81), seek an injunction from the High Court (sections 85 and 87); or apply to a court for a pecuniary penalty (section 90). Depending on the obligation that is breached, the maximum pecuniary penalty may be NZD 100 000 or NZD 200 000 for an individual or NZD 1 000 000 or 2 000 000 for a legal person. However, the range of sanctions available to the supervisors is insufficient, as they lack the power to apply administrative pecuniary penalties.

There is no power under the AML/CFT Act to withdraw, restrict or suspend the FI's licence or the FI's registration to the FSPR. For those FIs that are subject to licensing, although RBNZ and FMA can withdraw, restrict or suspend the licenses of respective supervising FIs under other legislation if there are is breach of licensing conditions or any prudential concerns, it is unclear as to whether a breach of AML/CFT obligation will lead to withdrawal, restriction or suspension of the licenses given the absence of specific legislative empowerment and case examples (sections 113 and 113A of the RBNZ Act; sections 21 and 56 of the NBDT Act; section 30 and part 4 of the IPS Act sections 396, 400, 403, 408 and 410 of the FMC Act; part 2 of the FMS Act; section 59 of the FA Act).

For those FIs that are not subject to licensing but only required to be registered on the FSPR (see R26.2), any non-compliance with AML/CFT Act will not lead to a deregistration from the FSPR as it is not one of the registration requirements under the FSP Act.

For those FIs that are not required to be licensed or registered in New Zealand (see R26.2), the lack of market entry requirements has an impact to the sanctions available for non-compliance with AML/CFT requirements.

Weighting and Conclusion

There are minor shortcomings with respect to New Zealand's ability to withdraw, restrict or suspend the license or registration of FIs for failure to comply with AML/CFT requirements and the range of sanctions that can be applied.

Recommendation 27 is rated Largely Compliant.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 3rd MER, New Zealand was rated non-compliant with these requirements because there were no designated supervisors for DNFBPs. Since then, New Zealand has made legislative amendments to bring DNFBPs under AML/CFT regulatory regime. New Zealand's 2nd Follow-Up Report found that these changes appeared to have partly addressed the deficiencies. The FATF requirements have also changed.

The scope issues regarding some TCSPs and DPMS apply here (see R22). No agency in New Zealand has a mandate to supervise for implementation of TFS obligations (see R26).

Criterion 28.1 - Casinos are subject to AML/CFT regulation and supervision as follows:

a) All casino operators in New Zealand are required to be licensed by the Gambling Commission under the Gambling Act (sections 119 and 124-137). New casinos are prohibited (section 10) but existing casino licenses may be renewed (sections 134-138). Renewed licenses are granted for 15 years. Internet gambling is banned (section 9). Any ship-based casinos must cease

operations while within New Zealand territorial waters due to the prohibition against new casinos.

b) The Gambling Commission examines the suitability of the applicant for a casino operator's license, including honesty, financial position, business skills and management structure of the applicant (sections 124 and 125 of the Gambling Act). The suitability check and investigation applies to any person who has significant influence including director, senior management and beneficial owners of the casino license holders (section 7 of Gambling Act).

c) All casino operators in New Zealand are supervised for compliance with AML/CFT requirements by DIA (section 130(d) of AML/CFT Act).

Criterion 28.2 and 28.3 - DIA is responsible for monitoring and ensuring compliance of DNFBPs in New Zealand with AML/CFT requirements (section 130(c) of AML/CFT Act).

Criterion 28.4

a) DIA has powers to supervise and monitor the compliance of DNFBPs with AML/CFT requirements, including the powers to require the production of documents, conduct onsite inspections, provide guidance, co-operate and share information, and initiate and act on requests from overseas counterparts (section 132 of AML/CFT Act).

b) As DIA does not register or license DNFBPs, market entry is controlled through other legislation as follows:

    a. Lawyers must have a practising certificate provided by the NZLS in order to practice in New Zealand under the *Lawyers and Conveyancers Act 2006* (LC Act) and *LC Act (Lawyers: Admission) Rules 2008*. While a lawyer can also act as a conveyancer, a person may also register by NZSC as a conveyancing practitioner without also practising as a lawyer. Lawyers must be fit and proper persons, and whether the person has been convicted of an offence in New Zealand or a foreign country is a relevant criterion (sections 41, 55 and 83 of the LC Act). Incorporated law firms can only have non-lawyer shareholders in very limited circumstances and are subject to controls over the operations of the firms. The same requirements apply to conveyancing practitioners (sections 49-51, 81 and 83 of the LC Act).

    b. Any person in New Zealand may call themselves an accountant. However, a person may only call themselves a chartered accountant, associate chartered accountant, registered accountant or accounting technician if they are a member of CAANZ and registered under section 14 of the *New Zealand Institute of Chartered Accountants Act 1996* (NZICA Act). Applicants to become chartered accountants who are resident in New Zealand have to provide a copy of their criminal conviction history record when they apply for membership and when they apply for a certificate of public practice. At both of these stages they also need to disclose any events that impact whether they are 'fit and proper'. Whilst they are a member, they must disclose unethical behaviour or criminal convictions and other disclosure events to CAANZ (section 19 of the NZICA Act; Rules 10 and 13 of NZICA Rules). There are no registration or fit and proper requirements for

individuals providing accountancy services outside of CAANZ membership.[47]

c. Real estate agents in New Zealand must be licensed by REA. An applicant must be a fit and proper person and a person with a conviction record of dishonesty offence in the last 10 years is prohibited from being licensed (sections 36 and 37 of the *Real Estate Agents Act 2008* (REA Act)). REA undertakes criminal conviction history checks for all new and renewed real estate licenses. A company may also be licensed as an agent if at least one officer of the company qualifies individual agents but there are no entry control requirements for management and beneficial owners of such corporate real estate agents.

d. TCSPs: Except for the securities trustees licensed the FMS Act, TCSPs are not required to be licensed or registered in New Zealand, and hence are not subject to entry controls.

e. DPMSs: DPMS in New Zealand are not subject to any entry controls.

c) Being the supervisor for DNFBPs, DIA can impose a range of civil and administrative sanctions to deal with DNFBPs that fail to comply with AML/CFT requirements (see also R27 and R35). DIA does not have the ability under the AML/CFT Act to withdraw, restrict or suspend the ability of a reporting entity to undertake financial activities for failures to comply with AML/CFT obligations. In addition to DIA, the following sanctions are available to the other competent authorities or self-regulatory bodies:

a. Lawyers' non-compliance with the AML/CFT regime can constitute misconduct or unsatisfactory conduct (Rules 1.4 of the *LC Act (Lawyers: Conduct and Client Care) Rules 2008* and Rule 10 of the *LC Act (Conveyancing Practitioners: Conduct and Client Care) Rules*). The NZLS Standards Committee can make findings of unsatisfactory conduct and make a range of orders, including ordering that the lawyer or conveyancer be reprimanded or pay a fine not exceeding NZD 15 000. The Disciplinary Tribunal is empowered to make a finding of misconduct and matters referred by a Standards Committee, and make an order striking off the roll, cancel registration or suspend from practice (sections 6, 7, 12, 156, 214 and 242 of the LC Act). Case studies on lawyers' non-compliance with the AML/CFT Act being raised with NZLS were provided.

b. Conveyancers: The same analysis as in (a) for lawyers applies to conveyancers, except the relevant body is NZSC.

c. Accounting professionals: CAANZ members have to notify the Professional Conduct Committee when a disclosure event occurs, which can include failure to comply with the AML/CFT Act. Upon investigation, the Professional Conduct Committee may undertake a range of actions, including to refer the matter to the Disciplinary Tribunal for a hearing. The Disciplinary Tribunal may exercise

47. The *Insolvency Practitioner Regulation Act 2019* received Royal Assent on 17 June 2019. This introduced registration requirements for insolvency practitioners (a number of whom would be lawyers or chartered accountants). However, this Act did not become operational until 17 June 2020.

disciplinary powers, including to cancel or suspend any certificate of public practice held by the member or to declare that the member is ineligible to hold a certificate of public practice for a period not exceeding 5 years (Rule 13 of the NZICA Rules). The above sanctions do not apply to individuals providing accountancy services outside of CAANZ membership.

d. Real estate agents: Any non-compliance with the AML/CFT Act (e.g. disciplinary action taken by DIA) could be considered unsatisfactory conduct or misconduct under the REA Act. Unsatisfactory conduct or misconduct cases are handled by a Complaints Assessment Committee and/or Disciplinary Tribunal, which are empowered to take disciplinary actions including an order censuring or reprimanding the licensee or imposing a fine. The Disciplinary Tribunal is empowered to cancel or suspend the licence (sections 72, 73, 75, 89 and 93 of the REA Act). However, the above sanctions do not apply to management and beneficial owners of corporate real estate agents.

e. TCSPs and DPMSs: There are no other sanctions available to deal with failure to comply with AML/CFT requirements other than DIA's powers under the AML/CFT Act.

Criterion 28.5 - DNFBP sectors in New Zealand were introduced into the AML/CFT regime under a staged approach (casinos and TCSPs on 1 June 2013, law firms and conveyancers on 1 July 2018; accounting practises on 1 October 2018; real estate agents on 1 January 2019; and HVDs on 1 August 2019). While DIA updated the SRA for DNFBP sectors in December 2019, it is still in the process of putting a comprehensive supervisory framework in place for AML/CFT supervision of DNFBP sectors due to the lack of robust data. By the end of 2019, most DNFBPs only submitted or yet to submit their first annual reporting to DIA. Except for TCSPs and casinos, the AML/CFT supervisory engagements of DNFBPs were predominantly education focused.

Weighting and Conclusion

There are no entry controls for accounting practices who are not CAANZ members, TCSP and DPMS sectors. Fit and proper testing does not extend to the management and beneficial owners of corporate real estate agents. Risk-based AML/CFT supervision is not established in most of DNFBP sectors and no agency has a mandate for supervision of FIs for implementation of TFS obligations. There are scope issues with the definition of TCSPs and DPMS.

Recommendation 28 is rated Partially Compliant.

Recommendation 29 - Financial intelligence units

In the last MER, New Zealand was rated largely compliant. Deficiencies included: no legal provision that authorised the FIU to obtain additional information from reporting parties when needed to properly undertake its functions. Effectiveness issues were considered as part of the previous assessment but under the 4th round are no longer included in this technical compliance assessment, but are assessed separately under IO.6.

Criterion 29.1 - The NZ Police Financial Intelligence Unit (the FIU) was established within the New Zealand Police in 1996 and comes under the authority of the Police

Commissioner. The AML/CFT Act gives financial intelligence functions to the Police Commissioner of New Zealand Police.

The financial intelligence functions of the Commissioner include receiving and analysing SARs, prescribed transactions reports, cash transactions reports, suspicious property reports and, if necessary, referring them to law enforcement agencies and AML/CFT supervisors; producing risk assessments relating to money laundering offences and the financing of terrorism to be used by the Ministry, the MOJ, AML/CFT supervisors, and the New Zealand Customs Service; providing guidance to reporting entities, etc.

In accordance with the AML/CFT Act, the Commissioner may share suspicious activity reports, prescribed transaction reports, cash reports, suspicious property reports, and other financial information and intelligence with regulators and domestic and international authorities for the AML/CFT purposes.

Criterion 29.2

(a) The FIU is the central agency for receipt of SARs which includes suspicious transaction reports.

(b) The FIU is also the central agency for receipt of prescribed transaction reports, being reports of international wire transfers of NZD1 000 or more and domestic physical cash transactions of NZD 10 000 or more, from 1 Nov 2017; cash reports being cross border cash reports of NZD 10 000 or more; suspicious property reports (suspicious property reports under the TSA are those where a FI or person suspects on reasonable grounds that is, or may be, in the possession or control of a designated terrorist entity, whether directly or indirectly).

Criterion 29.3

(a) Under the AML/CFT Act, the Police Commissioner may order production of or access to all records, documents or information from any reporting entity which is relevant to analysing information received under the Act, with or without a court order even where no original SAR filed to the FIU.

(b) In accordance with the AML/CFT Act, the Police Commissioner has access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information required to properly undertake his or her financial intelligence functions, including analysis.

Information Privacy Principle 11 in the Privacy Act 1993, allows any agency (both public and private) to disclose information to the FIU for the purposes of the detection and investigation of offences. This principle allows FIs to provide further information to the FIU in order for it to carry out analysis of STRs.

Criterion 29.4

(a) In accordance with the AML/CFT Act, the FIU analyses suspicious activity reports, cash reports, suspicious property reports and prescribed transaction reports to assess whether any should be referred to appropriate LEAs. The Targeting Team under the FIU undertakes operational analysis on request of the appropriate police agency and on reports identified as high risk through the Proactive Financial Targeting process.

(b) The FIU's functions under the AML/CFT Act include producing typologies of ML and TF transactions as well as risk assessments relating to money laundering offences

and the financing of terrorism to be used by the Police, the Ministry of Justice, AML/CFT supervisors, and the Customs Service. The Strategic Team under the FIU includes a data analyst. The FIU conducts strategic analysis including the National Risk Assessment (NRA). The NRA is designed to describe the scale and nature of the risks faced in the New Zealand context for money laundering and terrorism financing. The NRA uses a model based on international guidance, where risk is a function of threats, vulnerabilities and consequences.

Criterion 29.5 - The Commissioner of Police is authorised under the AML/CFT Act, to share suspicious activity reports, prescribed transaction reports, cash reports, suspicious property reports, and other financial information and intelligence with regulators and domestic and international authorities for the AML/CFT purposes.

Egmont Secure Web is used for international disseminations. With FIUs outside of Egmont Group other channels are used (for example via Police Liaison Officers).

Criterion 29.6

(a) The FIU follows the Protective Security guidelines, which outline storage, dissemination, and handling requirements for all classified material. New Zealand Police and the FIU is subject to the NZ Protective Security Guidelines which prescribes the conditions for maintaining, communicating, and storing information at different levels of classification. The FIU, under the Official Information Act will only release high level information such as general statistics but never to the point where an individual report or reporting entity could be identifiable. Disclosure of individual reports or SARs, STRs, PTRs would be a breach the requirement in the AML/CFT Act that reports are only disclosed for law enforcement purposes.

(b) All permanent staff within the FIU undergo Police vetting and background checks prior to employment and criminal convictions of police employees are taken into account in the employment process. FIU staff who are likely to be dealing with terrorism financing related material go through the security clearance process to receive a Top Secret clearance. The security clearance process is undertaken by the NZ Security Intelligence Service.

All FIU staff are bound by the Police Code of Conduct which includes a section relating to the confidentiality of information.

(c) According to information provided by New Zealand, the FIU itself is located within the Police National Headquarters Building in Wellington. Swipe cards and identification cards are required to gain access to the building as well as the FIU. Physical files held at the FIU are secured in accordance with the Protective Security guidelines, which outline storage, dissemination, and handling requirements for all classified material.

Criterion 29.7 - In relation to operational independence and autonomy:

(a) The FIU was established within the NZ Police in 1996 and comes under the authority of the Police Commissioner. The Police Commissioner has delegated authority for the decision-making in relation to the dissemination of financial intelligence to the Manager of the FIU. The FIU is part the Financial Crime Group (FCG) within the Police and within this structure the Head of the FIU reports to one of the senior managers in the National Manager: Financial Crime Group. On 18 June 2009, the Commissioner of Police signed a formal Acknowledgement and Delegation clarifying the legal basis of the FIU. This document formally delegated to the Head of FIU (or any member of the FIU who may relieve the Head of FIU during his absence)

the power, function and duty of the Commissioner regarding the core activities of the FIU established under the FTRA and the TSA.

The FIU has authority to analyse, request and disseminate financial intelligence (section 142 AML/CFT Act).

(b) The FIU is able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information. MoUs are signed by the Head of FIU or by any other person delegated to by the Commissioner.

(c) The FIU's core functions are out in Section 142 of the AML/CFT Act. These powers are distinct from those of other parts of New Zealand Police.

(d) The FIU is able to obtain and deploy the resources needed to carry out its functions. The FIU has its own budget that is managed by the National Manager of the Financial Crime Group. The FIU has demonstrated that it has adequate funding, and the head of the FIU deploys resources where they see appropriate. The recruitment process is managed within the FIU, with support from Police Human Resource services. Section 16 of the *Policing Act 2008* outlines that the Commissioner of Police must act independently of any Minister of Government regarding enforcement of law and decisions about employees.

Criterion 29.8 - The FIU is member of the Egmont Group. The FIU is also an active member of the Outreach Working Group of Egmont. In 2008, the New Zealand Police reconfirmed its commitment to the group by signing the Egmont Charter.

Weighting and Conclusion

Recommendation 29 is rated Compliant

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

While New Zealand was rated compliant on Recommendation 27 in 2019, Recommendation 30 contains much more detailed requirements than the former Recommendation 27.

Criterion 30.1 - New Zealand Police is the primary law enforcement agency for ML/TF investigations. There are also special ML Teams and special groups within Police who can investigate ML and TF offences. The National Security and CT Group within Police is responsible for TF investigations. Other law enforcement agencies also have responsibility for AML/CFT investigations such as the Serious Fraud Office for serious and complex fraud investigations.

Criterion 30.2 - The New Zealand Police can pursue ML/TF offences. SFO, Customs and IR can pursue related ML offences under that arise from their investigations. If the ML constitutes a breach of a casino licence or the minimum operating standards under which it must operate then, as illegal gambling, it can be investigated and prosecuted by DIA. Beyond this, DIA Gambling Regulators can also refer ML offences uncovered to the NZ Police.

Criterion 30.3 - The CPRA provides the legal framework for the freezing and confiscation of proceeds of crime and the Police is empowered under the Act.

The four Asset Recovery Units (ARUs) are delegated by the Commissioner of Police to conduct restraint and confiscation of proceeds of crime under the CPRA. ARUs are

attached to Police investigations and operations as well as those of other agencies such as Customs, IR, SFO. Where appropriate the ARU's involvement may commence as early as the pre-investigation stage. The Official Assignee has the role of managing the frozen assets until the final decision on their confiscation is taken.

Criterion 30.4 - Inland Revenue (IR) pursues financial investigations and parallel money laundering investigations related to tax crimes. IR has investigative powers under the Tax Administration Act 1994 (TAA) and the Search and Surveillance Act, which provide powers to access property or relevant or necessary documents. It can commence money laundering proceedings under the *Criminal Procedure Act 2011*.

Customs can also pursue financial investigations and parallel money laundering investigations as well as TF offences for under Customs Act read with the AML/CFT Act or the TSA. The DIA can also pursue financial investigations and parallel money laundering investigations for offences related to the gambling sector respectively.

Criterion 30.5 - Serious Fraud Office (SFO) is the lead agency for anti-corruption but the New Zealand Police also undertake corruption investigations. Under the *Serious Fraud Office Act 1990* (SFO Act), the SFO is able to investigate any form of serious or complex fraud, which can include money laundering offences, whether relating to corruption or otherwise. However, in practice, the New Zealand Police undertakes ML investigations relating to corruption.

The SFO does not have a specific mandate to track and trace proceeds of crime but will typically use its investigative powers of compulsion under the SFO Act. The Director of the SFO is then able to share this information and appropriate material with the ARU on the basis that it has a proper interest in this information.

Weighting and Conclusion

Recommendation 30 is rated Compliant.

Recommendation 31 – Powers of law enforcement and investigative authorities

In its 3rd round MER, New Zealand was rated compliant for former Recommendation 28. Recommendation 31 contains much more detailed requirements than the former Recommendation 28.

Criterion 31.1

(a) Production of records held by FIs, DNFBPs and other natural or legal persons

The New Zealand Police has powers to compel production of records from FIs, DNFPBs or any natural and legal persons under the Search and Surveillance Act. The SFO has powers under the SFO Act for the production of documents relevant to its investigation. Other investigative agencies have more limited powers under the Act. For instance, Customs have powers to compel production under the Customs and Excise Act and Search and Surveillance Act to obtain access to the necessary documents and information for investigations within their ambit. IR has investigative powers under the Tax Administration Act 1994 and the Search and Surveillance Act, which provide powers to access property or relevant or necessary documents.

(b) Search of Persons and Premises

The Search and Surveillance Act provides broad powers to the NZ Police to search persons and premises for ML, TF and associated predicate offences. The Customs and

Excise Act, the Tax Administration Act and the Gambling Act 2003 also provide the respective competent authorities powers to search persons and premises which can be invoked for ML, TF and associated predicate offences that come under their purview. A search warrant under the SFO Act can also be obtained to assist with investigations by the SFO.

(c) Taking Witness Statements

NZ Police can record voluntary witness statements. Also, an examination order under the Search and Surveillance Act is an investigative tool available in respect of suspected ML, TF and predicate offences to compel individuals to provide information. IR, SFO and Customs can compel witnesses to provide information in relation to their investigations (including suspected ML, TF and predicate offences under their purview) under Tax Administration Act, SFO Act, Customs and Excise Act respectively.

(d) Seizing and Obtaining Evidence

Powers of seizure are part and parcel of search powers under subpart 4 of Part 4 of the Search and Surveillance Act. In addition, production orders for specific documents may be obtained by the Police under the Search and Surveillance Act read with the AML/CFT Act for money laundering investigations. The other competent authorities such as IR, Customs and SFO have power to make seizures and obtain evidence under Tax Administration Act, Customs and Excise Act and SFO Act respectively.

Criterion 31.2

(a) Undercover Operations

Police may undertake undercover operations in accordance with the general law in respect of all offences and evidence from undercover police officers is admissible in accordance with the *Evidence Act 2006*. Customs also can undertake undercover operations.

(b) Intercepting Communications

Interception of communication through the use of an interception device requires a surveillance device warrant. Surveillance that involves an interception device or visual trespass surveillance is available to competent authorities conducting investigations only in relation to certain specific offences as well as offences punishable by minimum of 7 years or against certain sections of the Arms Act 1983 and Psychoactive Substances Act 2013. This covers ML, TF and most associated predicate offences.

Where a warrant to intercept cannot be obtained due to the threshold requirements, text messaging may be retrieved through a search warrant or production order.

(c) Accessing computer systems

Authority to access a computer system or data storage device may be authorised by way of a search warrant. Police and various agencies are entitled to apply for search warrants (see comment in respect of 31.1 (b) above). A search warrant that covers access to a computer system or data storage device is available in respect of the same suspected offences as other search warrants (Again, see the comment in respect of 31.1(b). A remote access search may be allowed to access to electronic information that is for all practical purposes unable to be physically searched (e.g. where the

information is held across numerous servers in different locations or the server on which it is hosted is constantly changing and so cannot be identified).

(d) Controlled Delivery

There is no legal impediment for competent authorities including Police and Customs to conduct controlled delivery. Section 244 of the Crimes Act is available as a general defence for the enforcement or intended enforcement under the AML/CFT Act. However, whether this would apply to Customs use of cash outside the Customs Controlled Area for controlled delivery remains untested.

Criterion 31.3

(a) FIU has powers for production of account information on accounts from Reporting Entities including beneficial ownership information. The Commissioner of Police can order the production of account information from any reporting entity under the AML/CFT Act for the purpose of analysing information. The New Zealand Bankers' Association has agreement with Police to provide information for the purpose of confirmation of the existence of a banking relationship generally within 48 hours. If the matter is urgent this information can be obtained immediately.

(b) Search warrants and production orders are issued ex-parte and the CPRA prohibits the disclosure of the existence or the operation of a search order except under the circumstances listed in the statute.

Criterion 31.4 - The FIU has a legal function to share information to LEAs and under the AML/CT Act, the Police Commissioner can share financial information and intelligence with domestic authorities.

Weighting and Conclusion

Law enforcement and investigative authorities generally have all the powers that they need to investigate ML/TF. It remains untested whether controlled delivery of cash can be conducted by Customs outside the Customs Controlled Area. This is considered minor.

Recommendation 31 is rated Largely Compliant.

Recommendation 32 – Cash Couriers

In its 3rd round MER, SRIX was rated partially compliant, noting several shortcomings.

Criterion 32.1 - New Zealand operates a declaration system for currency (cash and BNIs) being carried into or out of the country. Under section 68 of the AML/CFT Act, any person carrying NZD 10 000 or more (or foreign equivalent) in cash or BNIs must complete a 'border cash report' on arrival or departure and present that form to a Customs officer.

The AML/CFT Act provides that the system applies to all movements whether the person brings, takes or sends the cash or BNIs into or out of New Zealand.

For the purposes of the AML/CFT Act, 'cash' means physical currency and BNIs which consists of a bill of exchange, cheque, promissory note, bearer bond, travellers cheque, a money order, postal order or similar order or any other instrument prescribed by regulations (none are currently prescribed). The definition of BNIs under the AML/CFT Act covers the FATF definition and permits prescription of other types of instruments in regulations (there are none currently prescribed).

The declaration process also applies to unaccompanied cash crossing New Zealand's border. The person sending the unaccompanied cash must complete the border cash report to accompany the cash or BNIs.

Criterion 32.2 - For all arrivals into New Zealand, there is an obligation to report if the traveller is entering with NZD10 000 or more. The requirement to do so via a prescribed declaration that each traveller must sign and submit to a Customs officer, is contained on the arrival card completed by all arriving persons. In relation to departures, passengers are advised to fill in border cash report if they have NZD10 000 or more to declare. The advice is communicated through signs around the check-in and departure areas (and also in arrival areas).

Criterion 32.3 - New Zealand has implemented a declaration system for currency being carried into or out of the country. Nevertheless, both arriving and departing passengers may be questioned by a Customs Officer and are required to disclose information truthfully. It is an offence under the Customs and Excise Act 2018 for failure or refusal to answer or to give an incorrect answer.

Criterion 32.4 - In practice, the discovery of any undeclared or mis-declared cash would result in the carrier being interviewed further by Customs officers. The Customs and Excise Act as well as the AML/CFT Act provide Customs officers general powers of questioning which oblige the suspect to answer questions. Customs officers can compel a person to provide further information on the cash or BNIs including their origin and purpose.

Criterion 32.5 - Cash that is imported or exported and that is not declared is a prohibited good in accordance with the Customs and Excise Act 2018 (read with AML/CFT Act). This, as well as cash in relation to erroneous declarations, can be automatically forfeited.

Under the AML/CFT Act, where an offence is committed for false or non-declaration of cash, in lieu of prosecution this can be dealt summarily by the chief executive of the Customs Service with a sum not exceeding NZD 500. In 2019, compositions imposed ranged from NZD 150 to NZD 500. Most commonly, the offence was summarily dealt with at NZD 400, consistent with the message on Customs' website at the time of the onsite.

However, if prosecuted, the liability under the AML/CFT Act is a term of imprisonment of not more than 3 months and or a fine up to NZD 10 000. For a body corporate or partnership the fine is up to NZD 50 000.

The criminal sanction is appropriate and dissuasive. However, the administrative penalty imposed for false or non-declaration of cash through summary disposal is 20 times less than the minimum cash threshold required for reporting. Also, there is no information to show that the punishment imposed is commensurate with the amount of the cash involved or for repeat offenders. Therefore, these sanctions for false declaration are not proportionate and dissuasive.

Criterion 32.6 - Provisions under the AML/CFT Act allow Customs to share information and transmit border cash reports to the FIU at NZ Police. Customs and New Zealand Police have a Memorandum of Understanding dealing with information exchange and data access between these agencies. All border cash reports are forwarded by Customs to the FIU for collation and analysis. The FIU can request additional information on incidents or border cash reports from Customs if they require it. Customs intelligence analysts who evaluate reports from frontline Customs

officers may also proactively advise the FIU of any incident of interest involving border cash reporting or cash/liquid asset movements by way of a Tactical Intelligence Report. As appropriate, local and specialist police units may also be advised.

Criterion 32.7 - Customs works closely with Immigration officials, New Zealand International Aviation Security staff, Ministry of Primary Industry (Biosecurity) officials, Police officials, and Maritime New Zealand officials. New Zealand has established a Border Sector Governance Group and a National Targeting Centre to improve inter-agency co-ordination and co-operation among Government agencies operating at ports of entry. The MOU between Customs and Police records the agreement of both agencies to work together and share intelligence and information on areas of common interest, particularly drug importation offending and organised/trans-national crime.

The Integrated Targeting and Operations Centre has officials from Customs, Ministry for Primary Industries, Maritime New Zealand and Immigration. This body works towards operational collaboration amongst agencies at the border. It provides risk targeting across goods, craft, and persons using risk assessment methodologies and drawing on relevant information from across agencies to refine targeting.

Criterion 32.8 - The Customs and Excise Act 2018 allows the detention of goods suspected to be an instrument of crime or are tainted property, which includes cash that is imported or exported and that is not declared in accordance with the Customs and Excise Act 2018. Under the CPRA, tainted property makes further reference to "significant criminal activity" which consists of offence/s punishable by a term of imprisonment of 5 years or more or from which the proceeds/benefits of a value of NZD 30 000 or more have been acquired or derived which covers ML/TF offences. The restraint is initially for 7 days but may be extended by a reasonable period not exceeding 14 days (21 days in total) on application to the courts.

Criterion 32.9 - Customs uses a range of international co-operative arrangements with other customs administrations abroad, particularly with its key trade and regional partners. The arrangements cover provisions relating to the exchange of information on matters of money laundering and cross-border movement of cash and other liquid valuables. To facilitate such co-operation:

(a) All interactions with persons involving border cash reports are recorded in the Customs Intelligence system in the form of an Activity Report or Information Report. The FIU receives and retains the original copies of all border cash reports made.

(b) In situations where there is a false declaration or there is a suspicion of money laundering, full details of that interaction would be recorded electronically on Customs Intelligence indices. The FIU and/or other Police units would be advised of the incident.

Criterion 32.10 - All border cash report data is supplied to the FIU. A record of the transaction is maintained by Customs. Both agencies have security to protect their physical and electronic information and to prevent inadvertent or unauthorised dissemination. There are internal procedures and policies that are in place to protect all information applies to Customs' records of cash and BNIs detected as well. All Government organisations including Customs and FIU are required to adopt the New Zealand Cabinet mandated Protective Security Requirements and the New Zealand Information Security Manual. These establish strict requirements for security governance, personnel security, information security, and physical security. They also

contain best practice guidance, but also acknowledge differences within organisations and allow for flexible implementation. This applies to the data and information collected through NZ's declaration system as well.

The declaration system does not unreasonably restrict legitimate travel and trade.

Criterion 32.11 - If the person carrying out a physical cross-border transportation of currency or BNI is found to be related to ML/TF activity or activity related to predicate offences, then the sanctions in relation to the ML/TF activity will apply (R3.9 and R5.6). In relation to the confiscation of currency or BNIs, in addition to the measures available for detention and confiscation in the event of false or non-declaration, the legislative measures under the CPRA, Sentencing Act 2002 and the TSA will apply (R4.1).

Weighting and Conclusion

The summary disposal penalty for failing to make a declaration/disclosure or making a false declaration/disclosure is not sufficiently proportionate and dissuasive.

Recommendation 32 is rated largely compliant.

Recommendation 33 – Statistics

In its 3rd MER, New Zealand was rated largely compliant with these requirements, as it did not keep sufficient statistics on international requests for assistance in relation to the NZPFIU and SFO. Since then, the FATF requirements have changed.

Criterion 33.1 - New Zealand keeps statistics on matters relevant to the effectiveness and efficiency of its AML/CFT system, however not all statistics are sufficiently maintained as follows:

(a) The FIU keeps statistics on STRs and SARs received from reporting entities, which can be broken down by sector. The FIU also keeps statistics on disseminations of STRs and SARs. Including disseminations to other agencies, international partners and Egmont-related dissemination.

(b) New Zealand has statistics on ML/TF investigations, prosecutions, and convictions, however these are not sufficiently maintained in a comprehensive manner to enable New Zealand to monitor the effectiveness and efficiency of its AML/CFT regime. New Zealand Police has statistics on the overall number of ML/TF investigations, prosecutions, and convictions with respect to cases investigated by them. Prosecution and conviction statistics are also held by the MOJ. Customs and IR do not maintain separate statistics on ML investigations conducted by them.

(c) The Official Assignee maintains statistics on the majority of cases of freezing, seizures and confiscation, but not in all cases. The MOJ also maintains statistics on property confiscated by way of court order.

(d) CLO and the New Zealand Police records requests received and made by New Zealand for MLA and extradition. However, MLA statistics are not sufficiently maintained in a comprehensive manner to enable New Zealand to monitor the effectiveness and efficiency of its AML/CFT regime in a timely manner and cannot be broken down by offence type. There are also mechanisms for maintaining information pertaining to international requests through the New Zealand office of INTERPOL as well as international requests made and received in relation to other LEAs.

Weighting and Conclusion

New Zealand does not maintain sufficiently comprehensive statistics on MLA, ML investigations and prosecutions and on all property frozen, seized and confiscated.

Recommendation 33 is rated Largely Compliant.

Recommendation 34 – Guidance and feedback

In its 3rd MER, New Zealand was rated largely compliant with these requirements. The deficiency related to insufficient guidance provided to DNFBPs concerning how, in practice to identify legal persons/arrangements, beneficial owners and PEPs. Since then, the FATF requirements have changed and the number of sectors subject to AML/CFT supervision in New Zealand has substantially increased.

Criterion 34.1 - *Supervisors' guidance and feedback to FIs and DNFBPs*: RBNZ, FMA and DIA provide a wide range of guidance to the reporting entities they supervise to assist them in complying with their AML/CFT obligations, including joint guidelines, code of practice, sector-specific guidelines, factsheets, frequently asked questions, training videos and webinars. The guidance covers different AML/CFT areas, e.g. risk assessments, CDD, EDD, beneficial ownership, wire transfers and country assessments. They also conduct outreach sessions for their reporting entities. The supervisors provide feedback (e.g. findings and observations from on-site and off-site reviews) through regular reports to reporting entities (e.g. RBNZ's AML/CFT Update, FMA's AML/CFT Monitoring Report and DIA's Regulatory Findings). Due to the nascent AML/CFT regimes for the new DNFBP sectors, DIA conducted extensive training and outreach for these sectors, including the provision of sector-specific guidelines. Inevitably, less resources were put on feedback to the FIs and DNFBPs that were already under DIA's supervision. For example, no similar sector-specific guidelines were provided for TCSPs and casinos, which are assessed as high-risk and medium-high risk respectively by DIA.

FIU's guidance and feedback: The FIU publishes a SAR Guideline and provides training to reporting entities where they are taught how to submit SARs and understand what suspicious activity is. The FIU publishes quarterly statistics and guidance and advisories related to SARs, including FATF statements and advisories. It ceased however to publish quarterly typology reports in 2017, instead providing typologies through its reporting system to registered reporting entities. The FIU provides feedback to individual reporting entities on filing of SARs on a case-by-case basis.

Weighting and Conclusion

There are minor shortcomings with respect to the guidance and feedback provided by DIA and the FIU. There is a lack of sector-specific guidelines for TCSPs and casinos, which are assessed as high-risk and medium-high risk respectively by DIA.

Recommendation 34 is rated Largely Compliant.

Recommendation 35 – Sanctions

In its 3rd MER, New Zealand was rated partially compliant with these requirements due to the lack of effective, proportionate and dissuasive civil or administrative sanctions for FIs that breach AML/CFT requirements, and designated authorities to impose civil and administrative sanctions for breaches of AML/CFT requirements, except for registered banks. Since then, New Zealand has made legislative amendments to bring all FIs and DNFBPs under AML/CFT regulatory regime and empower relevant supervisors with powers to sanction non-compliance.

Criterion 35.1 - A range of proportionate and dissuasive criminal, civil and administrative sanctions are available as follows:

a) *Sanctions for targeted financial sanctions (R6):* Any natural or legal person who contravenes the provisions related to TFS under sections 8 to 10 of the TSA commits an offence and is liable on conviction to criminal sanctions. A person who commits financing of terrorism (section 8) is liable to a maximum of 14 years' imprisonment. A person who deals with property of, or derived or generated from property of, designated terrorist entity (section 9) or makes property, or financial or related services, available to designated terrorist entity (section 10) is liable to a maximum of 7 years' imprisonment.

b) *Sanctions for NPOs (R8*): DIA is empowered to impose a range of sanctions for non-compliance with the requirements in R8. These powers include deregistration; issuance of warning notice; publication of wrongdoing or breaches; and prosecution (sections 31, 54, 55 and 74 of the Charities Act). Overseas donee organisations may lose this status in response to wrongdoing. However, there are no relevant powers to impose sanctions in relation to other moderate-risk NPOs (see R8).

c) *Sanctions for preventive measures and reporting (R9-23)*: The supervisors (RBNZ, FMA and DIA) are authorised to impose a range of civil sanctions, including the ability to issue a formal warning; accept an enforceable undertaking and seek an order for breach of that undertaking; seek an injunction from the High Court; and apply to the court for a pecuniary penalty, if a reporting entity fails to comply with AML/CFT requirements[48] (subparts 1 and 2, Part 3 of AML/CFT Act). Two-tiered pecuniary penalties depend on which provision the reporting entity fails to comply with (e.g. non-compliance with CDD and record keeping requirement can be subject to higher fines: maximum NZD 200 000 for individual or NZD 2 million for body corporate). However, the range of sanctions available could be strengthened, as supervisors lack the power to apply administrative pecuniary penalties. In addition, engaging in such non-compliance conduct knowingly or recklessly; failure to report suspicious activity; and unlawful disclosure of SARs, are criminal offences. Criminal penalties are imprisonment for up to 2 years and/or a fine up to NZD 300 000 for individual and a fine up to NZD 5 million for a body corporate or partnership. However, such criminal sanctions do not apply to the employees of FIs and DNFBPs (see R35.2).

Other than sanctions under AML/CFT Act, RBNZ and FMA can withdraw, restrict or suspend the licenses of respective supervising FIs if there are is breach of licensing

48 Civil sanctions do not apply to failure to report suspicious activity, which is a criminal offence (section 92 of AML/CFT Act).

conditions or any prudential concerns on these FIs. It is unclear as to whether a breach of AML/CFT obligation will lead to withdrawal, restriction or suspension of the licenses given the absence of specific legislative empowerment and case examples. There are also minor shortcomings with respect to New Zealand's ability to withdraw, restrict or suspend a FI's license or registration for failure to comply with AML/CFT requirements (see R27.4).

For DNFBPs, DIA can make referrals for lawyers to the NZLS; conveyancers to the NZSC; chartered accountants to CAANZ; and real estate agents to the REA. Breaches of AML/CFT requirements may bring disciplinary actions or penalties, including withdrawal, restriction or suspension of relevant licenses. The lack of entry controls for accounting practices who are not CAANZ members, TCSP and DPMS sectors; and fit and proper test for the management and beneficial owners of corporate real estate agents, limit New Zealand's abilities to impose licensing sanctions on these reporting entities (see R28.4).

Criterion 35. - Civil sanctions set out in the AML/CFT Act can only apply to FIs and DNFBPs that are reporting entities, but not their directors and senior management (subparts 1, 2 and 3 of Part 3 of the AML/CFT Act). Criminal sanctions can however apply to directors and senior management of reporting entities (*R v QF, FC and JFL* [2019] NZHC 3058). Licensing authorities can also remove directors and senior management if they are found to contravene the fit and proper requirements (sections 113, 113A and 113B of the RBNZ Act; sections 143 and 144 of the IPS Act; section 56 of the NBDT Act; sections 383 or 385 of the Companies Act; section 517 of the FMC Act). However, for those FI and DNFBP sectors that are not subject to licensing or entry controls (see R27 and R28), no sanctions can be applied to their directors and senior management.

Weighting and Conclusion

No sanctions are available for moderate-risk NPOs. There is also a shortcoming in relation to sanctions applicable to FI and DNFBP sectors that are not subject to licensing or entry controls and the range of sanctions available to the supervisors could be strengthened. Civil sanctions available for breaches of AML/CFT requirements generally do not apply to directors and senior management of FIs and DNFBPs.

Recommendation 35 is rated Largely Compliant.

Recommendation 36 – International instruments

In its 3rd MER, New Zealand was rated largely compliant with these requirements. The deficiencies identified included (i) the purposive elements in *Proceeds of Crime Act 1991* (since repealed) requiring to prove third party ML were not in line with the Vienna and Palermo Conventions; and (ii) the lack of requirements to identify beneficial owners was not fully in line with the TF Convention.

Criterion 36.1 - New Zealand has ratified Vienna Convention (on 16 December 1988), Palermo Convention (on 19 July 2002), TF Convention (on 4 November 2002), and the Merida Convention (on 1 December 2015).

Criterion 36.2 - New Zealand has implemented the relevant articles of the Vienna, Palermo and TF Conventions. The deficiencies identified in preventive measures, e.g. wire transfer requirements in R16, indicate that the Merida Convention is not implemented fully.

Weighting and Conclusion

There are minor technical gaps in the implementation of the Merida Convention.

Recommendation 36 is rated Largely Compliant.

Recommendation 37 – Mutual legal assistance

In its 3rd MER, New Zealand was rated largely compliant with these requirements because the threshold condition for a range of coercive measures was unduly restrictive and might prevent New Zealand from responding to MLA requests from countries who do not meet the high threshold penalty for the underlying offence. Since then, New Zealand has made legislative amendments to lower the threshold.

Criterion 37.1

New Zealand has a sound legal framework for rapid provision of a wide range of MLA under MACMA, bilateral MLA agreements and multilateral conventions. MACMA provides an extensive framework for international assistance in criminal matters by allowing requests from and to New Zealand with any country. MACMA allows for requests to be made by prescribed foreign countries (currently 8 jurisdictions have been declared by regulations), convention countries (i.e. countries which are party to conventions listed in the Schedule to MACMA), and all other countries on an ad-hoc basis subject to conditions set out in section 25A of MACMA (e.g. on the basis of reciprocity).

Criterion 37.2 - MACMA designates the Attorney-General as the central authority for MLA in New Zealand and the Attorney-General's powers under MACMA are largely delegated to the Solicitor-General. The Office of the Solicitor-General, i.e. the CLO, therefore undertakes the legal work required for transmission and execution of requests. CLO has mechanisms in place to ensure the prioritisation and timely response to requests, although these mechanisms are informal. Incoming MLA requests are triaged based on urgency. The progress and timeliness of requests are monitored by regular internal meetings. CLO uses a spreadsheet for keeping records of all MLA requests rather than having a case management system for monitoring progress on requests.

Criterion 37.3 - Section 27(1) of MACMA sets out the mandatory grounds of refusal, which includes cases of a political character; prejudice based on colour, race, ethnic origin, sex, religion, nationality or political opinions; double jeopardy; military offences; and prejudice to New Zealand's sovereignty, security or national interests. Other possible grounds for denying a request (at the discretion of the Attorney-General) include absence of dual criminality (see R37.7); imposition of the death penalty; and prejudice to a criminal investigation or criminal proceedings in New Zealand (section 27(2)). The mandatory and discretionary grounds for refusal are reasonable and justified, and are not being interpreted or applied in an unreasonably restrictive way.

Criterion 37.4 - New Zealand does not impose a restriction on MLA on the sole ground that the offence is also considered to involve fiscal matters, and secrecy or confidentiality requirements are not grounds for refusing an MLA request.

Criterion 37.5 - MACMA does not have specific provision to safeguard the confidentiality of MLA requests they receive, and the information contained in them. The lack of specific provision in MACMA is partly mitigated by specific confidentiality

provisions in bilateral or multilateral agreements ratified by New Zealand, and some fundamental principles of domestic law, including the Privacy Act.

Criterion 37.6 and 37.7 - A country may request MLA from New Zealand either on the basis of a treaty or convention or as an "ad hoc request" made under section 25A of MACMA. For a request made on the basis of a treaty or convention, dual criminality principle applies, and the "criminal matter" that the request relates to must correspond to an offence listed in the Schedule to the MACMA if committed within the jurisdiction of New Zealand (section 24A). "Ad hoc requests" are considered by the Attorney-General on a discretionary basis taking into account the reciprocity aspect, the seriousness of the offence, the relevance as to the purpose of the MACMA and other matters they consider relevant (section 25A(2)). Dual criminality is a possible ground for refusal, but this is at the discretion of the Attorney-General (section 27(2)).

In providing MLA where dual criminality is required, New Zealand does not require that all the technical elements of the offence be identical to a corresponding offence from the requesting country. In relation to requests made on the basis of a treaty or convention, dual criminality and reciprocity follow from the fact that both New Zealand and the requesting country are parties to a convention that contains MLA obligations. The qualification of the offences must not necessarily be the same, but it should be among the offences listed in the Schedule. For an "ad hoc request" made under section 25A, the practice is that, as long as the requesting country certifies that the request relates to a criminal offence being investigated or prosecuted, New Zealand would not require that the elements of the offence be identical to a corresponding domestic offence.

Criterion 37.8

(a) MACMA provides powers to domestic competent authorities for production, search and seizure of information, document or evidence, including financial records, from FIs, or other natural or legal persons in order to respond to MLA requests (sections 31, 43 and 44). MACMA provides no specific powers in relation to the taking of witness statements, except for witness statements taken on a voluntary basis.

(b) MACMA does not empower the use of investigative techniques (e.g. undercover operations, intercepting communication, accessing computer systems and controlled delivery) in an international context for an MLA request. The investigative techniques available to competent authorities set out in R31.2 do not generally apply to MLA requests. Assistance not requiring coercive powers (e.g. voluntary interviews, providing evidence voluntarily via video link), however, may be provided under section 5 of MACMA.

Weighting and Conclusion

There are minor technical shortcomings in relation to the CLO's case management system, confidentiality provisions and the investigative techniques available in relation to MLA.

R**ecommendation 37 is rated Largely Compliant**.

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In its 3rd MER, New Zealand was rated largely compliant with these requirements because the threshold condition for a range of coercive measures was unduly restrictive and might prevent New Zealand from responding to MLA requests from countries who do not meet the high threshold penalty for the underlying offence. Since then, New Zealand has made legislative amendments to lower the threshold.

Criterion 38.1 - New Zealand can take expeditious action in response to requests by foreign countries to identify, freeze, seize or confiscate the proceeds of crime or laundered property acquired or derived from significant foreign criminal activity; or instruments used in or intended for use in a foreign qualifying forfeiture offence; or property of corresponding value (sections 54 and 55 of MACMA).

While most restraint or forfeiture requests can be registered in New Zealand with low thresholds (i.e. relating to significant foreign criminal activity), the threshold for restraint or forfeiture requests regarding an instrumentality of crime remains unduly restrictive as identified in the last MER.

Criterion 38.2 - Foreign restraining orders and foreign forfeiture orders registered in New Zealand have the same effect as restraining orders and forfeiture orders made under CPRA (section 57 of MACMA). CPRA establishes a civil-based asset confiscation regime (see R4.1). Under CPRA, assets can be confiscated regardless of criminal proceedings where it can be shown, on the balance of probabilities, that the assets were derived from criminal activity. No criminal proceedings are required for a civil forfeiture order. In registering a foreign forfeiture order, it does not need to be, or to have been, the subject of any criminal proceedings in New Zealand or a foreign country (section 15 of CPRA). Under CPRA and MACMA, a New Zealand court may enforce foreign country's restraining orders and forfeiture orders, so assistance to overseas LEAs in relation to non-conviction-based confiscation is available once the confiscation order has been submitted (sections 54 and 55 of MACMA; sections 124-127 of CPRA).

Criterion 38.3 - CLO does not have formal arrangements in place for co-ordinating seizure and confiscation actions with other countries although there is nothing in New Zealand's legislative framework that prevents such co-ordination. In practice, it has been done previously by liaising informally with the requesting state.

The Official Assignee is the designated asset management authority for all frozen, seized or confiscated property under foreign orders registered in the New Zealand Court. Similar to local restraining and forfeiture orders, the Official Assignee has the statutory responsibility, and necessary powers, to preserve and manage property subject to a foreign restraining order, and to administer property subject to a foreign forfeiture order until it is disposed of (see R4.4).

Criterion 38.4 - Asset sharing is possible in New Zealand and is governed by the provisions of any applicable treaty and the New Zealand Guidelines Relating to the Sharing of Confiscated Assets. The Guidelines have a presumption of returning 50% of the confiscated assets to the requesting country in the absence of any different pre-existing arrangement. The Guidelines allow the Attorney-General to exercise his or her discretion to return assets in a suitable case and set out factors taken into account when doing so.

Where a foreign forfeiture order is registered in New Zealand, the property recovered may be disposed of in accordance with section 86 of CPRA. This requires the Official

Assignee to dispose of property forfeited under a foreign forfeiture order and disburse the funds to the Attorney General after paying the costs recoverable under section 87 of CPRA.

New Zealand has MLA treaties with Korea, Hong Kong, China[49] and China, which specifically provide for the possibility of sharing assets by agreement. The New Zealand Guidelines on Asset Sharing provide guidance as to quantum in both contexts. Where there is no treaty, the assets may be shared at the discretion of the Attorney-General (section 86 of CPRA).

Weighting and Conclusion

A minor shortcoming in respect of the unduly restrictive threshold for restraint or forfeiture requests regarding an instrument of crime remains was identified.

Recommendation 38 is rated Largely Compliant.

Recommendation 39 – Extradition

In its 3rd MER, New Zealand was rated largely compliant with these requirements. The major deficiency was that extradition capacity for ML is restrained by limitations to one of the designated categories of predicate offences. The legal framework remains unchanged since the last MER.

Criterion 39.1 - New Zealand's legal framework for extradition is set out in the Extradition Act, which allows New Zealand to respond to extradition requests from certain treaty and Commonwealth countries (Part 3 of the Extradition Act), from Australia and designated countries (Part 4 of Extradition Act), and also from any other country on an ad hoc basis where no extradition treaty is in force. While the extradition procedures in place do not contain prescribed timelines for processing extradition requests, the statistical figures do not show any undue delay.

a) As ML and TF are both punishable in New Zealand by imprisonment for at least 12 months, they are extradition offences (section 4).

b) The Extradition Act does not designate any central authority but MFAT is New Zealand's contact point for all extradition inquiries, except for the requests under Part 4 which go through the New Zealand Police. Extradition requests received via MFAT are managed by CLO and are logged onto a spreadsheet similar to the one used for MLA requests (see R38). This system is used primarily for record-keeping. Counsels in the CLO are responsible for prioritising and monitoring the progress of requests.

c) The Extradition Act contains a number of mandatory and discretionary restrictions on surrender, including cases of a political character; prejudice based on race, ethnic origin, religion, nationality, sex, or other status, or political opinions; military offences; double jeopardy; and with special medical reasons (sections 7 and 8 of the Extradition Act). These restrictions do not appear unreasonable or restrictive.

Criterion 39.2 - New Zealand is able to extradite its own nationals pursuant to extradition requests. Whilst New Zealand retains the discretion not to extradite its nationals, the New Zealand practice is not to refuse extradition simply on the basis of

49 The MLA agreement between New Zealand and Hong Kong, China was suspended on 3 August 2020.

nationality. New Zealand has not refused an extradition request solely on the grounds of nationality for at least the last fifteen years.

Criterion 39.3 - Dual criminality is a requirement for extradition (sections 4(1)(a) and (2) of the Extradition Act). However, in assessing whether there is dual criminality, the totality of the conduct is to be taken into account and it does not matter whether, under the law of the extradition country and New Zealand, the acts or omissions are categorised or named differently; or the constituent elements of the offence differ (section 5(2)). The New Zealand courts have held, and the Extradition Act provides, that the focus in extradition should be on the offending itself and in particular its nature and quality, not the nomenclature of the offences or the constituent elements of the offences (*Cullinane v Government of the United States of America*, HC Hamilton, A116-00, 10 September 2001, *United States of America v Cullinane* [2003] 2 NZLR 1).

Criterion 39.4 - For certain treaty and Commonwealth countries, a formal extradition request to the Minister of Justice has to be made by a diplomatic or consular representative, or a Minister of the requesting country; or by other means prescribed in the relevant treaty (section 18 of the Extradition Act). For Australia and other designated countries, no formal request is required. In practice, a warrant for the arrest of a person issued in the requesting country is provided to a district court judge for endorsement through the Police (section 41). The extradition process can also be simplified when the person consents to be surrendered (sections 28 and 53).

Weighting and Conclusion

A minor shortcoming was identified in relation to the case management system used for managing extradition requests.

Recommendation 39 is rated as largely compliant.

Recommendation 40 – Other forms of international co-operation

In its 3rd MER, New Zealand was rated largely compliant with these requirements and the only shortcoming was the inability to assess effectiveness on how RBNZ exchanged information for AML/CFT purpose. These requirements were strengthened since the 3rd round MER and the assessment of effectiveness has been removed from the technical compliance assessment.

General principles

Criterion 40.1 - Competent authorities in New Zealand can provide a range of information in relation to ML, associated predicate offences and TF to their foreign counterpart authorities.

New Zealand Police is able to spontaneously and by request exchange information through international channels, such as INTERPOL (via the National Central Bureau under the International Services Group) and a network of liaison officers deployed to other jurisdictions. New Zealand Police has also entered into a number of bilateral and multilateral MOUs and memorandums of agreement (MOAs) to enable exchange of information with overseas LEAs.

The FIU is able to exchange financial information and intelligence with international authorities under section 143(1)(b) of AML/CFT Act. It primarily uses the Egmont Group's Egmont Secure Web and the New Zealand Police Liaison Office Network for regular communication and outreach. The FIU has also entered into several MOUs and

MOAs with foreign FIUs that are outside the Egmont network or where the partners require such arrangement.

Customs is able to disclose information to overseas enforcement agencies for assisting the authority to carry out its functions related to, or involving, the prevention, detection, investigation, prosecution, or punishment of offences (section 318 of Customs and Excise Act). It also uses a range of co-operative arrangements for the exchange of information on matters of common interest with other customs administrations, including bilateral MOUs with a number of key trade and regional partners.

IR is able to exchange information spontaneously and upon request under Double Taxation Agreements, Tax Information Exchange Agreements and the Multilateral Convention on Mutual Administrative Assistance in Tax Matters (section BH1 of Income Tax Act).

SFO is able to enter into an agreement (orally or in writing) with any person in any other country whose functions are or include the detection and investigation of cases of fraud or the prosecution of proceedings, which relate to fraud. The agreements provide for the supply or receipt of information on a particular case or cases of fraud by the SFO (section 51 of the SFO Act).

The three supervisors (RBNZ, FMA and DIA) all have the function of co-operating with international counterparts to ensure the consistent, effective, and efficient implementation of the AML/CFT Act and they have necessary powers to initiate and act on requests from any overseas counterparts (sections 131(e) and 132(2)(e) of the AML/CFT Act). RBNZ can exchange information with overseas regulatory authorities under section 105 of the RBNZ Act even in the absence of MOUs. RBNZ has signed a number of MOUs and established information conduits in form of regular meetings with overseas authorities. FMA is able to exchange information to overseas regulators in the manner that the FMA thinks fit under section 30 of FMA Act. It has also signed a number of bilateral and multilateral MOUs (e.g. the IOSCO Multilateral MOU) for cross-border information sharing. DIA has more limited informal channels for international co-operation, including contacts established by individuals; membership of established international forums; and networking opportunities at conferences and forums.

Criterion 40.2

a) Competent authorities in New Zealand have a lawful basis for providing co-operation (FIU: section 143(1)(b) of the AML/CFT Act; New Zealand Police: section 10 and 95A-95D of the Policing Act; SFO: section 51 of the SFO Act; Customs: section 318 of the Customs and Excise Act; RBNZ: section 131(e) and s.132(2)(e) of the AML/CFT Act and section 105 of the RBNZ Act; FMA: sections 131(e) and 132(2)(e) of the AML/CFT Act and section 31 of the FMA Act; DIA: sections 131(e) and 132(2)(e) of the AML/CFT Act).

b) Nothing prevents competent authorities from using the most efficient means to co-operate.

c) Competent authorities use clear and secure gateways to transmit information, such as Egmont Secure Web used by the FIU and INTERPOL's I-24/7 system used by New Zealand Police. Communications with non-Egmont countries may also be undertaken through Police Liaison Officers based at Embassies or High Commissions.

d) Most competent authorities, except FMA, do not have internal guidelines or written procedures that explicitly set out the prioritisation and timeliness for execution of requests. In practice, competent authorities prioritise requests on a case-by-case basis based on the time sensitivity and severity of the matter.

e) Competent authorities in New Zealand prioritise and execute requests from overseas counterparts on a case-by-case basis, and respond in accordance with the timeline agreed by the requesting authorities. Some authorities, for example Customs, have internal policies and procedures governing disclosure of information to overseas authorities including the response time.

f) All Government organisations in New Zealand must adopt New Zealand's Protective Security Requirements and Information Security Manual. These establish strict requirements for security governance, personnel security, information security, and physical security. These requirements can apply to information received through international co-operation. Additionally, competent authorities have internal policies and procedures to ensure information received is safeguarded, such as the internal Information Management Policies of FMA.

Criterion 40.3 - Competent authorities in New Zealand have negotiated and signed bilateral agreements with their respective overseas counterparts in a timely manner.

Criterion 40.4 - Competent authorities in New Zealand can provide feedback through direct response to overseas counterparts (e.g. email), regular liaison channels (e.g. bilateral meetings) or surveys conducted by international organisation (e.g. Global Forum on Transparency and Exchange of Information and IOSCO).

Criterion 40.5 - Competent authorities in New Zealand do not prohibit or place unreasonable or unduly restrictive conditions on the provision of information or assistance on the grounds under R40.5 as long as the request is within their scope of purview.

Criteria 40.6 - Competent authorities in New Zealand appear to have controls and safeguards to ensure that information exchanged is used only for the purpose for, and by the authorities for which the information was sought or provided. This is done through various means. For example, all Government organisations in New Zealand are required to adopt the New Zealand Protective Security Requirements and Information Security Manual (see R40.2). Competent authorities have internal policies and procedures to ensure information received is safeguarded and only used appropriately, such as the internal Information Management Policies of FMA. Bilateral and multilateral agreements signed by authorities contain confidentiality provisions and specify safeguards to protect the use of information exchanged. Laws such as the Privacy Act also provide for provision that stipulate as to when relevant information can be disclosed. However, the supervisors are not subject to any explicit provision to have prior authorisation or consent of the requesting competent authority to disclose information exchanged.

Criteria 40.7 - New Zealand has laws to protect the confidentiality of any request for co-operation and the information exchanged (in the RBNZ Act, FMA Act, TA Act and SFO Act). There are no explicit confidentiality provision in the AML/CFT Act. Besides, the various means mentioned in R40.6, internal policies and procedures of competent authorities, and confidentiality provisions in bilateral and multilateral agreements help protect the confidentiality of information exchanged.

Criterion 40.8 - There is no explicit provision in the AML/CFT Act which allows RBNZ, FMA and DIA to conduct enquiries on behalf of foreign counterparts (section 132(2)(e) of AML/CFT Act). FMA is able to conduct inquiries on behalf of foreign counterparts and provide information obtained from the FIs under its supervision to the foreign counterparts (sections 25(2), 30 and 31 of FMA Act). There are no similar provisions for RBNZ and DIA. LEAs can make enquiries on behalf of foreign counterparties and share related information (section 143 of AML/CFT Act; sections 252 and 318 of the Customs and Excise Act; section 51 of the SFO Act; sections 17 and 17B of the TA Act) and various bilateral and multilateral agreements.

Exchange of information between FIUs

Criterion 40.9 - The FIU has adequate legal powers under section 143 of the AML/CFT Act to exchange information with foreign FIUs.

Criterion 40.10 - The FIU can provide feedback to their foreign counterparts, upon request and whenever possible, on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided.

Criterion 40.11 -The FIU has the power to access, directly or indirectly, on a timely basis the financial, administrative and law enforcement information required to properly undertake its financial intelligence functions. The FIU can exchange these information to its foreign counterparts (sections 142(f) and 143 of AML/CFT Act).

Exchange of information between financial supervisors

Criterion 40.12 - RBNZ, FMA and DIA have the function of co-operating with international counterparts to ensure the consistent, effective, and efficient implementation of the AML/CFT Act, and they have necessary powers to initiate and act on requests from any overseas counterparts (sections 131(e) and 132(2)(e)). RBNZ and FMA have additional legal bases for providing co-operation, including the exchange of supervisory information with their foreign counterparts (section 105(2)(f) of the RBNZ Act and section 30 of the FMA Act).

Criterion 40.13 - RBNZ, FMA and DIA are able to obtain information domestically, including information held by their supervised reporting entities (section 132(2)(a) of AML/CFT Act). They have legal bases to exchange obtained information with foreign counterparts (see R40.12).

Criterion 40.14 - RBNZ, FMA and DIA are able to exchange information including (a) regulatory information; (b) prudential information; and (c) AML/CFT information (sections 132 and 137 of the AML/CFT Act). There is no provision to limit the scope of exchangeable information.

Criterion 40.15 - There is no explicit provision in the AML/CFT Act that allows RBNZ, FMA and DIA to conduct enquiries on behalf of foreign counterparts. However, section 132(2)(e) of the AML/CFT Act allows AML/CFT supervisors to initiate and act on requests from any overseas counterparts in accordance with the AML/CFT Act and any other enactment. RBNZ can authorise a home country supervisor to conduct its own inquiries in New Zealand to facilitate effective group supervision (section 98A of the RBNZ Act), but there is no explicit provision to conduct inquires on behalf of foreign counterparts. FMA is able to conduct inquiries on behalf of foreign counterparts and provide information obtained from the FIs under its supervision to the foreign counterparts (sections 25(2), 30 and 31 of the FMA Act), but FMA is not empowered to authorise or facilitate foreign counterparts to conduct their own inquiries in New Zealand.

Criterion 40.16 - While the RBNZ Act and FMA Act have provisions to protect confidentiality of information exchanged, there is no explicit provision for RBNZ and FMA to have prior authorisation or consent of the requested financial supervisors to disclose information exchanged. The lack of explicit provision is partly mitigated by provisions in bilateral or multilateral agreements signed by AML/CFT supervisors with their overseas counterparts.

Exchange of information between law enforcement authorities

Criterion 40.17 - LEAs are able to exchange domestically available information with foreign counterparts in the manner set out under R40.1.

Criterion 40.18 - As set out under R40.3 and R40.8, LEAs are able to conduct inquiries and obtain information on behalf of foreign counterparts.

Criterion 40.19 - LEAs are able to undertake joint investigations with foreign counterparts where the need arises.

Exchange of information between non-counterparts

Criterion 40.20 - New Zealand authorities can exchange information indirectly with non-counterparts. New Zealand Police are able to exchange information indirectly with non-counterparts which fulfil the same functions in their countries. The functions set out in section 9 of the Policing Act are broad. RBNZ, FMA and DIA can respond to requests from any overseas counterparts (section 132(2)(e) of the AML/CFT). Customs and SFO have powers to share information with overseas authorities which are not confined to their usual counterparts. Furthermore, information can also be exchanged with non-counterpart through FIU-FIU channels.

Weighting and Conclusion

Minor shortcomings in relation to the supervisors' abilities to conduct inquires on behalf of foreign counterparts and specific provisions to have prior authorisation or consent of the requested financial supervisors to disclose information exchanged were noted.

Recommendation 40 is rated Largely Compliant.

Summary of Technical Compliance – Key Deficiencies

Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	LC	• New Zealand's exemption process has meant not all exemptions have been granted where there is proven low risk of ML/TF in strictly limited or justified circumstances. • There is no explicit prohibition from carrying out simplified CDD where there is a suspicion of ML/TF. • There is no requirement that reporting entities' AML/CFT programmes are approved by senior management
2. National co-operation and co-ordination	C	• This Recommendation is fully met.
3. Money laundering offences	C	• This Recommendation is fully met.
4. Confiscation and provisional measures	C	• This Recommendation is fully met.
5. Terrorist financing offence	LC	• There is no specific offence for individuals who travel for the purposes related to terrorist acts or providing or receiving terrorist training. The general terrorism financing offences under the TSA does not appear to cover all circumstances set out in 5.2bis.
6. Targeted financial sanctions related to terrorism & TF	LC	• Facilitation of terrorist acts is not a standalone ground for implementation of TFS. • Freezing obligations under the TSA does not extend to all property of persons or entities acting on behalf of, or at the direction of, designated persons or entities. • The TSA does not expressly extend to prohibiting making assets available to entities owned or controlled by designated entities (except for UNSCR 1373 where such entities may be listed), nor to persons acting on behalf of designated persons or entities, where the making available of property is not for the benefit of the designated person or entity named in relevant sanctions lists. • Reporting entities that are not registered on goAML do not receive communications UNSCR 1373 designations from the FIU within one working day of the designation or change to a designation, nor communication relating to de-listing requests. • The de-listing procedure does not include information on applying to the UN Focal Point for Delisting (relevant to UNSC Resolution 1988 sanctions). • The Prime Minister's broad legal discretion to maintain a designation even where the designation criteria are no longer met affects the ability for refusals to de-list persons or entities under UNSCR 1373 to be judicially reviewed. • Communication on de-listing requests does not include the UN Focal Point for De-listings in relation to UNSC Resolution 1988. • The "Advisory on Obligations to Suppress Terrorism under the TSA" does not include guidance on what to do when an entity is delisted. • The exception to prohibitions relating to property of designated terrorist entities expressly extends to dealing "to satisfy the essential human needs of" a designated individual or their dependent, in a manner that does not comply with the UNSCRs.
7. Targeted financial sanctions related to proliferation	PC	• There is no mechanism in place to communicate changes in Iran and DPRK designations to reporting entities, beyond providing a link to the relevant UN web site listing individuals and entities. • There is no obligation to report assets frozen under, or other action taken to comply with, targeted financial sanctions under the Iran and DPRK Regulations. • There is no legislation that protects the rights of bona fide third parties in the Iran Regulations or the DPRK Regulations. • There are no mechanisms for monitoring or ensuring compliance by financial institutions and DNFBPs with Iran or DPRK Regulations.

Recommendations	Rating	Factor(s) underlying the rating
		• There is no information provided on how to apply for delisting, either through MFAT or to the UN Focal Point on De-listings. • Procedures for unfreezing funds or de-listing are not publically known. • There is no mechanism to communicate changes in Iran and DPRK designations to reporting entities, beyond providing a link to the relevant UN web site, nor guidance on what to do in the case of delisting.
8. Non-profit organisations	LC	• New Zealand's legislation does not focus on NPOs identified as vulnerable to abuse for TF, nor considers the proportionality or the effectiveness of regulatory actions available to addressing the TF risk. • Some non-charity NPOs and tax-exempt non-resident charities that may present some risk of abuse for TF, are only subject to policies to combat tax evasion. • There has been insufficient work with NPOs on development and refinement of best practices to address TF risks and vulnerabilities and protection against TF abuse. • Some categories of NPOs identified as being of moderate risk of abuse for TF including foreign charities, overseas donee organisations and charitable trusts, are not subject to risk-based monitoring or supervision. • There are no relevant powers to impose sanctions in relation to other moderate-risk NPOs such as non-charity NPOs and tax-exempt non-resident charities. • The focus under some legislation governing legal persons and arrangements, is on investigating compliance rather than broader wrongdoing by the NPO.
9. Financial institution secrecy laws	C	• This Recommendation is fully met.
10. Customer due diligence	LC	• There is no explicit requirement that CDD be conducted in all situations where there is suspicion of ML/TF. • The definition of beneficial owner does not include the term "ultimate" when describing ownership and control. • In ongoing due diligence, there is no explicit requirement to verify new information and to keep updated records for customer relationships where EDD is not triggered. • For customers that are legal persons or legal arrangements, there is no explicit requirement for reporting entities to understand the nature of their customer's business and its ownership and control structure. • There is no explicit requirement for the reporting entities to identify the powers that regulate and bind a legal person or arrangement. • There is no explicit requirement to identify individuals holding senior management positions when no natural person can be identified in verifying the identity of beneficial owners of legal persons. • The beneficial ownership requirements for trusts do not explicitly set out that reporting entities must identity the settlor, trustee or protector • There are no specific CDD requirements for life insurance. • When conducting CDD on existing customers, the AML/CFT Act does not specify that the reporting entity must take into account whether and when CDD measures were last undertaken or the adequacy of data obtained. • The range of EDD measures in the AML/CFT Act are insufficiently broad. • There is no explicit requirement to refrain from applying simplified CDD measures where there is a suspicion of ML/TF or in situations posing higher ML/TF risk. • There is no requirement permitting a reporting entity to not pursue CDD where it may tip off the customer.
11. Record keeping	LC	• There is no retention period specified for reporting entities to keep account files, business correspondence and written findings.
12. Politically exposed persons	PC	• The definition of foreign PEP excludes important political party officials and restricts the time frame for holding a prominent public function to any time within the past 12 months rather than basing it on an assessment of risk. • There are no requirements to obtain senior management approval before establishing a new business relationship with a PEP. • Reporting entities are only required to obtain source of wealth or funds in relation to a PEP, rather than source of wealth and funds. • New Zealand does not extend its PEP requirements to include domestic PEPs or PEPs from international organisations. • There are no explicit requirements in the AML/CFT Act for determining whether beneficiaries, or beneficial owners of beneficiaries, of life insurance policies are PEPs.

Recommendations	Rating	Factor(s) underlying the rating
13. Correspondent banking	LC	• It is not clear whether New Zealand's correspondent banking rules apply to non-bank relationships with similar characteristics.
14. Money or value transfer services	PC	• There is insufficient action to identify unregistered MVTS providers. • There is no specific requirement for MVTS agents to be registered or licensed. Nor are MVTS providers required to maintain a current list of their agents that is accessible by competent authorities. • MVTS providers do not have include agents in the full scope of their AML/CFT programme or monitor their agents' compliance with their programme.
15. New technologies	LC	• There is not a sufficiently explicit requirement for reporting entities to identify and assess the ML/TF risks that may arise in relation to the development of new products, business practices, or technologies. • This is not a sufficiently explicit requirement for reporting entities to undertake risk assessments of new products, business practices or technologies prior to the launch or use of such products, practices and technologies and take appropriate measures to manage and mitigate the risks. • Not all VASPs are covered by the AML/CFT Act. • New Zealand has not introduced specific requirements for R10 and R16 for virtual assets and VASPs. • The deficiencies in R6, 10-21, 26-27 and 37-40 apply here.
16. Wire transfers	PC	• The wire transfer rules do not apply to credit and debit card transactions. Even though they could be used to conduct a wire transfer. • For wire transfers with a value of less than NZD 1 000, there are no applicable requirements. • There are insufficient record-keeping requirements to ensure that full beneficiary information is maintained by the ordering institution. • There is no explicit requirement however to stop executing a wire transfer if it lacks the required beneficiary information. • There are insufficient requirements for intermediary FIs when processing wire transfers. • There are no explicit requirements that beneficiary institutions take reasonable measures to identify international wire transfers that lack required originator or beneficiary information. • There are no specific legal requirements for MVTS providers either to review ordering and beneficiary information to decide whether to file a SAR or to ensure that a SAR is filed in any country affected and make transaction information available to the NZPFIU.
17. Reliance on third parties	LC	• Reporting entities may rely on a non-reporting entity in certain DBGs. • For overseas-based third parties, there are insufficient requirements for reporting entities to have regard to the level of country risk.
18. Internal controls and foreign branches and subsidiaries	PC	• In AML/CFT programmes, the compliance officer is not required to be at the management level. • There is no specific requirement for financial groups to implement group-wide programs against ML/TF applicable and appropriate to all branches and subsidiaries.
19. Higher-risk countries	PC	• There are insufficient requirements for reporting entities to apply EDD, proportionate to the risks, to customers and transactions involving countries for which this is called for by the FATF. • The range of EDD measures are insufficient.
20. Reporting of suspicious transaction	C	• This Recommendation is fully met.
21. Tipping-off and confidentiality	C	• This Recommendation is fully met.
22. DNFBPs: Customer due diligence	PC	• The AML/CFT Act does not apply to all TCSPs and DPMS. • The CDD requirements for real estate agents and DPMS do not meet the FATF Standards. • The record-keeping requirements for DPMS do not meet the FATF Standards and DPMS do not have PEP and new technology requirements. • The deficiencies identified in R10, R11, R12, R15 and R17 apply here.
23. DNFBPs: Other measures	PC	• The AML/CFT Act does not apply to all TCSPs and DPMS. • DPMS do not have sufficient obligations regarding the obligations in R18, R19, R21 and R22. • The deficiencies identified in R18 and R19 apply here.
24. Transparency and beneficial ownership of legal persons	PC	• Insufficient information on limited partnerships is available publicly. • There are no requirements for limited partnerships to maintain records of proof of their incorporation or certificate of registration.

Recommendations	Rating	Factor(s) underlying the rating
		• Incorporated societies, incorporated charitable trusts, building societies, credit unions and industrial and provident societies do not have specific requirements to maintain required basic information. • There are insufficient requirements for limited partnerships, incorporated societies, building societies, credit unions and industrial and provident societies to keep basic information up-to-date. • There are insufficient requirements to ensure information on beneficial ownership of legal persons is available, accurate and up-to-date. • There are insufficient measures to ensure that legal persons co-operate with competent authorities to determine who the beneficial owners are. • There is not a general obligation for legal persons (or their representatives) to maintain information and records for at least five years after the date on which the company is dissolved. • The ML/TF risks of bearer share warrants have not been mitigated. • The M/TF risks of nominee directors and shareholders have not been sufficiently mitigated. • There are insufficient sanctions for legal or natural persons that fail to comply with the basic and beneficial ownership requirements. • The deficiencies in R37 impact New Zealand's ability to provide international co-operation in relation to basic ownership and the beneficial ownership information.
25. Transparency and beneficial ownership of legal arrangements	PC	• There are not sufficient requirements for all trustees to obtain and hold adequate, accurate and current information on the identity of the settlor, the trustees, the protector and the beneficiaries or class of beneficiaries and any other natural person exercising ultimate effective control, and keep this information up-to-date. • There are no specific provisions for trustees to hold basic information on other regulated agents and service providers including investment advisors, accountants and tax advisors • There are no explicit requirements for trustees to disclose their status to reporting entities when forming a business relationship or carrying out an occasional transaction above the threshold. • There are insufficient sanctions and/or liability for trustees that fail to comply with information requirements.
26. Regulation and supervision of financial institutions	PC	• No agency in New Zealand has a mandate to supervise for implementation of TFS obligations. • RBNZ does not extend the fit and proper test to shareholders or controllers of NBDTs and life insurers. • Some core principle FIs are only required to be registered on the FSPR without a need to be licensed. • Providers of factoring, tax pooling, payroll remittance, debt collection, cash transport and safety deposit boxes are not required to be licensed or registered in New Zealand. • Fit and proper test only applies to controlling owner of FIs with beneficial ownership equal to or more than 50% under the FSPR registration regime. • Core Principles FIs are not regulated and supervised fully in line with the Core Principles that are relevant to AML/CFT. • The supervisors do no always review the assessment of a FI's ML/TF risk profile when there is a major event or development.
27. Powers of supervisors	LC	• However, the range of sanctions available to the supervisors is insufficient, as they lack the power to apply administrative pecuniary penalties under the AML/CFT Act. • It is unclear whether supervisors can withdraw, restrict or suspend FIs' licenses or registration for breaches of the AML/CFT Act.
28. Regulation and supervision of DNFBPs	PC	• No agency in New Zealand has a mandate to supervise for implementation of TFS obligations. • The AML/CFT Act does not apply to all TCSPs and DPMS. • There are no entry controls for accounting practices who are not CAANZ members, TCSP and DPMS sectors. • Fit and proper testing does not extend to the management and beneficial owners of corporate real estate agents. • Risk-based AML/CFT supervision is not established in most of DNFBP sectors.
29. Financial intelligence units	C	• This Recommendation is fully met.
30. Responsibilities of law enforcement and investigative authorities	C	• This Recommendation is fully met.

Recommendations	Rating	Factor(s) underlying the rating
31. Powers of law enforcement and investigative authorities	LC	• As New Zealand law does not allow any cash to leave a Customs Controlled Area, it is not clear whether Customs can conduct controlled delivery relating to cash.
32. Cash couriers	LC	• The administrative penalty for false or non-declaration of cash through summary disposal is not proportionate and dissuasive.
33. Statistics	LC	• New Zealand does not maintain sufficiently comprehensive statistics on MLA, ML investigations and prosecutions and on all property frozen, seized and confiscated.
34. Guidance and feedback	LC	• The NZPFIU provides insufficient guidance and feedback on typologies. • There is a lack of sector-specific guidelines for TCSPs and casinos.
35. Sanctions	LC	• No sanctions are available for moderate-risk NPOs. • There are insufficient sanctions applicable to FI and DNFBP sectors that are not subject to licensing or entry controls. • The range of sanctions available to the supervisors could be strengthened, particularly in relation to administrative pecuniary penalties. • Civil sanctions available for breaches of AML/CFT requirements generally do not apply to directors and senior management of FIs and DNFBPs
36. International instruments	LC	• There are minor technical gaps in the implementation of the Merida Convention.
37. Mutual legal assistance	LC	• CLO has an insufficient case management system for MLA. • MACMA does not have specific provision to safeguard the confidentiality of MLA requests they receive, and the information contained in them. • MACMA provides no specific powers in relation to the taking of witness statements and does not empower the use of the full range of investigative techniques.
38. Mutual legal assistance: freezing and confiscation	LC	• The threshold for restraint or forfeiture requests regarding an instrument of crime is unduly restrictive.
39. Extradition	LC	• CLO has an insufficient case management system for extradition.
40. Other forms of international co-operation	LC	• The supervisors are not subject to any explicit provision to have prior authorisation or consent of the requesting competent authority to disclose information exchanged. • There is no explicit provision in the AML/CFT Act that allows RBNZ, FMA and DIA to conduct enquiries on behalf of foreign counterparts. • There is no explicit provision for RBNZ and FMA to have prior authorisation or consent of the requested financial supervisors to disclose information exchanged.

Glossary of Acronyms[50]

Abbreviations	
AML	Anti-money laundering
AML/CFT Act	Anti-Money Laundering and Countering the Financing of Terrorism Act 2009
APG	Asia/Pacific Group on Money Laundering
ARIN-AP	Asset Recovery Interagency Network - Asia Pacific
ARU	Asset Recovery Unit
ASIC	Australian Securities and Investments Commission
AUSTRAC	Australian Transaction Reports and Analysis Centre (FIU)
BCP	Basel Core Principles for Banking Supervision
BCR	Border Cash Report
BNI	Bearer negotiable instruments
BO	Beneficial ownership
BS Act	Building Societies Act 1965
CA	Crimes Act
CAANZ	Chartered Accountants Australia New Zealand
CARIN	Camden Asset Recovery Inter Agency Network
CDD	Customer due diligence
CEA	Customs and Excise Act
CFT	Counter-terrorist financing
CLAG	Combined Law Agency Group
CLO	*Crown Law Office*
CPF	Counter-proliferation financing
CPRA	*Criminal Proceeds (Recovery) Act 2009*
CT	Counter-terrorism
CT Act	*Charitable Trusts Act 1957*
CTAG	Combined Threat Assessment Group
CTCC	Counter-Terrorism Co-ordination Committee
CVE	Counter-violent extremism
DBG	Designated business group
DIA	Department of Internal Affairs
DIMS	Discretionary investment management services
DNFBP	Designated non-financial businesses and profession
DPMC	Department of Prime Minister and Cabinet
DPMS	Dealer in precious metals or stones
DPRK	Democratic People's Republic of Korea
EDD	Enhanced due diligence
FA Act	*Financial Advisors Act 2008*
FATF	Financial Action Task Force
FCG	Financial Crime Group
FCPN	Financial Crime Prevention Network
FI	Financial institution
FIU	Financial Intelligence Unit

50 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

Abbreviations	
FMA	Financial Markets Authority
FMC Act	*Financial Markets Conduct Act 2013*
FMS Act	*Financial Markets Supervisors Act 2011*
FSCU Act	*Friendly Societies and Credit Unions Act 1982*
FSPR	Financial Services Providers Register
FSPR Act	*Financial Services Providers (Registration and Dispute Resolution) Act 2008*
FSRB	FATF-style regional body
FTF	Foreign terrorist fighter
FTR Act	*Financial Transaction Reports Act 1996*
GCSB	Government Communications Security Bureau
GDP	Gross domestic product
HVD	High value dealer
IET	Integrity and Enforcement Team
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organization
IO	Immediate Outcome
IOSCO	International Organization of Securities Commissions
IPS Act	*Industrial and Provident Societies Act 1908*
IR	Inland Revenue
IS	*Incorporated Societies Act 1908*
ISIL	Islamic State of Iraq and the Levant
LC Act	*Lawyers and Conveyancers Act 2006*
LEA	Law enforcement agency
LP Act	*Limited Partnerships Act 2008*
MACMA	*Mutual Assistance in Criminal Matters Act 1992*
MBIE	Ministry of Business, Innovation and Employment
MER	Mutual evaluation report
MFAT	Ministry for Foreign Affairs and Trade
MIS	Managed investment services
ML	Money laundering
MLA	Mutual legal assistance
MLT	Money Laundering Team
MMOU	Multilateral Memorandum of Understanding
MOA	Memorandum of agreement
MOJ	Ministry of Justice
MOU	Memorandum of understanding
MPI	Ministry of Primary Industries
MSD	Ministry of Social Development
MVTS	Money or value transfer services
NBDT	Non-bank deposit taker
NBDT Act	*Non-bank Deposit Takers Act 2013*
NCC	National Co-ordination Committee
NIC	National Intelligence Centre
NOCG	National Organised Crime Group
NPO	Non-profit organisation
NRA	National Risk Assessment
NSCTG	National Security and Counter-Terrorism Group
NSG	National Security Group
NSIT	National Security and Investigation Team
NSS	National Security System
NZ	New Zealand
NZ Police	New Zealand Police
NZCS	New Zealand Customs Service

Abbreviations	
NZD	New Zealand Dollar
NZHC	New Zealand High Court
NZICA Act	*New Zealand Institute of Chartered Accountants Act 1996*
NZLS	New Zealand Law Society
NZPFIU	New Zealand Police Financial intelligence Unit
NZSC	New Zealand Society of Conveyancers
NZSIS	New Zealand Security Intelligence Service
OA	Official Assignee
OC	Oversight Committee
ODESC	Officials' Committee for Domestic and External Co-ordination
OIO	Overseas Investment Office
PAL	Pacific Aerospace Limited
PEP	Politically exposed person
PF	Proliferation financing
PFO	Profit Forfeiture Order
PFT	Proactive Financial Targeting
PTR	Prescribed transaction report
RBNZ	Reserve Bank of New Zealand
RBNZ Act	*Reserve Bank of New Zealand Act 1989*
REA	Real Estate Authority
REA Act	*Real Estate Agents Act 2008*
RITA	Racing Industry Transition Agency
SAP	Strategic Action Plan
SAR	Suspicious activity report
SFO	Serious Fraud Office
SITG	Security Intelligence and Threats Group
SOP	Standard operating procedure
SRA	Sector risk assessment
SSA	Search and Surveillance Act
STR	Suspicious Transaction Report
TA Act	*Tax Administration Act 1994*
TAA	Tax Administration Act
TBML	Trade Based Money Laundering
TCSPs	Trust and company service providers
TDWG	Terrorist Designation Working Group
TF	Terrorist financing
TFS	Targeted financial sanctions
TSA	*Terrorism Suppression Act 2002*
UN	United Nations
UN Act	*United Nations Act 1946*
UNSCR	UN Security Council Resolution
VASP	Virtual asset service provider

www.fatf-gafi.org | www.apgml.org

April 2021

Anti-money laundering and counter-terrorist financing measures - New Zealand

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in New Zealand as at the time of the on-site visit from 26 February to 15 March 2020.

The report analyses the level of effectiveness of New Zealand's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.