Report on the review of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

MINISTRY OF JUSTICE
Tāhū o te Ture

Te Kāwanatanga o Aotearoa
New Zealand Government

Important notice

The information in this publication is, according to the Ministry of Justice's best efforts, accurate at the time of publication. The Ministry will make every reasonable effort to keep it current and accurate. However, users of this publication are advised that:

- the opinions contained in this document are those of the Ministry and do not reflect official government policy.
- the information does not alter the laws of New Zealand, other official guidance, or requirements, nor does it constitute legal advice. Readers are advised to seek specific legal advice from a qualified professional person before undertaking any action in reliance on the contents of this publication.
- the Ministry does not accept any responsibility or liability whatsoever whether in contract, tort, equity or otherwise for any action taken as a result of reading, or reliance placed on the Ministry because of having read, any part, or all, of the information in this discussion document or for any error, inadequacy, deficiency, flaw in or omission from the discussion document.
- All references to websites, organisations, or people not within the Ministry are for convenience only and should not be taken as endorsement of those websites, information contained in those websites, nor of organisations or people referred to.

Published in July 2022 © Crown Copyright
Cover image by Kevin Matos on Unsplash

ISBN: 978-0-473-64218-1

Presented to the House of Representatives in accordance with section 156A(3) of the *Anti-Money Laundering and Countering Financing of Terrorism Act 2009*.

Contents

Glossary of terms

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
Act	The AML/CFT Act 2009
AML/CFT supervisors	The Department of Internal Affairs, the Financial Markets Authority, and the Reserve Bank of New Zealand, are the entities which regulate reporting entities covered by the Act
CDD	Customer Due Diligence
DBG	Designated Business Group
DIA	The Department of Internal Affairs
Discussion Document	The public discussion document published by the Ministry of Justice in October 2021 to support the review (available on the Ministry's website)
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FATF Recommendations / Standards	The international standards on combatting money laundering and the financing of terrorism and proliferation (available on the FATF's website)
FIU	New Zealand Police Financial Intelligence Unit
FMA	The Financial Markets Authority
HVDs	High Value Dealers
IFT	International Funds Transfer
IR	Inland Revenue
ME	Mutual Evaluation (undertaken by the FATF)
PPCs	Policies, procedures, and controls
PTR	Prescribed transaction report
RBNZ	The Reserve Bank of New Zealand
SAR	Suspicious activity report
Summary Document	A summary of all public submissions received by the Ministry following the discussion document (available on the Ministry's website)
TCSP	Trust and Company Service Provider
TFS	Targeted financial sanctions
VASPs	Virtual Asset Service Providers

Executive summary

1. The Ministry of Justice has reviewed the Anti-Money Laundering and Countering Financing of Terrorism Act (the Act) to assess how it has performed since 2017 as well as whether any amendments should be made. This review was required by section 156A of the Act and began on 1 July 2021.

2. We saw the review as being the start of a conversation about how New Zealand's AML/CFT regime can be the best it can be, and we have identified a number of areas where changes could be made. A large number of these changes can be made through amendments to the Act, but a significant portion can also be made through issuing secondary legislation (e.g., regulations) or through operational enhancements.

3. The recommendations we have made reflect a consensus of the regime, which we formed through extensive engagement with AML/CFT agencies as well as the industry. However, in some places we have deliberately not made a firm recommendation for what amendments should be made and have instead recommended a direction of travel for the regime. This is to ensure that the conversation with industry and agencies continues and that specific changes are identified following detailed and comprehensive engagement with stakeholders.

Summary of findings

4. Overall, we consider that the Act provides for a generally sound regulatory regime that is effective to some extent at detecting and deterring money laundering and terrorism financing. However, there are some foundational issues that we consider prevent the regime from being the best it can be for New Zealand and major improvements are needed to the regime. This is broadly consistent with the findings of the Financial Action Task Force (FATF) when they conducted the Mutual Evaluation of New Zealand.

5. The biggest issue that we have identified is that the Act is not taking a sufficiently risk-based approach in that efforts by agencies and businesses are not always being prioritised towards areas of highest risk. Some requirements in the Act are overly prescriptive which prevents a flexible risk-based approach being taken. In addition, where a requirement is flexible, businesses generally do not have enough information or awareness about how to apply a risk-based approach. This is due to insufficient guidance or strategic intelligence being produced.

6. The national assessment of New Zealand's money laundering and terrorism financing risks is out-of-date and has not been updated according to the agreed or recommended schedule. The outdated NRA undermines the strategic risk-based approach as we cannot be certain that we are addressing most important current risks. In particular, information on money laundering methods is almost a decade old and we cannot fully consider the impact to the risk environment of key changes to the system such as the Phase 2 reforms. There is also a significant risk that the regime participants are failing to combat areas of greatest threat as risks have not been assessed and communicated to agencies or industry.

7. We also consider that the regime is not sufficiently resourced to deliver its functions. We received clear feedback from those within agencies that they do not have enough resources to fulfil their responsibilities. Insufficient resourcing was also identified by the FATF as a deficiency. Furthermore, the private sector does not consider the regime to be sufficiently resourced, which has limited how responsive the regime is to the needs of industry. The insufficient resource levels, along with an absence of mechanisms to ensure appropriate resource allocation across the regime, is likely contributing to the operation of the Act not being sufficiently risk based. These issues are likely further compounded

by multiple agencies' having to coordinate their efforts to deliver services in the regime, such as supervision.

8. The net outcome of these issues is that the regime is not as effective as it could be, and it is harder (and likely more expensive) than it needs to be for businesses to comply with the Act. Ultimately this undermines efforts from businesses to detect and deter money laundering and terrorism financing. We received clear feedback from industry that they thought the regime largely takes a 'one size fits all' approach, in that a provincial law firm is expected to comply with the Act in the same way as a large multinational bank. Given that most businesses in the regime are small, we consider that more needs to be done to make it easy for these businesses to comply with their obligations. In turn, this will make the regime more effective.

9. Finally, we consider that the Act can be utilised to provide much-needed regulatory support for businesses who have sanctions obligations, particularly financial sanctions to combat terrorism financing and financing the proliferation of weapons of mass destruction. We note that very little support is provided to businesses in implementing their sanctions obligations. This carries a material risk that sanctions obligations will be breached. To avoid this, we consider that the Act should be amended to provide additional obligations on businesses to ensure that sanctions obligations are appropriately implemented, with AML/CFT supervisors empowered to support and monitor compliance.

Background to the review

10. The Act was introduced in 2009, substantively amended in 2015 and 2017, and plays a pivotal role in New Zealand's effort to combat serious and organised crime as well as terrorism by making it harder for illicit financial activity to occur. Money laundering enables and incentivises offending that impacts the health and wellbeing of New Zealand communities and threatens New Zealand's international reputation. Further, while the risk of large-scale terrorism financing in New Zealand is low, the consequences of lone actors self-raising funds can be devastating.

11. New Zealand is a member of the FATF, which is the global money laundering and terrorism financing watchdog. The inter-governmental body has produced a set of binding standards that countries are expected to apply when establishing their AML/CFT regimes, known as the FATF Recommendations. New Zealand underwent a comprehensive assessment between 2020-21 by the FATF, known as a Mutual Evaluation, which assessed the extent of compliance with the Recommendations as well as the extent to which the regime is effective. The FATF found that New Zealand's efforts to combat money laundering and terrorist financing are delivering good results, but more needs to be done on improving the availability of beneficial ownership information, strengthening supervision and implementation of targeted financial sanctions.

Chapter 1: Achieving the objects of the Act

12. In this chapter, we consider the extent to which the Act is achieving its objects or purposes in order to assess how well it has performed since 2017. The purposes of the Act are outlined in section 3 and are to:

    - detect and deter money laundering and the financing of terrorism
    - maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force (FATF), and
    - contribute to public confidence in the financial system.

13. Overall, the Act provides a necessary basis to detect and deter money laundering and terrorism financing, which is its primary purpose. This conclusion is largely in line with the

findings of the FATF in New Zealand's Mutual Evaluation. However, there are two main barriers to the Act being as effective as it could be: the lack of an up-to-date national assessment of risks, and a number of important gaps in the Act's measures to deter money laundering and terrorism financing. Furthermore, as discussed elsewhere in this report, the Act's ability to effectively detect and deter money laundering is heavily impacted by the level of resourcing for the regime as well as how easy it is for businesses to submit reports through to the FIU.

14. The Act is intended to be an inherently risk-based regime, in that efforts by government and businesses should be prioritised to areas of highest risk. However, the out-of-date assessment of national risks means that the regime may not be responding to new or emerging risks that have not been identified. In addition, we received a large amount of feedback that the overall risk assessment framework can be improved in terms of how information is communicated to businesses as well as the nature of the information that is shared. Generally larger businesses have a better understanding of their risks, while smaller businesses or businesses that have not been in the regime for as long had a more developing understanding of their risks and New Zealand's risks overall.

15. The Act generates a large amount of financial intelligence to be analysed and turned in to intelligence products. Most of the reports come from larger and more sophisticated financial institutions, with generally low levels of reporting from DNFBP sectors and smaller financial institutions. The low level of reporting does not reflect the risks associated with those sectors, and likely results from the variance in risk understanding between financial institutions and other sectors. The FIU in turn produces a large amount of intelligence products, but the FATF found that the FIU did not fully exploit the potential of financial intelligence being used to detect criminal activity by persons not already known to law enforcement. Nevertheless, several investigations and prosecutions have made extensive use of financial intelligence provided by the FIU.

16. Deterrence of money laundering and terrorism financing is undermined by gaps in obligations for businesses, as well as gaps in the overall regulatory regime, which leave many businesses vulnerable to being misused. These gaps are, in turn, further undermined by the AML/CFT supervisors lacking sufficient enforcement powers to respond to all instances of non-compliance with the Act and impose effective, proportionate, and dissuasive penalties. Notwithstanding this, we consider that law enforcement authorities will be having some deterrent effect through investigating and prosecuting this offending and being highly effective at recovering assets.

17. While we have identified several gaps in the Act and many areas for improvement, we note that the FATF found New Zealand to be relatively effective compared to many other countries, including Australia, Canada, and the United States. Importantly, New Zealand was not found to warrant public identification by the FATF as a high-risk jurisdiction, which would have occurred with a weaker regime. As such, we consider that the Act has generally maintained and enhanced New Zealand's international reputation, but there is still more that could be done regarding preventing misuse of companies and trusts.

18. Finally, we were not able to identify any negative impacts following AML/CFT reform in the levels of investor confidence, ease of doing business, and the rate of business registrations in New Zealand. We generally consider that the Act appears to have fulfilled its third purpose of contributing to public confidence in the financial system to the extent public confidence can be measured.

Chapter 2: How the regime has operated

19. This chapter considers how the regime has operated or delivered its outcomes in terms of the cost of the regime, overall regulatory maturity, and consistency with Te Tiriti o Waitangi. Reporting entities to were asked to complete a survey of their estimated costs for the financial year ending 31 March 2022, which was used to derive the estimated per-business cost as well as a total private sector cost of the regime. This was then combined with the actual costs from the public sector to determine the total per annum cost of the regime. We similarly assessed the regulatory maturity of the AML/CFT regime by sending

a survey to everyone in government who works on the regime. Finally, we assessed the consistency of the regime with Te Tiriti by considering the extent to which the Crown has operated consistently with the principles of Te Tiriti as expressed by the Waitangi Tribunal.

20. We estimate that the AML/CFT regime costs New Zealand approximately NZD 260 million per annum, split between the private sector (NZD 246 million) and the public sector (NZD 14 million). While this is a significant sum, we also estimate that the regime has significant monetary and non-monetary benefits, including disrupting NZD 1.7 billion worth of illegal drugs and fraud and NZD 5 billion of broader criminal activity over a ten-year period. We also note that not having an AML/CFT regime, or having a significantly weaker regime, would result in New Zealand being identified by the FATF as a high-risk jurisdiction. This would damage New Zealand's international reputation and result in an estimated reduction of capital inflows of between 4.6 percent and 10.5 percent of GDP (between NZD 15 and 35 billion, or 58 to 134 times the estimated cost of the regime).

21. In terms of regulatory maturity, the average scores from the survey suggest that the AML/CFT regime is generally defined and evolving, which indicates that there is recognition of the need for shared outcomes and more consistent ways of working with work underway to support more coordinated approaches across the system. However, given the regime has been in place for 12 years, we consider that this result is lower than it should be. A particular area of weakness identified was the low levels of resourcing of the regime, which appears to be causing underperformance in other areas (specifically the regime's efficiency, effectiveness, and durability). However, the regime does appear to be sufficiently mature with respect to its governance, leadership, and strategic direction.

22. Finally, we consider that the Crown can and should do more to satisfy its duty to be sufficiently informed about whether there are impacts for Māori or Māori interests in the operation of the Act. We note that there has been little, if any, engagement with Māori throughout the course of the Act's operation. This is despite there likely being some Māori interests in the Act resulting from impacts on the criminal justice, financial inclusion, data sovereignty, and the operation of post-settlement governance entities

Chapter 3: Institutional arrangements and stewardship

23. This chapter makes a number of recommendations for changes to the fundamental components of the overall regime, such as the purposes of the Act, the approach the regime should take to regulation, and how the various agencies are structured and operate.

24. We recommend a number of changes to the purpose of the Act. One major change we recommend is that the Act should have the purpose of supporting businesses in their implementation of sanctions obligations under the *Terrorism Suppression Act 2002*, *United Nations Act 1946*, and *Russia Sanctions Act 2022*. We also recommend some smaller tweaks to the purpose of the Act, namely ensuring it refers to the Act taking a risk-based approach, accurately reflects its broader societal outcomes, and also combats proliferation financing. We do not, at this stage, recommend that the Act's purpose be changed to include prevention of money laundering and terrorism financing, but nonetheless recommend that further prevention-focused obligations be explored and strengthened where appropriate.

25. We recognise that the Act has not been sufficiently risk-based for a number of reasons, which has the net impact of the Act not being as effective as it could be as well as being more expensive for businesses. We recommend strengthening the framework for understanding and sharing risk information through creating a specific power for the National Coordination Committee (NCC) to request the production of a risk assessment, as well as further progressing the development of a framework for sharing dynamic and/or live risk information. We also recommend that further and more detailed guidance is provided to businesses to ensure they empowered to comply with their various risk-based obligations, and that further regulatory exemptions for low-risk products, businesses, and transactions are issued. Finally, we also recommend that more is done to

make it easy for smaller and/or lower capacity business to comply with their obligations, such as through creating a centralised source of AML/CFT information or developing additional tools or resources for businesses.

26. In terms of the agency arrangements or structure, we broadly recommend that further analysis is conducted to determine whether an alternative approach to the structure of the regime is viable and addresses issues we have identified with the current structure. This could include creating a new agency to deliver policy, administration, and financial intelligence function, creating a single supervisory agency (instead of the current multi-supervisory model), or creating a combined supervisor and Financial Intelligence Unit (FIU). This further work should also include conducting a full analysis of the costs and benefits of any change, given that changing the agency structure would be very disruptive to the regime. Irrespective of the agency structure, we recommend amending the Act to the FIU has the necessary independence to deliver AML/CFT services, formalising existing private sector advisory group models, and exploring a hybrid public/private funding model to ensure the regime is sufficiently resourced.

27. Finally, we make a series of changes to the powers or functions of agencies as well as improving information sharing within the regime. In particular, we recommend empowering the AML/CFT supervisors to supervise the implementation of targeted financial sanctions, can appropriately inspect businesses that operate from private residences, and can inspect businesses remotely. Subject to developing appropriate privacy protections and safeguards, we also recommend providing powers to the FIU to request information from businesses that are not reporting entities, conduct ongoing monitoring of transactions and accounts in high-risk situations, and can freeze accounts and/or block certain transactions to prevent harm.

Chapter 4: Scope of the Act

28. This chapter considers and makes various recommendations as to whether the Act is capturing the right activities and businesses to mitigate New Zealand's risks of money laundering and terrorism financing. It also considers whether the definitions and terminology for existing activities or services are fit-for-purpose, especially given technological advancements.

29. We have identified a number of ways the Act could be strengthened to combat areas of high risk. In particular, we are concerned that illicit capital is still able to enter the real estate market despite the inclusion of law firms, conveyancers, and real estate agents in the regime between 2018 and 2019. Similarly, we consider that the Act could (and should) do more to combat trade-based money laundering through potentially increasing obligations for some businesses and/or enhancing information sharing between agencies. However, we recommend conducting a thorough risk assessment to identify the particular ways in which real estate and the trade system are or could be exploited to ensure that any changes are appropriately risk-based. We also recommend a number of changes to clarify and strengthen obligations for virtual asset service providers and high-value dealers to order to protect against the use of virtual assets or high-value goods for money laundering and terrorism financing.

30. In terms of current terminology, we make a large number of recommendations to improve the clarity of the various capture points in the Act, particularly for designated non-financial businesses and professions (DNFBPs). We further recommend clarifying how the Act applies to stored value instruments, businesses that provide multiple activities, and the scope of "in the ordinary course of business". We also consider that there should be greater alignment between the definition of 'financial institution' in the Act and the definition of 'financial services' in the *Financial Service Providers (Registration and Dispute Resolution) Act 2008*, which could involve amendments to either or both Acts.

31. We generally do not recommend that any additional activities should be captured by the Act as did not consider there to be sufficient risks of money laundering or terrorism financing that would justify the changes. Specifically, we do not recommend capturing businesses that act as a secretary of a company or partner in a partnership, criminal

defence lawyers, non-life insurance businesses, or non-profit organisations that are moderately vulnerable to terrorism financing. The one exception is with respect to businesses that could provide financial intelligence by virtue of the services they provide, such as fintech providers offering open banking solutions or marketplace operators. For these businesses, we recommend further exploring whether these businesses should be reporting entities, and if so, how obligations could be appropriately tailored.

32. We also make a number of recommendations to issue new exemptions for various low-risk sectors or products, in line with our general recommendations regarding taking a more risk-based approach. For example, we recommend issuing new exemptions for certain businesses that act as a trustee or nominee, provide low value loans, and various Crown-owned or controlled entities that provide certain captured activities using public funds. We also recommend reviewing and/or clarifying the scope of some existing exemptions, such as for internet auctioneers, special remittance card facilities and non-finance businesses that transfer money or value.

33. Finally, amending the Act to define its territorial scope to ensure that offshore businesses that provide captured activities to or in New Zealand have the same obligations as businesses based in New Zealand. We consider that this approach will ensure an even playing field and that New Zealand businesses are not unfairly disadvantaged by being in New Zealand and having AML/CFT obligations. However, we do not have a firm recommendation for how the territorial scope should be defined and recommend that further analysis is conducted to identify the best approach that could be taken. In the interim, we recommend reviewing and updating the existing territorial scope guidance to ensure it is sufficiently clear, appropriate, and consistent with the approach taken in related regulatory regimes.

Chapter 5: Supervision, regulation, and enforcement

34. This chapter makes a number of recommendations to improve the supervision, regulation, and enforcement of the regime. A core component of the AML/CFT regime is that it needs to enable effective supervision and regulation of businesses. The supervision and monitoring of businesses should address and mitigate money laundering and terrorism financing risks in the economy, in part by promptly identifying, remedying, and sanctioning (where appropriate) businesses that do not adequately comply with their obligations. We have also considered whether there should be any regulation of businesses that provide services to reporting entities, specifically auditors, agents, and consultants.

35. We note that there are no specific AML/CFT specific registration or licensing framework, but that the regime relies on other sector-specific frameworks, such as the Financial Services Provider Register. However, this approach was criticised by the FATF and results in some sectors not having any registration requirements, others sectors not being subject to sufficient fit and proper or market entry checks, and some high-risk sectors not being licensed when they arguably should be. We recommend agencies further develop specific options for a comprehensive registration framework, which includes amending the Act to create a specific registration requirement for those sectors that have no existing requirements. We also recommend amending the Act to create a specific AML/CFT licensing framework for high-risk sectors that are not already required to be licensed (for example remitters and trust and company service providers).

36. We recognise the valuable contribution that many auditors, agents, and consultants provide to the AML/CFT regime. However, we also recognise that there are instances of unsatisfactory audits occurring in some sectors, and that the Act is not sufficiently mitigating the risks posed by agents. As such, we recommend further regulation of audits and auditors, such as creating a code of practice that details the requirements of an audit as well as amending the Act to introduce an accreditation regime for auditors. We consider that these steps will likely improve the quality and value of audits, but we also note that further work may be required if these changes do not sufficiently improve audit outcomes. With respect to agents, we recommend issuing regulations to ensure that businesses that use agents are appropriately vetting and training their agents as well as

ensuring their agents comply with the requirements of the Act. We do not recommend any additional regulation for consultants at this stage.

37. Finally, we make a number of recommendations to ensure that effective, proportionate, and dissuasive penalties can be applied against businesses that fail to comply with the Act. In particular, we recommend allowing for infringements or fines to be imposed against businesses as well as for supervisors to be able to restrict, suspend, or cancel a business' AML/CFT or prudential licence or registration for non-compliance with the Act. We also recommend increasing the available penalties in the Act to ensure they are able to be proportionate to serious misconduct irrespective of the size or nature of the business involved, as well as for civil penalties to be imposed against employees, directors, and senior managers in appropriate circumstances. However, we also recognise that penalties should be risk based and proportionate in their application and recommend amending the Act to prescribe a non-exhaustive list of AML/CFT-specific aggravating and mitigating factors that must be considered when penalties are applied.

Chapter 6: Preventive measures

38. This chapter considers and makes a large number of recommendations regarding the obligations that businesses have in the Act in order to prevent or mitigate the risk of being misused for money laundering or terrorism financing. Effective preventive measures should be informed by and reflect an understanding of money laundering and terrorism financing risks and ultimately protect businesses from harm. However, AML/CFT obligations also impose significant and sometimes disproportionate compliance costs on businesses, particularly where they are not imposed in an efficient way or do not allow for innovative approaches to be taken.

39. We make a number of recommendations regarding customer due diligence (CDD) obligations that we anticipate will ease compliance costs and frustrations for businesses as well as support a more risk-based approach being taken. For example, we recommend reviewing and updating the Identity Verification Code of Practice to reflect the Digital Identity Trust Services Framework (once enacted), issuing regulations to exempt all businesses from the requirement to verify address information except where enhanced CDD is required, and also issuing regulations to relaxing the requirement to conduct enhanced CDD for customers that are trusts. We also recommend issuing regulations to clarify the definition of a beneficial owner, expanding what information needs to be collected about legal persons and legal arrangements, and expanding the range of measures that businesses can take to mitigate a customer that is higher risk. Finally, we recommend issuing regulations to provide further clarity for CDD obligations in respect of various non-financial activities.

40. We note that the Act's requirements with respect to Politically Exposed Persons (PEPs) were criticised by the FATF and do not reflect the risk in New Zealand. As such, for foreign PEPs, we recommend amending the definition of PEP in the Act, requiring businesses to have appropriate risk management systems in place to determine whether a customer is a foreign PEP and specifying that PEP checks should conducted at the appropriate time depending on the level of risk involved with the relationship. We also recommend that the definition of PEP should be amended to include domestic PEPs, given there have been several instances of public sector corruption and fraud observed while the Act has been in operation. However, we recognise that domestic PEPs are typically less risky than foreign PEPs and recommend lesser requirements for identifying and mitigating the risk of a domestic PEP compared with foreign PEPs.

41. The FATF also made a number of criticisms about the requirements regarding sending and receiving funds via a wire transfer. Given that wire transfer obligations are intended to prevent terrorists and other criminals from having unregulated access to international payment systems and to enable misuse to be easily detected, we make a number of recommendations for change that should be progressed through issuing regulations. In particular, we recommend introducing limited requirements to collect identity about the parties to an international wire transfers below NZD 1,000 as well as further obligations on intermediary and beneficiary institutions to detect and respond to incomplete wire transfers. However, we also recognise that terminology in the Act relating to wire

transfers is outdated and needs considerable reform, and we recommend repealing and replacing the terminology in the Act in consultation with the private sector. We note that this would also provide an opportunity to resolve issues with prescribed transaction reporting.

42. We also make a series of recommendations regarding the provisions in the Act relating to reliance. Relying on a third party to conduct CDD is one of the main ways that businesses can reduce their compliance obligations, particularly where a customer is in another country or where there are multiple businesses involved in a transaction or activity. We note that the Digital Identity Services Trust Framework and register of beneficial ownership for companies and trusts will likely reduce the extent to which CDD is duplicated across the regime and address issues raised by submitters. Nevertheless, we recommend continuing to explore the reliance provisions in the Act, including whether the "approved entity" scheme can ever be used and the provisions relating to reliance within a designated group of businesses.

43. New Zealand is exposed to global or international risks of money laundering or terrorism financing from other countries or transnational organised crime groups: some of these countries have been publicly identified by the FATF as being high risk, but other customers from countries should also be considered in appropriate circumstances. We recommend updating existing guidance to provide further detail about dealing with other countries to ensure a more nuanced and risk-based approach can be taken by businesses, and also recommend issuing regulations to clarify how to deal with countries that are on the FATF's greylist or blacklist. However, some countries are so risky that further countermeasures are justified, and as such, we recommend issuing regulations to mitigate the risk posed by Iran and the Democratic People's Republic of Korea. We also recommend amending the Act to ensure a sufficiently broad range of countermeasures can be imposed if required, which should include exploring the feasibility of issuing countermeasures against specific transnational crime groups to combat the threat those groups pose to New Zealand.

44. Finally, we also make a number of more minor recommendations relating to record keeping, correspondent banking, money or value transfer services, the use of new technologies, and internal controls. These recommendations include further clarifying and reconciling record keeping obligations to align with the *Privacy Act 2020*, updating requirements for correspondent banking relationships, requiring businesses to conduct a risk assessment before using a new technology or product, and providing businesses with the option of having a compliance officer as a senior manager in the business. We also recommend amending the Act to ensure that groups of businesses develop programmes to mitigate their group-level risks, and agencies further explore what obligations should be developed to support the implementation of targeted financial sanctions obligations.

Chapter 7: Financial intelligence

45. This chapter focuses on the relevant requirements for three types of report required to be submitted under the Act, specifically suspicious activity reports (SARs), prescribed transaction reports (PTRs), and border cash reports (BCRs). The collection, analysis, and dissemination of financial intelligence is a fundamental purpose of the Act, and is core to identifying suspicious or illicit activity, developing strategic intelligence, and fundamental to an effective risk-based approach.

46. With respect to SARs, we recommend providing further guidance about submitting these reports, reviewing the legislative requirements for submitting SARs, and reviewing and potentially replacing goAML with an appropriate system if it is not possible to make goAML more user friendly. We also recommend amending the requirements for lawyers to ensure they can appropriately navigate their legal privilege and SAR obligations and consider amending the information sharing provisions for SARs to enable a more collaborative approach to be taken by industry.

47. With respect to PTRs, we note that many of the challenges with these reports result from the wire transfer terminology in the Act, which we recommend repealing and replacing in

consultation with industry. In the interim, we recommend issuing regulations to clarify the types of transactions that should be reported as well as tailoring obligations when non-financial businesses are involved with sending or receiving wire transfers on behalf of an underlying customer. In the long term, and once known issues are satisfactorily resolved, we recommend lowering the reporting threshold for international funds transfers (i.e., to NZD 0) and large cash transactions (e.g., to NZD 5,000) if the costs are justified by the benefits.

48. Finally, we recommend amending the Act and issuing regulations to require BCRs in respect of other forms of value, such as casino chips and precious metals. This will ensure that BCRs continue to provide valuable intelligence about cross-border value movements and enable broader detection and deterrence of money laundering and terrorism financing. We also recommend increasing the penalties that can be imposed by Customs and the courts in respect of falsely declared or uncleared cash movements, as well as providing Customs with the power to investigate whether a person has provided false or misleading information in connection with a BCR.

List of recommendations

49. The following is a list of all the recommendations for change we make in Part B of the report. The full text of the recommendation is outlined, as is whether implementing the recommendation requires one or more of the following:

- **a legislative change,** requiring amendments to the Act
- **a regulatory change,** requiring new regulations to be issued using powers in sections 153, 154, or 155 of the Act, or changes to one of the existing AML/CFT regulatory instruments. Changes marked with an asterisk (*) can be progressed at an earlier stage if required.
- **a code of practice,** such as amending the existing Identity Verification Code of Practice or issuing a new code using powers in section 64 of the Act
- **a Ministerial exemption** issued using the powers in section 157 of the Act
- **an operational change,** requiring changes to an agency/ies operational practices or an operational output, such as guidance or a risk assessment

Institutional arrangements

#	Recommendation	Type
Actively preventing money laundering and terrorism financing		
R1	Existing prevention-focused obligations in the Act should be further strengthened to ensure that, where it is appropriate, suspicious or risky transactions are stopped to reduce the ability for illicit money to enter or flow through the financial system.	Legislative, regulatory *
R2	Introduce, subject to a cost-benefit assessment, additional prevention-focused obligations, such as requiring enhanced customer due for certain types of high-risk transactions, such as cash transactions over a certain threshold or cash deposits into third party accounts.	Legislative, regulatory *
R3	If it is necessary to implement any additional obligations or powers identified, consider changing the purpose of the Act to include prevention of money laundering and terrorism financing.	Legislative
Supporting the implementation of financial sanctions		
R4	Amend the purpose of the Act to include "supporting the implementation of financial sanctions".	Legislative
Countering proliferation financing		
R5	Amend the Act to include "combatting proliferation financing" as a general purpose.	Legislative
Ensuring a risk-based approach is taken		
R6	Amend the purpose of the Act to include explicit reference to implementation of the Act using a risk-based approach.	Legislative

#	Recommendation	Type
Contributing to public confidence in the financial system		
R7	Insert a new subsection that outlines the intended outcomes of the Act. This section should state that the outcomes of the Act are that it contributes to combatting financially motivated crimes, maintains and enhances New Zealand's international reputation, and contributes to public confidence in, and transparency of, the financial system.	Legislative
R8	Remove "contribute to public confidence in the financial system" as a purpose of the Act and remove "maintain and enhance New Zealand's international reputation" from section 3(1)(b).	Legislative
Framework for understanding and sharing risk information		
R9	In the long term, amend the Act to provide for the National Coordination Committee to request that an agency produce a risk assessment with the specific requirements for the risk assessment, including scope, approach, methodology, and timeframes for completion.	Legislative
R10	Develop a framework for sharing more dynamic and/or live risk information with the private sector and/or within the private sector, such as through establishing an information sharing mechanism with appropriate safeguards and protections.	Legislative, regulatory
R11	In the interim, agencies should review the content and format of risk assessments with a business-focused lens and explore opportunities for increased private sector involvement in the production of risk assessments.	Operational
Business risk assessment requirements		
R12	Amend section 58 to improve clarity and distinguish between factors relevant to some businesses versus those relevant to all businesses.	Legislative
R13	As part of amending section 58, require businesses to assess their general risk of sanctions evasion, including proliferation financing sanctions.	Legislative
R14	Supervisors should further update risk assessment guidance to address areas of uncertainty and ambiguity and consider including examples of best practices where appropriate.	Operational
Balancing prescription with risk-based obligations		
R15	Issue any further regulatory exemptions to tailor obligations for low-risk products, businesses, and transactions, as well as opportunities for making greater use of simplified CDD	Regulatory
R16	Agencies should issue further and more detailed or granular guidance to empower businesses in applying a risk-based approach. Agencies should, in consultation with the private sector, identify areas where more guidance is needed and prioritise their efforts accordingly	Operational
Capacity of smaller and larger reporting entities		
R17	Create a centralised source of AML/CFT information and resources that consolidates all information from the Ministry, AML/CFT supervisors, and FIU.	Operational

#	Recommendation	Type
R18	Develop further tools and resources designed to assist small businesses in complying with their obligations and that are accessible to a range of audiences (e.g., translating guidance, ensuring simple language is used, complying with accessibility standards).	Operational
R19	Explore amending the Act to provide for an accreditation or certification process for technological solutions to make it easier for businesses to identify what products will be useful. In the interim, the AML/CFT supervisors should issue guidance about how businesses can use technology.	
Coordinating within the regime and between other regimes		
R20	Invite further regulatory, law enforcement, and intelligence agencies to join the NCC to enhance the coordination of efforts with complementary regimes.	Operational
Supervisory structure		
R21	In the long term, explore whether an alternative approach to supervisory arrangements would address issues related to risk-based approach to supervision, supervisory consistency, and the ability for complaints to be resolved.	Legislative
R22	In the short term, explore options for ensuring that NCC is able to resolve issues of inconsistency and decide how the law should be applied given its statutory responsibility of facilitating good practices and consistent approaches to AML/CFT supervision (section 152(e)).	Operational
Ensuring FIU independence to deliver AML/CFT services		
R23	Amend the Act to constitute the FIU as distinct entity from the Police to improve accountability against legislative functions	Legislative
R24	As part of changing how the regime is resourced, agencies should explore how to ensure stewardship and strategic functions are sufficiently resourced (see Recommendation R29).	Operational
Position of the FIU within the regime		
R25	As part of exploring alternative approaches to the structure or framework of the regime, explore changing the position of the FIU within the regime.	Operational
Policy and administration		
R26	As part of considering an alternative institutional framework for the AML/CFT regime, consider options for co-administration if this would result in prompter reform, better linkages with complementary regimes and improved or more well-rounded policy advice.	Legislative
The role of the private sector		
R27	Formalise and consolidate the existing advisory group arrangements to increase the amount of private sector input into the operation and governance of the AML/CFT regime. Agencies should ensure that the regime-wide advisory group is sufficiently representative and transparently operated.	Operational
Ensuring there are sufficient resources to deliver the regime		
R28	As part of considering an alternative institutional framework for the AML/CFT regime, seek increases to the baseline appropriations for agencies. The necessary increase would depend on whether any changes are progressed to consolidate or centralise functions, as this would likely reduce the resourcing needs of the regime.	Operational

#	Recommendation	Type
R29	Amend the Act to establish a hybrid public/private funding model to partially support the regime's operation, subject to further consultation on the viability of the model and how it would work in practice.	Legislative
Potential alternative approaches to agency structure		
R30	Further explore alternative approaches to agency structure to determine whether any other approaches would result in the regime being more effective and efficient. This should include conducting a cost-benefit analysis of any alternative model(s) as well as an assessment of transition costs for the regime.	Legislative
Supervising the implementation of targeted financial sanctions		
R31	Include supervision of implementation of financial sanctions within the scope of the existing AML/CFT supervisor responsibilities (noting that additional funding would be sought to support this function).	Legislative
Inspecting businesses that operate from home		
R32	Amend the Act to state that an onsite inspection may be conducted at the part of a dwellinghouse (i.e., home office space) that is used to provide a captured activity.	Legislative
Remote inspections		
R33	Amend section 132 of the Act to explicitly allow supervisors to utilise virtual tools, such as video conferencing technology, when appropriate and subject to technical and data security considerations, as part of their supervision and monitoring a reporting entity's compliance with the Act. Employees, officers, or agents should be advised of the right not to answer a question if the answer would or could incriminate them (to align with the onsite inspection requirement of section 133(3)).	Legislative
Allowing information to be requested from other businesses		
R34	Subject to further exploration of how such a power could be exercised appropriately, amend the Act to provide a power that enables the FIU to request information from non-reporting entities and requires them to supply the information.	Legislative
Providing for ongoing monitoring of transactions and accounts		
R35	Explore, in consultation with the Privacy Commissioner, what appropriate safeguards might need to be applied should the FIU be provided with the power to request ongoing information relevant to high-risk individuals.	Operational
R36	Subject to appropriate safeguards being available, amend the Act to allow the FIU with appropriate powers to request ongoing information.	Legislative
Freezing or stopping transactions to prevent harm		
R37	Explore, in consultation with the Privacy Commissioner, what appropriate safeguards might need to be applied should the FIU be provided with the power to freeze accounts and/or block transactions for the purposes of determining whether criminal activity is occurring.	Operational
R38	Subject to appropriate safeguards being available, amend the Act to provide the FIU with the appropriate powers to freeze accounts and/or block transactions in appropriate circumstances.	Legislative

#	Recommendation	Type
Secondary legislation making powers generally		
R39	Adjust secondary legislation making powers to ensure that secondary legislation can be efficiently issued and administered. This adjustment should reflect any changes to the institutional arrangements of the regime and could result in new types of secondary legislation being issued (e.g., AML/CFT rules) or agencies being given new powers to make or amend secondary legislation.	Legislative
Forms and reports prescribed by the Act under section 153		
R40	Amend the report and form making power in section 153(1)(b) to delegate the ability to make or amend forms to the appropriate operational decision makers with the appropriate safeguards and oversight.	Legislative
Making or amending codes of practice under section 64		
R41	Noting the general recommendation regarding secondary legislation (see Recommendation R40), amend the Act's framework for codes of practice to ensure the framework is useable, provides enough flexibility and scope for innovation for businesses towards meeting AML/CFT obligations, while also providing assurance of minimum requirements and mitigating risks.	Legislative
Stewardship of the Ministerial exemptions regime		
R42	Subject to securing sufficient resourcing, progress options to enhance the stewardship of the Ministerial exemption regime (subject to further engagement), including identifying more regulatory and class exemptions, introducing some form of light-touch supervision of exempt entities, reviewing how obligations should be exempted and clarifying the approach to expired exemptions, and proving avenues beyond judicial review if an exemption application is declined.	Operational, legislative
Application process for Ministerial exemptions		
R43	Progress options to streamline and provide clarity to the application process for Ministerial exemptions including publishing clear guidance, creating a standard application process, simplifying the reapplication process, and setting fixed timeframes for processing exemptions.	Operational
R44	If it is required to ensure there are sufficient resources to process applications for exemptions, amend the Act to charge applicants a fee subject to further engagement and sufficient operational improvements being made.	Legislative
How decisions are made to grant or decline a Ministerial exemption application		
R45	Review factors in section 157(3) to ensure they are clear and given the appropriate weight as part of making a decision. This would include specifying what risk is assessed i.e., the business' risk or the risk associated with the exemption and clarifying that only low-risk entities can be granted exemptions.	Legislative
Direct data access to FIU information for other agencies		
R46	Issue regulations to support a direct data access arrangement for RBNZ, FMA, DIA and Customs, following consultation with the Privacy Commissioner.	Regulatory *
R47	Once direct data access is embedded, consider extending the arrangement to other regulatory, intelligence, and law enforcement agencies who are able to demonstrate their need to access the information.	Regulatory

#	Recommendation	Type
De-risking		
R48	Request that the AML/CFT supervisors develop a code of practice for businesses (particularly banks) to rely on when onboarding high-risk businesses and customers, including remitters.	Code of practice
Financial exclusion		
R49	Explore whether there are any further regulatory exemptions needed to address financial inclusion challenges in the event that broader changes to CDD requirements still result in instances of financial inclusion.	Regulatory

Scope of the Act

#	Recommendation	Type
Ensuring illicit capital cannot enter the real estate market		
R50	Agencies, particularly FIU and DIA, undertake further analysis to assess the money laundering and terrorism financing risks in the real estate sector to identify the particular methods or typologies that are being used to place, layer, or integrate the proceeds of crime through real estate and which sectors or businesses would have visibility of or exposure to those typologies.	Operational
R51	Following the risk assessment, consider whether any further AML/CFT controls to prevent/deter this from happening. This could include additional obligations for real estate agents and law firms (e.g., by imposing additional requirements for private sales, on selling, list and sell, measures where nominees are used for purchases, risks associated with non-finance or privately funded purchases and increasing cooperation between the parties involved).	Regulatory, legislative
Obligations for businesses to combat TBML		
R52	Agencies, particularly FIU and Customs, conduct a risk assessment and general analysis of the trade finance system to identify the extent of TBML that may be occurring in New Zealand as well the businesses that are involved in activities that are at risk of being misused for TBML. This analysis should then be used to inform future advice regarding the costs and benefits of including any new sectors or activities within the AML/CFT regime.	Operational
Enhancing intelligence collection and sharing for TBML, including data-matching		
R53	As part of the analysis of the trade finance system, agencies should also identify what intelligence should or could be collected to enhance detection of TBML, as well as whether any FIU data should be matched with trade data to enhance transparency of the trade and trade finance system.	Legislative, operational
Providing a clear definition of a Virtual Asset Service Provider (VASP)		
R54	Include virtual asset service providers as a type of reporting entity, in line with the definition provided by the FATF. This should be achieved initially through issuing regulations, and then the definition should be included in the Act itself.	Regulatory *
Ensuring occasional virtual asset transactions are captured appropriately		
R55	Issue regulations to declare all virtual asset transactions at or above NZD 1,000 at the time of the transaction as occasional transactions, including virtual asset to virtual asset transfers.	Regulatory *

#	Recommendation	Type
Implementing the FATF's travel rule to improve transparency and traceability		
R56	Issue regulations that require all virtual asset transfers to be considered international wire transfers *unless the entity is satisfied otherwise*, with	Regulatory *
Definition of "high-value dealer"		
R57	Review the list of articles in the definition of an HVD to consider whether it should be removed or amended in order to be further strengthened or clarified.	Legislative
R58	Amend the Act to remove the phrase "in the ordinary course of business" from the definition of a high-value dealer. This will set the capture point as an HVD as any business that transacts in cash over the relevant threshold. In the interim, AML/CFT supervisors should produce guidance which provides a clearer interpretation of "in the ordinary course of business".	Legislative
R59	Conduct a risk assessment to understand the potential money laundering risks of non-cash transactions for high-value articles and explore whether applying some form of obligations to such transactions is necessary and, if so, the amount at which the threshold should be set.	Operational, legislative
R60	Amend the Act to remove the exclusion for industrial dealers in precious metals and stones.	Legislative
R61	Amend the exemption to no longer apply to pawnbroker activities that meet the definition of HVDs and clarify that pawning is not captured under the Act as providing a loan.	Regulatory *
Appropriate cash transaction threshold		
R62	Retain the current NZD 10,000 threshold for high-value dealers but revaluate whether the threshold should be lowered once other recommended changes to high-value dealer obligations have been implemented.	Regulatory
High value dealer obligations		
R63	Amend the Act to increase obligations for HVDs. At minimum, HVDs should have a mandatory SARs obligation, and other obligations should be imposed if they are necessary to combat risks. However, any additional obligations should be tailored, if possible, to reflect the nature of the sector.	Legislative
"In the ordinary course of business"		
R64	Review the intended meaning of "in the ordinary course of business" in section 5 with a view to amending or defining the phrase. Analysis should be undertaken to understand the risks associated with obligations that only apply if an activity is conducted in the ordinary course of business. Depending on this analysis, amendments to the Act should be made to provide clarity to DNFBPs around their obligations if they only undertake certain activities infrequently.	Legislative
Businesses providing multiple types of activities		
R65	Amend the Act to remove the term "only to the extent that" from section 6(4). In the meantime, issue regulations to clarify that a reporting entity that undertakes captured activities other than relating to its category of reporting entity must comply with the Act.	Legislative, regulatory *

#	Recommendation	Type
Overlap between "managing client funds" and financial institution activities		
R66	Issue regulations to exclude from the definition of TCSP, any person, whose only activity is a DNFBP activity (iv) if that person is already captured by the Act as a financial institution. This should then be changed in the Act itself.	Regulatory
"Sums paid as fees for professional services"		
R67	Issue regulations to explicitly limit the exclusion "of sums paid as fees for professional services" in the definition of managing client funds as being the DNFBP's own professional fees. This should then be changed in the Act itself.	Regulatory
"Engaging in or giving instructions"		
R68	Amend the definition of DNFBP activity (a)(vi), including the phrase 'engaging in or giving instructions', to clarify those activities that are required to be subject to this DNFBP activity. Note that this DNFBP activity is intended to apply to circumstances where a DNFBP has no direct involvement in managing a customer's funds, acting as a nominee or trustee, or undertaking real estate agency work.	Legislative
R69	In the interim, issue regulations to provide clarity around the scope of this activity, such as its application to processing and preparing invoices (other than when also managing client funds) or involvement in real estate transactions (other than when undertaking real estate agency work).	Regulatory
Definition of financial institution activities		
R70	Coordinate with MBIE and determine whether the *Financial Service Providers (Registration and Dispute Resolution) Act 2008* and/or the Act can be amended to ensure the terminology used to define financial activities are completely aligned with the FATF Standards.	Operational
Stored value instruments		
R71	Amend the definition of stored value instruments in the *AML/CFT (Definitions) Regulations 2011* to be technology neutral to capture electronic or digital forms of stored value.	Regulatory *
Other businesses that could provide financial intelligence		
R72	Review whether there is benefit in including fintech providers offering open banking solutions and commerce or marketplace operators as reporting entities. This analysis should also include a comparison with other financial services related legislation to ensure consistency. Subject to the analysis, include them as a type of financial institution in the Act and implement appropriate AML/CFT obligations to align with their role in the financial system. This could be implemented by issuing regulations or by amending the Act.	Regulatory, legislative
Acting as a secretary of a company or partner in a partnership		
R73	Maintain the status quo and do not include acting as company secretary within the scope of the Act.	Nil
Criminal defence lawyers		
R74	Maintain the status quo and do not include criminal defence lawyers within the scope of the Act.	Nil

#	Recommendation	Type
Non-life insurance businesses		
R75	Maintain the status quo and do not include non-life insurers within the scope of the Act.	Nil
Non-profit organisations vulnerable to terrorism financing		
R76	Maintain the status quo and do not include non-profit organisations which are not registered charities and non-resident tax charities within the scope of the Act. Agencies will continue to explore alternative options for increasing the monitoring or supervision of the charities.	Operational
Internet auctioneers and online marketplaces		
R77	Revoke Regulation 21A of the *AML/CFT (Definitions) Regulations 2011* which excludes internet auction providers from the Act, including online marketplaces	Regulatory *
R78	Explore whether to issue an appropriate exemption for some AML/CFT obligations based off a risk assessment for online marketplaces if there are aspects which are demonstrably low risk.	Regulatory
Special remittance card facilities		
R79	Revoke Regulation 10 of the *AML/CFT* (*Exemptions*) *Regulations 2011* which provides a limited exemption for special remittance cards, subject to final confirmation that it is no longer in use.	Regulatory *
Non-finance businesses which transfer money or value		
R80	Explore amendments to Regulation 18A *AML/CFT (Definitions) Regulations 2011* to clarify its scope, including the option of limiting the exclusion from being a financial institution under the Act.	Regulatory *
Workplace savings retirement schemes		
R81	Explore whether any amendments should be made to Regulation 20A of the *AML/CFT (Exemptions) Regulation 2011* regarding workplace savings retirement schemes. This should involve assessing the risks associated with workplace savings retirement schemes and whether the existing settings are in line with those risks, as well as the impact to the broader sector that could result from any changes.	Regulatory *
Non-court appointed liquidations		
R82	Review the application of the Act to non-court appointed types of liquidation with a view to exempting some AML/CFT obligations that are incompatible with the nature of the liquidator's work, while also ensuring other AML/CFT requirements are appropriate to the money laundering and terrorism financing risks faced in the sector.	Regulatory
Acting as a trustee or nominee		
R83	Issue a regulatory exemption for companies that act as a trustee or nominee and are controlled by a parent reporting entity in New Zealand (that has full AML/CFT responsibilities for activities of the nominee or trustee company), subject to further engagement with the sector to determine how control should be defined and the appropriate amount of oversight that the parent reporting entity should maintain over the companies.	Regulatory *

#	Recommendation	Type
Crown entities, Crown agents etc		
R84	Issue a regulatory exemption for Crown entities, agents etc that applies where the Crown is the sole customer of the activity and where they are using public funds to provide loans to the public. The exemption should include appropriate conditions in respect of the latter activity, such as prohibiting loans being paid off early or through cash and requiring the entity to be subject to sufficient public accountability mechanisms.	Regulatory *
Low-value loan providers		
R85	Issue a Ministerial class exemption for registered charities providing loans to customers below where the maximum amount that can be loaned to a customer is no more than NZD 6,000. This exemption should include conditions which limit the loans to one per customer and restrict the ability to repay loans quickly and in cash.	Ministerial exemption
Application of Act to real estate agents for commercial leasing		
R86	Review the level of risk associated with commercial leasing and consider regulations to reduce or amend AML/CFT obligations for real estate agents to align with the risks, or exempt commercial leasing from the Act. This risk assessment should consider whether some AML/CFT obligations should apply to commercial lessees.	Operational, regulatory
Other exemptions		
R87	In line with other recommendations regarding the risk-based approach and financial inclusion, agencies should continue to work through the suggestions for exemptions and assess the money laundering and terrorism financing risks associated with the proposals.	Regulatory, Ministerial exemption
Territorial scope		
R88	Conduct further analysis of potential approaches for defining the Act's territorial scope, including the initially preferred approach of defining the scope to include overseas businesses which provide activities to New Zealand above a prescribed threshold. Agencies should also consider the appropriateness of any exemption regime which could apply where the business is based in a jurisdiction with equivalent AML/CFT controls and sufficient levels of international cooperation with New Zealand.	Legislative
R89	In the interim, supervisors should review and update the existing territorial scope guidance to ensure it is sufficiently clear, appropriate, and consistent with similar guidance produced by other agencies in relation to other regulatory regimes.	Operational

Supervision, regulation, and enforcement

#	Recommendation	Type
Registration for all reporting entities		
R90	Further develop and progress options for AML/CFT reporting entity registration so that supervisors have visibility of their supervised populations and consistent fit and proper or criminal record checks adequately prevent businesses being owned or controlled by criminals or their associates This should include further engagement with relevant agencies and the private sector.	Legislative

#	Recommendation	Type
R91	For sectors registered or licensed by peak bodies or government agencies (other than RBNZ and FMA), develop options to ensure the AML/CFT supervisor and the FIU are notified that a business is a reporting entity.	
AML/CFT licensing for some reporting entities		
R92	Subject to further engagement (particularly regarding costs), amend the Act to include an AML/CFT licensing framework for high-risk sectors (that are not licensed under other legislations). Licensing should be undertaken by the AML/CFT supervisor or another appropriate body and be a pre-requisite for registration on the FSPR to provide the relevant service.	Legislative
Regulating independent auditors		
R93	Request that the AML/CFT supervisors develop code of practice that sets out more explicit provisions for an independent audit to comply with the requirements of the Act,	Code of practice
R94	For the longer term, and subject to review of the impact of Recommendation R93 above, consider whether additional measures are required to regulate auditors and independent audits. This could include amending the Act to state an audit must test the effectiveness of an AML/CFT programme, allow creation of auditor standards, a registration, accreditation or licensing framework and	Legislative
Regulating consultants		
R95	Remain with the status quo and do not regulate consultants in the Act.	Nil
Regulating agents		
R96	Request the AML/CFT supervisors develop guidance to clarify the different circumstances and types of agents that can be used by reporting entities under the Act.	Operational
R97	Require a reporting entity to do the following by issuing regulations: • include PPCs in its AML/CFT programmes for training and vetting of agents. • include PPCs in its AML/CFT programmes for all AML/CFT functions undertaken by an agent on its behalf (including identifying grounds under section 31(2)(b) for reporting a SAR). • maintain a list of its agents (as part of its AML/CFT programme). The list of agents must be provided to the AML/CFT supervisor on request.	Regulatory *
R98	For the longer term, if these recommendations do not provide sufficient clarity or effective controls regarding the use of agents, consider if further regulations or amendments to the Act are required. For example, this could define and explicitly prescribe the different AML/CFT functions that an agent is able to undertake for a reporting entity and liability for compliance.	Legislative, regulatory
Range of offences in the Act		
R99	Create new offences for reporting entities obstructing the FIU (consistent with section 102) or knowingly or recklessly providing the FIU with false information (consistent with section 103) following a request under section 143.	Legislative
R100	Amend the structuring offence in section 101 to include structuring any non-transaction-based AML/CFT obligations (e.g., using a false identity or other document to avoid AML/CFT obligations).	Legislative

#	Recommendation	Type
R101	Create a new offence for knowingly or recklessly structuring a legal person or legal arrangement to avoid or obstruct inquiries into the beneficial ownership of the legal person or arrangement.	Legislative
Allowing for intermediary enforcement options		
R102	Amend the Act to enable infringement notices to be issued in appropriate circumstances (e.g., failure to provide annual report on time, failure to have an AML/CFT programme).	Legislative
R103	Enable AML/CFT supervisors to restrict, suspend, or cancel a business' AML/CFT or prudential licence or registration (and/or request the relevant registration or licensing authority to do so) following AML/CFT non-compliance.	Legislative
R104	As part of implementing Recommendation R103, agencies should conduct further engagement with the relevant agencies and bodies which are responsible for maintaining and administering the regimes under which reporting entities are licensed or registered to ensure that the overall regulatory regime is cohesive and coherent.	Legislative
Allowing for higher penalties at the top end of seriousness		
R105	Amend the Act to increase available penalties ensuring they are able to be proportionate to the level of non-compliance and appropriate to the size or nature of the business. This could be achieved by increasing the maximum penalties available or prescribing different maximum penalties depending on the size or the type of business.	Legislative
Ensuring penalties are risk-based and proportionate		
R106	Amend the Act to prescribe a non-exhaustive list of AML/CFT-specific aggravating and mitigating factors that need to be considered when applying penalties, such as the gravity and duration of the breach, compliance history, the extent of any reliance on advice in good faith, and a consideration of the consequences of the breach on the broader AML/CFT system.	Legislative
Sanctions for employees, directors, and senior management		
R107	Extend civil sanctions to directors, senior managers, employees, and agents in appropriate circumstances, such as where they were responsible for making the decision that resulted in the business not complying with their AML/CFT obligations.	Legislative
R108	Provide a statutory defence for compliance officers where they have acted in good faith, but the reporting entity has not complied with their AML/CFT obligations.	Legislative
Time limit for prosecuting AML/CFT offences		
R109	Extend the time limit for prosecuting AML/CFT offences from three years to seven years.	Legislative
Liquidation following non-payment of AML/CFT Penalties		
R110	Amend section 132(2) to clarify supervisors' standing to recover penalties and costs awarded in proceedings undertaken under the Act.	Legislative
R111	As part of the above amendments, make a consequential change to section 241(2)(c) of the *Companies Act 1993* to include "if the company is a reporting entity under the *Anti-Money Laundering and Countering Financing of Terrorism Act 2009,* the AML/CFT supervisor for the company."	Legislative

#	Recommendation	Type
R112	Include a new section 90A of the Act to align with the approach to recovery of penalties to that of other enactments permitting the recovery of pecuniary penalties and state "if the court orders that a person pay a pecuniary penalty, the court must also order that the penalty must be applied first to pay the AML/CFT supervisor's actual costs in bringing the proceedings."	Legislative

Preventive measures

#	Recommendation	Type
Identity Verification Code of Practice (IVCOP)		
R113	Request the AML/CFT supervisors review and replace the IVCOP with a new code of practice setting out best practice verification requirements in relation to name and date of birth. This should review provisions for face-to-face verification, use of certified copies and electronic identity verification. The review and implementation of the new code of practice should be completed by and aligned with the implementation of the Digital Identity Services Trust Framework.	Code of practice
Verifying address information		
R114	Issue regulations to exempt the address verification requirement for all customers, beneficial owners and persons acting on behalf of a customer other than when enhanced CDD is required. As part of this process, and for customers requiring standard CDD, consider whether regulations should be introduced requiring businesses to verify an address as genuine according to the level of risk. These changes should then be amended in the Act itself.	Regulatory *
Unavailability of independent verification sources		
R115	Issue regulations stating that in circumstances when it is not possible to verify required information regarding legal persons or legal arrangements from a reliable or independent source, it is possible to use reliable (but not independent) verification data, documents, or information. This does not apply to biographical information or information regarding source of wealth or source of funds.	Regulatory *
Beneficial ownership register(s)		
R116	Review and amend the definition of beneficial owner in the Act. This should include coordination with MBIE and alignment with the definition to be used for the beneficial ownership register for legal persons. As part of this process: • Ensure the definition applies to persons with ultimate ownership or control, and only applies to POWBATICs if they exercise indirect ownership or control over the customer. • Consider whether there is a need to also prescribe certain types of persons who must be identified/verified for legal arrangements (e.g., settlors or protectors of trusts, nominees in relation to legal persons). • Review the potential use of the beneficial ownership register by reporting entities to meet AML/CFT requirements. This includes identifying those low-risk situations where reporting entities may be able to rely wholly on the register compared to situations where additional beneficial ownership verification may be required	Legislative

#	Recommendation	Type
R117	Concurrent to the above, agencies should undertake further work to explore the feasibility of a register of beneficial ownership of trusts and legal arrangements. This should include consideration of use of the register for reporting entities to assist meeting AML/CFT obligations in relation to trusts and legal arrangements.	Legislative
R118	Issue regulations to clarify that the definition of beneficial owner includes a person with ultimate ownership or control, and only applies to a POWBATIC that meets this threshold, whether directly or indirectly.	Regulatory *
R119	Revoke Regulation 24 (Exemptions) in relation to trust accounts.	Regulatory *
R120	Review whether the Managing Intermediaries Exemptions remain necessary and amend or revoke if they are not.	Ministerial exemption
Specific information for legal persons and legal arrangements		
R121	Issue regulations requiring reporting entities to obtain information about legal form and proof of existence, ownership and control structure, and powers that bind and regulate, and verify this information according to the level of risk. These changes should then be amended in the Act itself.	Regulatory *
Source of wealth or source of funds, additional enhanced CDD measures		
R122	Review whether the current sections 23 and 24 enhanced CDD requirements are appropriate or require amendment. This should include consideration of whether businesses should be required to take further additional measures in addition to, or instead of, the current source of wealth or funds requirements in order to manage and mitigate the risk their customers present. As part of this, consider whether the Act should also be amended to differentiate between the requirement to obtain and verify source of wealth or source of funds as is required to mitigate identified money laundering and terrorism financing risks.	Legislative
R123	Issue regulations to require a business to differentiate when information must be obtained and verified regarding source of wealth or source of funds, or both, as is required to mitigate the risks.	Regulatory *
R124	Issue regulations to require a business to implement any additional enhanced CDD measures at the start and for the duration of a business relationship as are required to mitigate the risks.	Regulatory *
Mandatory enhanced CDD for all trusts		
R125	Review whether mandatory CDD remains necessary for all customers that are trusts or other vehicles for holding personal assets. If not, repeal sections 22(1)(a)(i) and 22(1)(b)(i) of the Act.	Legislative
R126	In the interim, implement Regulations to prescribe a process for conducting enhanced CDD on trusts, including identifying types of trusts that are suitably low risk and other factors to consider when assessing the level of risk. If certain low-risk criteria are met, an exemption from verification requirements should apply. This should be accompanied by guidance from supervisors regarding a risk-based approach.	Regulatory *

#	Recommendation	Type
Conducting customer due diligence in all suspicious circumstances		
R127	Issue regulations (pursuant to section 14(1)(d)) so that CDD must be conducted if a person seeks to conduct an activity or transaction through a reporting entity that is outside a business relationship and not an occasional transaction or activity. This obligation arises in any circumstances where there may be grounds to report a suspicious activity as per section 39A of the Act.	Regulatory *
Avoiding tipping off		
R128	Issue guidance around the use of enhanced CDD (s22(1)(c) and (d)) to assist in determining grounds for suspicion, the prohibitions under section 37 and the Act's tipping off provisions relating to the existence of a SAR, to ensure these requirements are understood by reporting entities.	Operational
R129	Repeal section 22A of the Act.	Legislative
R130	Review the current circumstances in which a lower level of CDD is permitted to avoid alerting the customer to potential law enforcement interest. Consider if there are grounds to expand this, for example in relation to bank accounts in some circumstances.	Regulatory
Eligibility for simplified CDD		
R131	Undertake a review to identify further categories of customer and any products or services where the money laundering and terrorism financing risk is sufficiently low to enable simplified CDD. Issue regulations to allow simplified CDD measures for these situations. These changes should then be amended in the Act itself.	Regulatory, legislative
Conducting simplified CDD on persons acting on behalf of large organisations		
R132	Issue regulations enabling a senior manager of a customer (that has been identified and verified in accordance with sections 19-20) to delegate authority to employees to act on behalf of the customer by electronic means. The senior manager must provide the delegated employees' authorised contact details (e.g., email address) to the reporting entity, with the reporting entity then exempt identifying and verifying the full name and date of birth for those delegated employees. These changes should then be amended in the Act itself.	Regulatory *
Risk-rating of customers		
R133	Issue regulations to include an explicit requirement that reporting entities risk-rate new customers (including consideration of guidance issued by supervisors). This risk rating must then be considered and updated as part of ongoing CDD and account monitoring of a business relationship. These changes should then be amended in the Act itself.	Regulatory *
Updating CDD information and account monitoring, including for existing customers		
R134	Issue regulations to clarify that the requirement of section 31(4)(a) and (b) to review a customer's account activity, transaction behaviour and CDD information (or for an existing customer, other information held) is according to the level of risk involved. This should then be amended in the Act itself.	Regulatory *

#	Recommendation	Type
R135	Introduce an additional ongoing CDD requirement to update (for a post-Act customer) or obtain (for an existing customer) CDD information if required. This should be a risk-based requirement, also considering the timing when CDD was last conducted. Appropriate wording should be developed in consultation with the private sector, covering requirements for post-Act and existing customers respectively. These requirements should be introduced through regulations initially and then be amended in the Act itself.	Legislative, regulatory *
Monitoring non-financial activities		
R136	Issue regulations of the Act to state "regularly review any customer's activities described in the definition of designated non-financial business or profession in section 5(1) of the Act." These changes should then be enacted in section 31 of the Act.	Regulatory *
Beneficiaries of life and other investment-related insurance		
R137	Retain the status quo and do not impose any additional requirements for beneficiaries of life insurance policies.	Nil
Definition of customer		
R138	Issue regulations to prescribe that when establishing a facility for a trust, the relevant trust is the customer (and not the trustees who may be the facility holder).	Regulatory *
R139	Issue regulations to prescribe appropriate CDD obligations for the formation of a legal person or legal arrangement. This should include a requirement to identify and verify the identities of the beneficial owners of the (to be formed) legal person or arrangement, as well as any person acting on their behalf.	Regulatory *
R140	Issue regulations to prescribe the customer as the relevant legal person or arrangement when acting or arranging for someone to act as a nominee director, nominee shareholder or a trustee.	Regulatory *
Managing funds in DNFBP trust accounts		
R141	Undertake a review of the money laundering and terrorism financing risks associated with DNFBP trust accounts and implement any additional AML/CFT requirements as required to mitigate the risks. This could include inclusion of an additional enhanced CDD requirement in the Act that a DNFBP must take any additional measures that may be needed to mitigate and manage the risks associated with managing funds in its trust account.	Operational, regulatory
R142	Issue regulations that state a non-client holding funds in a DNFBP's trust account is exempt from being a customer under the Act, except if the non-client is undertaking an occasional transaction.	Regulatory
R143	Review whether any additional occasional transactions are required in relation to transactions through DNFBP trust accounts by non-clients (e.g., funds received exceed what is expected, elevated level of risk, payments to third-parties).	Regulatory
Timing of CDD obligations within a DNFBP business relationship		
R144	Review and amend the Act to clarify the application of AML/CFT obligations in circumstances when a DNFBP has a repeat client but does not have ongoing instructions, activities or transactions occurring with a business relationship. Concurrently, review and clarify the point at which CDD is required by a DNFBP if a non-captured activity transitions to captured activity.	Legislative, regulatory *

#	Recommendation	Type
Record keeping		
R145	In consultation with the Privacy Commissioner, develop and issue further guidance which covers a) the extent to which legally privileged records can be requested by supervisors and auditors b) expectations on businesses to keep records of the document used to verify a person's identity and c) the application of relevant *Privacy Act 2020* principles, including the extent to which businesses should be destroying records.	Operational
R146	Amend the Act to clarify the timeframe within which businesses are required to comply with requests to produce records. This timeframe should be consistent with existing jurisprudence on the issue as well as the FATF's requirement that records are provided swiftly.	Legislative
R147	Reconcile record keeping requirements in the Act with other relevant legislation (e.g., *Tax Administration Act, Financial Markets Conduct Act*) to ensure businesses have consistent requirements to keep the same record under the various regimes.	Legislative
Transactions outside a business relationship		
R148	Revoke Regulation 8 of the *AML/CFT (Exemptions) Regulations 2011* applying to a transaction that occurs outside of a business relationship but is not an occasional transaction. The business would then have to keep records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold.	Regulatory *
Time limitation of the PEP definition		
R149	Extend the timeframe for which a person is considered a PEP from 12 to 24 months and require businesses to take a risk-based approach to determine whether a person should still be treated as a PEP after 24 months.	Legislative
Identifying whether a customer is a foreign PEP		
R150	Amend the current 'reasonable steps' requirement in section 26 to instead require businesses to have appropriate risk management systems in place to determine whether a customer or beneficial owner is a foreign PEP.	Legislative
When PEP checks should occur		
R151	Amend the Act to require PEP checks to be conducted at an appropriate time depending on the level of risk involved in the business relationship. For high-risk circumstances, this should result in PEP checks occurring before services are provided to the customer.	Legislative
R152	Undertake further analysis and then introduce regulations or amend the Act to prescribe types of business relationship or activities where PEP checks must be conducted before providing the service (e.g., before a company or trust is formed). As part of this, introduce regulations or amend the Act to specify that for an occasional transaction or activity, a PEP check is only required prior to the transaction or activity if information is received that clearly indicates the customer is a PEP.	Legislative
Mitigating the risks of a foreign PEP		
R153	Amend the Act to require senior manager *or* compliance officer approval to establish or continue a business relationship with a foreign PEP, and to take reasonable steps to obtain information and verify the source of wealth *and* source of funds of the foreign PEP.	Legislative

#	Recommendation	Type
Definition of a domestic or international organisation PEP		
R154	Amend the Act to include domestic PEPs in the definition of PEP. The definition should include a person holding a 'prominent function' within New Zealand, which should be prescribed appropriately (e.g., holding final approval over procurement processes above a certain level, decision making powers over subsidies or grants, or responsibility for budgetary spending). The definition should also prescribe a specific monetary threshold for the functions to ensure that only people with sufficient seniority meet the definition of a PEP.	
R155	Amend the Act to include international organisation PEPs in the definition of PEP. The definition should include a person entrusted with a prominent function by an international organisation (e.g., director, deputy director, and a member of the board or equivalent position).	Legislative
Identifying whether a customer is a domestic or international organisation PEP		
R156	Amend the Act to require businesses to take reasonable steps, according to the level of risk involved, to identify whether a customer or beneficial owner is a domestic or international organisation PEP.	Legislative
Mitigating the risks of a domestic or international organisation PEP		
R157	Amend the Act to require businesses to determine what, if any, additional measures are required to manage the risk of the domestic or international organisation PEP according to the level of risk involved with the relationship or transaction/activity.	Legislative
Supporting the implementation of financial sanctions		
R158	Agencies continue to explore through consultation what obligations are appropriate to support businesses in implementing their financial sanctions obligations, with the following obligations as a starting point: • a requirement for businesses to assess their exposure to potential breach, non-implementation, or evasion of sanctions obligations. • a requirement for businesses to include appropriate PPCs in their compliance programme which reflects their risk assessment and the nature of their business. • a specific requirement for businesses to ensure they are promptly notified about changes to sanctions lists, with the government providing a free solution that covers sanctions for terrorism, proliferation of weapons of mass destruction, and any other relevant sanctions in force. • an obligation for businesses to report what actions they have taken as a result of a sanctions notification (if any), including when attempted transactions are stopped. • developing a process for dealing with possible matches, with agencies confirming when a person is not a sanctioned individual and that assets can be unfrozen.	Operational
Correspondent banking		
R159	Amend section 29 to improve clarity, including by removing "effective" from section 29(2)(c). In addition, the requirements should apply to reporting entities in general, rather than just banks.	Legislative
R160	RBNZ should issue further guidance to clarify what is expected to meet correspondent banking requirements.	Operational

#	Recommendation	Type
Licensing of MVTS providers		
R161	Develop a licensing framework for MVTS providers (to potentially include currency exchange noting this is often provided alongside MVTS) that: • introduces fit and proper requirements (including to prevent MVTS providers being owned, controlled, or operated by criminals or their associates) and ensure only providers with sufficient AML/CFT capability are able to provide a MVTS service. • has appropriate and proportionate mechanisms for sanctioning non-compliance. This includes restricting or cancelling an ability to provide the service, as well as taking action against providers operating without a licence. Obtaining a licence should also be a pre-requisite for FSP registration.	Legislative
Agents of MVTS providers		
R162	As part of the development of a licensing framework, examine the role of agents in a MVTS provider's AML/CFT programme. This should include considering whether some AML/CFT obligations should be imposed directly onto agents, for example SAR reporting in circumstances where they have identified grounds for suspicion and whether sanctions for non-compliance could be imposed on an agent rather than the provider (if the provider had taken all reasonable steps to comply).	Legislative
Master agents and tipping off provisions		
R163	Introduce the following measures by regulations: • Exempt a master agent from being a reporting entity in relation to training, monitoring and other assurance activities undertaken for a network of sub-agents (on behalf of a MVTS provider). This is to clarify that in these circumstances, it acts on behalf of the principal MVTS provider (as part of the MVTS provider's AML/CFT programme). This is discrete from other circumstances when it may itself be an agent of a network provider or a reporting entity for separate financial services it provides. • Exempt a MVTS provider, its master agent and if necessary, a sub-agent, from tipping off restrictions under section 46, allowing them to share SAR information between themselves when necessary for the purposes of AML/CFT compliance.	Regulatory *
R164	In conjunction with Recommendations R161, R162, and R163 consider whether it is necessary to amend the DBG provisions for the MVTS sector or repeal them on the basis they are redundant.	Regulatory *
Submitting Suspicious Activity Reports		
R165	Issue regulations that MTVS providers, who control both the ordering and beneficiary end of a wire transfer, should consider information from both sides of the transfer to determine whether a SAR is required. If so, the SAR should be submitted to the FIU in any countries affected by the suspicious transfer.	Regulatory *
Mitigating the risks of new technologies		
R166	Issue regulations to require businesses to assess the money laundering and terrorist financing risks associated with new products and new business practices. The risk assessment should consider new delivery mechanisms, as well as the use of new or developing technologies for new and existing products. The risk assessment must be conducted before the technology or product is used.	Regulatory *

#	Recommendation	Type
Terminology involved in a wire transfer		
R167	Repeal and, in consultation with the private sector, replace all wire transfer terminology with appropriate terms that reflect the reality of wire transfers.	Legislative
R168	In the short term, explore whether regulations should be issued to carve in or out various transactions as wire transfers and ensure appropriate obligations for the parties involved. In particular: • issue regulations to ensure all transactions occurring within an include all forms of informal MVTS systems are subject to the wire transfers provisions, • examine whether 'Original Credit Transactions' should be included prescribed as wire transfers, and • consider whether BPAY and other similar payment systems should be excluded from the wire transfer provisions on the basis of a low risk of money laundering and terrorist financing.	Regulatory *
Ordering institutions		
R169	Issue regulations to require ordering institutions to obtain and transmit name and account or transaction numbers for an originator and beneficiary of an international wire transfer below NZD 1,000. The regulation should specify that this information does not need to be verified unless there may be grounds to report a SAR.	Regulatory *
R170	Amend the Act to explicitly prohibit executing international wire transfers where the required information regarding the originator and beneficiary does not accompany the transfer.	Legislative
Intermediary institutions		
R171	Issue regulations to require intermediary institutions in New Zealand to include in their compliance programme the reasonable steps they will take to identify wire transfers lacking required information and the risk-based policies and procedures they will apply when a wire transfer lacking the required information is identified.	Regulatory *
R172	Issue regulations to require intermediary institutions to keep records for five years where technological limitations prevent the relevant information about the parties from being transmitted with a related domestic wire transfer.	Regulatory *
R173	Amend the Act to require intermediary institutions to retain the information about the parties with the wire transfer, rather than provide it as soon as practicable after the transaction occurs.	Legislative
Beneficiary institutions		
R174	Issue regulations to require beneficiary institutions to specify in their compliance programme the reasonable steps they will take to identify international wire transfers lacking required originator and beneficiary information. These measures should be risk-based and can include post-event or real time monitoring where feasible and appropriate.	Regulatory *
Reliance on other reporting entities		
R175	Undertake further analysis to consider circumstances in which duplication of CDD across multiple reporting entities can be reduced. This could include information sharing mechanisms that comply with section 33 requirements, including leveraging the beneficial ownership register and the Digital Identity Services Trust Framework to assist compliance with the Act.	Operational

#	Recommendation	Type
R176	Issue regulations pursuant to section 33(2)(e) to require the relying party to consider the level of country risk if the relied-on party is not in New Zealand.	Regulatory *
R177	Issue regulations pursuant to section 33(2)(e) to require the relying party to take steps to satisfy itself that the relied-on party has record keeping measures in place and will make verification information available as soon as practicable on request, but within five working days.	Regulatory *
"Approved entities" and liability for reliance		
R178	Undertake further analysis to determine whether the approved entity settings are viable, and if so, identify those circumstances in which it could be used and activate its use. If not, the provisions should be repealed.	Legislative
Role of a DBG within New Zealand's AML/CFT framework		
R179	Undertake a review of the Act's DBG provisions, including whether they are fit-for-purpose, mitigate money laundering and terrorism financing risk and provide cost saving for businesses. This should inform whether any changes are required, including considering an alternate option of prescribing group-wide compliance requirements (within which businesses are able to rely on each other for CDD and other AML/CFT functions) without need for an upfront election process, eligibility to form, supervisor consideration etc.	Legislative
Criteria for forming a DBG		
R180	In conjunction with the recommendation above, undertake a review of the appropriate eligibility criteria for financial institution and DNFBP DBGs respectively. If DBG provisions are to be repealed and replaced by prescribing requirements at a group level, consider whether separate provisions are required for reliance within a group of DNFBPs that is broader than the FATF Standards (e.g., members of a real estate agency franchise).	Legislative
Process for forming a DBG		
R181	Issue regulations to prescribe that the relevant AML/CFT supervisor is required to approve formation of a DBG	Regulatory *
Compliance officers		
R182	Amend the Act to require compliance offices to be either a senior manager or report to a senior manager.	Legislative
Group-wide programme requirements		
R183	Amend the Act to introduce group-level compliance requirements for financial and non-financial groups (e.g., consisting of a parent company or equivalent legal person exercising control and coordinating functions over the rest of the group) in consultation with the private sector.	Legislative
Understanding and identifying country risk		
R184	AML/CFT supervisors should update existing country risk guidance to provide further detail about the risks that can emerge when dealing with customers from or businesses involved other countries. This will enable businesses to take a more nuanced and risk-based approach.	Operational

#	Recommendation	Type
Requiring businesses to apply enhanced CDD measures		
R185	Issue regulations to specify that the references to countries with insufficient AML/CFT systems or measures in place in sections 22(1)(a)(ii), 22(1)(b)(ii), and 57(1)(h) refers exclusively to those countries identified by the FATF as being high-risk jurisdictions subject to a Call to Action.	Regulatory *
Imposing countermeasures when called for by the FATF		
R186	Amend the Act to ensure the power in section 155 is sufficiently broad to enable the full range of countermeasures to be imposed if required.	Legislative
R187	Agencies should undertake further analysis to identify what countermeasures are required to mitigate risks posed by DPRK and Iran. With respect to DPRK, regulations should be issued to prohibit businesses from establishing correspondent relationships with DPRK banks.	Regulatory
Imposing countermeasures on specific individuals or entities		
R188	Explore the feasibility of issuing countermeasures against specific transnational organised crime groups to combat the threat that those groups pose to New Zealand.	Legislative

Financial intelligence

#	Recommendation	Type
Ensuring the FIU receives high-quality and accurate SARs		
R189	Review and update suspicious activity reporting (SAR) guidance in collaboration with the private sector to ensure it is fit for purpose and meets the needs of reporting entities. This guidance should include examples of best practice and explain how SARs are used by law enforcement agencies.	Operational
R190	Explore options for issuing regulations to reduce or remove the requirement to submit a SAR in instances where there is little intelligence value to be gained, such as low value frauds.	Regulatory
R191	Review the legislative requirements for submitting SARs to ensure they appropriately facilitate the provision of accurate and high-quality intelligence. In particular, agencies should consider whether a strict legislative timeframe is the best approach, as well as whether the Act should differentiate between forming an initial suspicion (which requires further investigation) and having reasonable grounds to suspect (which requires a SAR).	Legislative
R192	Review goAML's functionality to determine whether it can be made sufficiently user friendly and meet industry needs. If it is not possible to improve the functionality of goAML, agencies should work towards replacing goAML with an appropriate system.	Operational
Navigating legal privilege and SAR obligations		
R193	The FIU and DIA should review and update existing guidance to ensure that lawyers are able to navigate their competing obligations of legal privilege and suspicious activity reporting.	Operational

#	Recommendation	Type
R194	Issue regulations to extend the timeframe for law firms to submit a SAR (e.g., from three working days to five working days) to allow enough time for law firms to determine whether any information within a SAR is privileged.	Regulatory *
R195	Review and amend the legal privilege settings in the Act regarding SARs, in particular whether section 44(4)(b) should be repealed so that law firms can rely on a statutory defence to any prosecution if they have provided the information in good faith	Legislative
Enabling a more collaborative approach to reporting suspicions		
R196	Progress options for amending section 46 of the Act to expand the circumstances in which SAR information can be shared between agencies and reporting entities. This should be subject to appropriate conditions determined by analysis of the privacy risks and impacts and in consultation with the private sector and the Privacy Commissioner.	Legislative
Types of transactions requiring PTRs		
R197	In consultation with the private sector, issue regulations to carve in or carve out prescribed transaction reporting (PTR) obligations in respect of specific transactions, e.g., MT202s and certain currency exchange transactions.	Regulatory *
PTR obligations for non-bank financial institutions and DNFBPs		
R198	Require DNFBPs to submit a PTR when undertaking or receiving international wire transfers through another reporting entity on behalf of an underlying client. The DNFBP should only be required to submit the relevant information it holds as well as information (e.g., a unique reference number) necessary to enable the FIU to match the complimentary PTR from the other reporting entity.	Regulatory *
R199	Declare that the DNFBP is not the ordering or beneficiary institution of a wire transfer when undertaking or receiving international wire transfers through another reporting entity on behalf of an underlying client.	Regulatory *
R200	In consultation with the private sector, undertake further analysis to identify what, if any, wire transfers involving NBFIs (on behalf of underlying clients) should attract PTR obligations. Then issue appropriate regulations if the benefit of the additional reporting is justified by the costs. If it is not, exempt NBFIs from PTR wire transfer obligations.	Regulatory
PTR obligations for remittance businesses		
R201	Amend Regulation 6A *AML/CFT (Exemptions) Regulation 2011* to exclude remitters or money or value transfer service businesses from the scope of the exemption.	Regulatory *
Applicable threshold for reporting prescribed transactions		
R202	In the long term, reduce the PTR threshold for international funds transfers to NZD 0. This change should only be made once operational challenges with the PTR regime are resolved and the FIU has sufficient capability and capacity to receive the increased number of PTRs.	Regulatory
R203	Agencies conduct a cost/benefit assessment to identify what intelligence value a lower large cash transaction threshold (e.g., NZD 5,000) would provide and whether the costs of the change are justified.	Operational, regulatory

#	Recommendation	Type
What PTRs should contain		
R204	Review the current requirements specified in the *AML/CFT (Prescribed Transaction Reporting) Regulations 2016* to ensure that only information that is necessary for the FIU to produce relevant intelligence products is reported. This review should also ensure PTR obligations are aligned with ISO 20022 standards as well as ensuring that all relevant country information is collected by requiring the originator's address and location of their account to be collected.	Regulatory
Ensuring quality PTRs are submitted within statutory timeframes		
R205	Extend the timeframe for submitting PTRs from 10 to 20 days.	Legislative, regulatory *
R206	Explore the feasibility of a targeted exemption which could apply when businesses identify a technological issue which undermines the accuracy of reports being submitted.	Regulatory
Requiring BCRs for other forms of value movement		
R207	Issue regulations to require border cash reports (BCRs) for stored value instruments and casino chips in the short term.	Regulatory
R208	Amend the Act to require BCRs for stored value instruments, casino chips, and precious metals and stones.	Legislative
R209	Amend the Act to give Customs the power that provides discretion to prove that a particular form of item located in possession of or consigned by a person is being used for value movement purposes and to investigate whether it is happening or not.	Legislative
When BCRs should be filed for unaccompanied cash		
R210	Define import and export in the Act.	Legislative
R211	Set the timing in the Act of the requirement to complete a BCR for unaccompanied cash movement to 72 hours before the cash arrives in or leaves New Zealand and address this through regulations in the short term.	Regulatory *
Powers to search and seize cash to investigate its origin		
R212	Expand the Act to give Customs the power to investigate whether a section 110 offence has been committed.	Legislative
Sanctions for falsely declared or undeclared cash		
R213	Amend the Act to explicitly link the penalty for falsely/undeclared cash to a range of between 15 percent to 200 percent of the falsely/undeclared amount. Penalties	Legislative
Requiring mandatory deletion of financial intelligence		
R214	In consultation with the FIU and the Privacy Commissioner, amend the Act to specify the length of time personal information received in a SAR, PTR, or BCR can be held by the FIU. This timeframe will likely be different for PTRs and BCRs compared to SARs, due to the different nature of the reports.	Legislative
R215	In the interim the FIU should, in consultation with other agencies and the Privacy Commissioner, review and update its privacy policies to specify when it will destroy reports received or remove personal information within those reports to comply with Privacy Principle 9 of the *Privacy Act 2020.*	Operational

Background to the review

50. Like every country, New Zealand faces money laundering and terrorism financing risks. Money laundering is a process that criminals use to 'clean' money that has been obtained from crime. Successful money laundering allows criminals to amass illicit wealth and furthers the cycle of criminality by making funds available for reinvestment in crime. These crimes cause direct financial losses to individuals, community harm, and in some cases, loss of human life.

51. Money laundering enables and incentivises offending that impacts New Zealand communities. Drug offending, particularly the methamphetamine market, is enabled by criminals being able to launder money, which in turn impacts New Zealand's health, justice, mental health, and welfare systems. Money laundering also enables fraud and tax offending, particularly where larger values are involved.

52. Overseas criminals are also attracted to New Zealand's reputation as a safe country that is free from corruption. Because of this, transnational organised crime groups seek to hide funds in New Zealand or exploit New Zealand companies or trusts from overseas for international money laundering. This can tarnish New Zealand's reputation and, in doing so, affect our economy.

53. Terrorism financing refers to how funds are raised, moved, or used to facilitate the planning, preparation, or commission of a terrorist act. The risk of large-scale terrorism financing in New Zealand is low, but we are vulnerable to small-scale domestic terrorism financing, including by lone actors who self-raise funds, e.g., through gainful employment. The consequences of this type of terrorism being carried out in New Zealand are devastating, as was seen in the terrorist attack on the Christchurch masjidain on 15 March 2019.

The AML/CFT regime helps keep New Zealand safe from illicit capital

54. The AML/CFT regime improves New Zealand's safety by making it harder for criminals to profit from their offending. Similarly, by making it harder to finance terrorism the Act disrupts terrorist activities, both in New Zealand and worldwide. By keeping dirty money out, the Act helps ensure markets are not distorted by illicit funds and helps to maintain integrity of financial institutions and professions such as lawyers, accountants, and real estate agents.

55. The AML/CFT system also generates the largest and most detailed financial intelligence available to the government and law enforcement agencies. This results in wide-ranging benefits, such as: enhancing national security, combatting terrorism, disrupting and dismantling serious and organised crime (including transnational organised crime), protecting New Zealand from bribery, corruption, foreign interference, and restraining criminal assets.

56. These outcomes are achieved by imposing obligations on businesses that provide specific financial and non-financial services, known as reporting entities. At a very high level, the Act requires reporting entities to assess their money laundering and terrorism financing risks, identify and know their customers, report suspicious activities and certain transactions, and maintain various records. Our AML/CFT measures are broadly in line with international best practices identified by the Financial Action Task Force (FATF).

57. The regime also involves a wide range of agencies to deliver the outcomes:

    - The Ministry of Justice is responsible for administering the Act and the overall regime and assessing how it is performing.

- The Reserve Bank of New Zealand, Financial Markets Authority, and Department of Internal Affairs act as supervisory agencies to ensure compliance by reporting entities. The AML/CFT Supervisors are vested with various powers and can prosecute reporting entities for criminal breaches of the AML/CFT regime.

- In addition, the New Zealand Police's Financial Intelligence Unit is responsible for receiving, analysing, and disseminating financial intelligence, while the New Zealand Customs Service is responsible for addressing risks of cross-border cash movements and sanctioning falsely or undeclared cash at the border. The Police, Inland Revenue, and the Serious Fraud Office all use intelligence gained from the AML/CFT regime when investigating and prosecuting financial crimes, including money laundering.

- The Ministry of Business, Innovation and Employment is also involved with the AML/CFT regime as they are responsible for administering various licensing and registration regimes, as well as maintaining registers of legal persons (such as companies and limited partnerships). Finally, Ministry of Foreign Affairs and Trade is jointly responsible with the Ministry of Justice for implementing targeted financial sanctions (e.g., designations under the *Terrorism Suppression Act 2002*).

Substantive amendments were made to the Act in 2015 and 2017

58. The first Act that was introduced in New Zealand that aimed to combat money laundering and terrorism financing was the *Financial Transaction Reporting Act 1996* (FTRA). This Act was designed to facilitate the prevention, detection, investigation, and prosecution of money laundering and the recovery of criminal assets. The Act imposed relatively limited obligations on various businesses to verify some customers identities, report suspicious transactions, and retain various records.

59. However, it became apparent that the FTRA was no longer in line with the international standards set by the FATF. As a result, the Act was introduced in 2009 to comprehensively reform New Zealand's AML/CFT regime and meet international obligations in areas such as customer due diligence, record keeping, and supervision. The Act aimed to take a risk-based approach for dealing with money laundering and terrorism financing, in that it aimed to ensure the regime's collective effort was prioritised towards areas where money laundering or terrorism financing was most likely. The Act provided a set of reporting requirements, created a comprehensive enforcement regime, and introduced a regime for supervision, monitoring, and enforcement of AML/CFT obligations by agencies appointed as supervisors. However, only casinos and financial institutions were included within the Act at this stage.

60. The Act was then amended in 2015 following the *Organised Crime and Anti-Corruption Legislation Bill.* This Bill was aimed at strengthening the law to combat organised crime and corruption, as well as allowing New Zealand to ratify the UN Convention Against Corruption. The Bill made amendments to a number of laws, but the amendment it made to the Act was to require businesses to submit prescribed transaction reports to the Financial Intelligence Unit when they engaged in specific transactions above a specific threshold. In particular, businesses were then required to submit these reports in respect of cash transactions at or above NZD 10,000 or international wire transfers at or above NZD 1,000.

61. The most recent (and arguably the most substantive) amendments were made in 2017, where the Act was amended to include various designated non-financial businesses or professions (DNFBPs). Prior to this, the Act only applied to financial institutions (such as banks), casinos, and trust and company service providers. However, the Government recognised that other businesses, such as lawyers, accountants, real estate agents, and high-value dealers, are also exposed to money laundering and terrorism financing risks. As such, the Act was amended to extend obligations to DNFBPs, and in doing so, more than doubled the number of businesses that have AML/CFT obligations. This Bill also inserted section 156A, which required this review to be conducted.

International AML/CFT policy is set by the Financial Action Task Force

62. The Financial Action Task Force (FATF) is the global money laundering and terrorism financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

63. The FATF was established following a G7 summit in 1989 in response to mounting concern over money laundering, and issued a report containing a set of Forty Recommendations in 1990 to outline a comprehensive plan of action needed to fight money laundering. Then, in 2001, the FATF included terrorism financing within its mission and developed a further eight "Special Recommendations" to deal with terrorism financing, which became nine in 2004. These recommendations were then reviewed and consolidated in 2012 as the FATF Recommendations, which outline all the steps governments should take to protect the integrity of the global financial system.

64. The FATF reviews money laundering and terrorism financing techniques and continuously strengthens its standards to address new risks, such as the regulation of virtual assets, which have spread as cryptocurrencies gain popularity. The FATF also monitors countries to ensure they implement the FATF Standards fully and effectively and holds countries to account that do not comply. Countries that are found to have particularly weak AML/CFT systems are publicly identified by the FATF as having strategic deficiencies and placed under increased monitoring, while the FATF calls on countries to impose countermeasures against exceptionally high-risk or non-cooperative jurisdictions.

New Zealand was assessed by the FATF in 2020-21

65. New Zealand has been a member of the FATF since 1991. As a member New Zealand is required to undergo periodic assessments known as a mutual evaluation, which is an assessment of the country's actions to tackle money laundering and the financing of terrorism and the proliferation of weapons of mass destruction. Mutual evaluations examine a range of issues to ensure that the country has implemented these standards. These issues include whether the country has enacted the necessary laws, established the right policies and whether its competent authorities, including its financial intelligence unit and financial supervisors, are properly resourced. However, mutual evaluations also examine how effective a country is, and whether countries make good use of the rules and tools at their disposal.

66. New Zealand's most recent mutual evaluation concluded in February 2021 with the publication of the Mutual Evaluation Report of New Zealand. This report provides a comprehensive assessment of New Zealand's effectiveness against 11 immediate outcomes, specifically how well:

- **Immediate Outcome 1:** money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.
- **Immediate Outcome 2:** international cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
- **Immediate Outcome 3:** supervisors appropriately supervise, monitor, and regulate financial institutions, DNFBPs and VASPs for compliance with AML/CFT requirements commensurate with their risks
- **Immediate Outcome 4:** financial institutions, DNFBPs and VASPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.

- **Immediate Outcome 5:** legal persons and arrangements are prevented from misused for money laundering and terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments
- **Immediate Outcome 6:** financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.
- **Immediate Outcome 7:** money laundering offences and activities are investigated, and offenders are prosecuted and subject to effective, proportionate, and dissuasive sanctions.
- **Immediate Outcome 8:** proceeds and instrumentalities of crime are confiscated.
- **Immediate Outcome 9:** terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate, and dissuasive sanctions.
- **Immediate Outcome 10:** terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.
- **Immediate Outcome 11:** persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

67. The report also assessed the extent of New Zealand's technical compliance with the FATF Recommendations and identified several areas where New Zealand only partially complies with the international standards. Overall, the FATF found that measures to combat money laundering and terrorist financing are delivering good results, but more needs to be done on improving the availability of beneficial ownership information, strengthening supervision and implementation of targeted financial sanctions.

68. The report provides a large number of priority and recommended actions that New Zealand should take to enhance its effectiveness, and as outlined in Methodology and approach, these were used as a basis for assessing the performance of the Act and whether any amendments should be made. We also noted the results of the Mutual Evaluation as part of assessing the extent to which the Act has maintained and enhanced New Zealand's international reputation (*see* Compliance with the FATF Standards).

Methodology and approach

Setting the foundation for the review

69. In line with section 156A of the Act, on 1 July 2021 the previous Minister of Justice, Hon Kris Faafoi referred to the Ministry a review of the operation of the provisions of the Act since 11 August 2017 and determine whether any amendments were necessary or desirable. This review required the completion of a report to the Minister of Justice within one year from the date of being referred, i.e., 30 June 2022. However, the review was required by law to begin no later than 1 July 2021, and we undertook preparatory work to ensure it had strong governance arrangements, clear scope and terms of reference, and would be conducted with the appropriate levels of engagement with the public.

Confirming the scope and approach for the review with the Minister

70. In March 2021, we briefed the then Minister of Justice to seek confirmation about the scope and approach to the review. This briefing was provided following the conclusion of New Zealand's Mutual Evaluation and provided a proposed work programme to strengthen New Zealand's AML/CFT regime. The Minister agreed to our recommendations to:

- conduct a broad review of the AML/CFT regime that considered the FATF's recommendations as well as whether the Act operates efficiently and proportionately.
- engage in two rounds of consultation, by seeking Cabinet's agreement to release a public discussion document and then engage in more iterative consultation with targeted group(s) of private sector stakeholders to develop recommendations for change.
- establish an Industry Advisory Group formed from key industry stakeholders and peak bodies.

71. We also recommended progressing earlier changes through regulations prior to the end of the review, if possible. Ultimately it was not possible to do this due to resourcing constraints as well as a significantly higher number of submissions received on the Discussion Document than originally anticipated.

Establishing the Industry Advisory Group

72. Following Ministerial agreement, we sought agency input as to who should be invited to join the Industry Advisory Group (IAG). In total, forty-nine people were identified as being potentially suitable candidates, in that they would be able to provide strategic insights and guidance as the review progressed. Invitations were sent on 21 May 2021 inviting people to join and sign the Terms of Reference for the IAG (which included an agreement to keep all information confidential). Thirty-seven people responded accepting the invitation.

73. We met with the IAG twice (once on 10 June 2021 and again on 27 September 2021) to seek their input and advice. We also ran a facilitated workshop with the IAG on 28 October 2021 to receive views about the performance and changes to the Act (*see* IAG Hui Report). We also provided the IAG the Terms of Reference, draft consultation document for comment and sought their views as to how to conduct both the cost survey and targeted engagement workshops in April 2022. All IAG members were also

invited to the engagement workshops, with most attending and contributing. Unfortunately, due to COVID restrictions, we were not able to meet with the IAG as much as we had initially intended. In addition, the timeframes for conducting the review also limited how much engagement we could meaningfully conduct (*see* Limitations of the approach).

Developing the Terms of Reference

74. We developed the Terms of Reference for the review (the Terms) in consultation with agencies and the IAG. The Terms set out that the aspiration for the review was for New Zealand to become the hardest place in the world for money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction. In doing so, the AML/CFT regime will help maintain a safe, trusted, and legitimate economy.

75. The Terms also set out that the review would be guided by the following principles as they relate to AML/CFT:

- create a financial environment that is hostile to serious and organised crime and national security threats by maintaining and enhancing our ability to detect and deter money laundering, terrorism financing, and financing the proliferation of weapons of mass destruction so that New Zealanders' economic wellbeing and security is protected
- appropriately and responsively **manage the risks New Zealand is exposed** to across the system through clear obligations on businesses, agencies, and the public that strike the appropriate balance between prescriptive obligations and performance expectations
- ensure policy, law enforcement, national security, regulatory and supervisory agencies within the regime have **proportionate and appropriate powers and functions** and are enabled to exercise them effectively and efficiently
- facilitate, support, and enhance **domestic and international collaboration and cooperation** between and within the private sector and government
- adopt **international best practices** where appropriate in the New Zealand context and ensure that New Zealand fulfils its international obligations and addresses matters of international concern so that New Zealanders' economic wellbeing and national security is protected
- **work in cooperation** with industry, public, and Māori to ensure the effectiveness and efficiency of our AML/CFT regime
- ensure the AML/CFT regime produces the **necessary type and quality of information** to support other frameworks which the regime intersects with and assist regulatory, supervisory and law enforcement agencies to combat money laundering, terrorism financing, and serious and organised crime
- ensure that **human rights and privacy considerations** are addressed and that intrusions on personal rights and freedoms are no more than is necessary to achieve the purpose of the AML/CFT regime
- support **efficient long-term administration** of the AML/CFT regime, including through enabling the use of technology.

Part A: Assessing the operation of the provisions of the Act

76. The first part of the review required the Ministry to consider how the provisions of the Act had performed since the commencement of section 156A (i.e., 11 August 2017). We have interpreted this as requiring an assessment of the extent to which the Act has delivered its objects or purposes (i.e., what the regime has done) as well as how the

regime has performed in delivering those objects (i.e., how the regime has achieved delivery).

Measuring the extent to which the Act has achieved its purposes

77. We conducted this part of the assessment in the following ways:

Purpose of the Act	How achieving the purpose was assessed
Detecting and deterring money laundering and the financing of terrorism	Reported and updated relevant findings of the FATF in New Zealand's Mutual Evaluation as they relate to detection and deterrence of money laundering and terrorism financing (*see* New Zealand was assessed by the FATF in 2020-21). Specifically: - the extent to which New Zealand understands its money laundering and terrorism financing risks (Immediate Outcome (IO) 1) - how well businesses report suspicious activities (IO.4), what the FIU does with the intelligence it receives (IO.6), and how it is used to support money laundering and terrorism financing investigations or prosecutions (IO.7, IO.9) - how well businesses understand and implement appropriate preventive measures to deter money laundering and terrorism financing (IO.4), how the AML/CFT supervisors ensure that businesses comply, including taking appropriate enforcement action (IO.3), and the extent of general deterrence of money laundering or terrorism financing resulting from investigations, prosecutions, and asset confiscation (IO.7, IO.8, IO.9)
Maintaining and enhancing New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force (FATF)	The overall results of New Zealand's Mutual Evaluation in terms of technical compliance and effectiveness, how they compare to other countries, and the impact of those results on the Basel Index and Financial Secrecy Index.
Contribute to public confidence in the financial system	It was not possible to directly assess this as there are no measures of public confidence in the financial system or measures which isolated the Act's impact compared to other impacts on confidence (e.g., interest rates, global pandemics, financial crises). We instead looked at other proxy measures to determine whether there was any negative impact following the Act being passed or being amended in 2017. These proxy measures were the Investor Confidence Survey, Ease of Doing Business Index, and new or total business registrations per 1,000 people.
Facilitates cooperation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies	Reported and updated relevant findings of the FATF in New Zealand's Mutual Evaluation in Core Issue 1.5 of IO.1, which examines the level of cooperation and coordination in the AML/CFT regime (*see* New Zealand was assessed by the FATF in 2020-21).

Assessing how the regime has achieved delivery

78. In addition to examining what the regime has delivered, we have also assessed how this delivery has been achieved, in terms of cost to New Zealand, level of regulatory

maturity, and consistency with Te Tiriti o Waitangi. The cost of the regime has always been a concern for businesses and government and thus we considered it necessary to examine the actual costs as part of this review. Furthermore, examining the regulatory maturity allows us to assess how well the regime is working at a particular point in time in line with the existing policy and institutional framework, and provide insights as to whether there are any areas of weakness or risks of regulatory failure. Finally, the Crown has an obligation as a Treaty partner to ensure that the Act is operated consistently with the principles of the Treaty.

Understanding the costs of the regime

79. There has never been a full assessment of the actual costs of the regime. Accordingly, we contracted a third-party provider (Nexus Research) to assess the private sector's costs of complying with the Act in the financial year ending 31 March 2022. The objective of the survey was to collect cost estimates for complying with financial crime obligations broken down by staff cost, staff cost on AML/CFT, financial crime software, and vendors, service providers and contractors. The survey also collected other information such as the number of employees required to undertake financial crime compliance work.

80. The online survey was conducted from 31 March to 27 April 2022. The questions in the survey were developed in consultation with the other AML/CFT agencies as well as the IAG (*see* Establishing the Industry Advisory Group), and asked respondents for:

- **information about the business completing the survey:** who their supervisor is, the type of business, when they became a reporting entity, the size of the business, their total revenue for the financial year ending 31 March 2022
- **information about how they comply:** whether they are a member of a designated business group, whether they outsource any of their obligations, and whether they rely on Ministerial exemptions
- **estimated costs of complying with financial crime obligations:** how many employees contribute to managing financial crime compliance obligations, the annual cost of those employees, the proportion of those employees' time spent on AML/CFT, total financial crime licensing costs, total vendor, service provider, and contractor costs, and whether they pass any costs on to their customers
- **level of accuracy and consistency of the estimates:** whether there have been any significant developments impacting their AML/CFT obligations and costs, how confident they were in the accuracy of their estimates, and how representative they considered their estimates to be compared with previous years
- **most and least expensive compliance costs:** which three obligations they considered to be the most expensive, and which three obligations are the least expensive.

81. The AML/CFT supervisors directly emailed the entirety of their reporting entity population at the beginning of April to invite them to participate in the survey and sent two further reminders while the survey was in the field. In total, 5,199 reporting entities were invited to participate with 1,117 responses received (23 percent response rate). Approximately 1,000 of DIA's reporting entities did not receive the survey as they did not have up-to-date or accurate contact details about the reporting entity's compliance officer. 425 responses were excluded from the final sample if a) the respondent had low confidence in their estimates or b) provided unlikely or internally inconsistent answers or c) responses contained data for more than one organisation. The final sample was N=725.

82. Total private sector AML/CFT costs were estimated by taking a trimmed average value[1] of the total AML/CFT specific labour costs, software costs, and vendor, service provider and contractor costs. These were then added to the AML/CFT-specific public sector

[1] The trimmed average is the average with the top 5% and bottom 5% of values removed. This gives an average value that is less impacted by outliers and more reflective of the bulk of reporting entities.

costs incurred by the Ministry of Justice, DIA, FMA, RBNZ, New Zealand Police (Financial Intelligence Unit), and New Zealand Customs Service to derive the total per annum costs of the regime.

Assessing the maturity of the AML/CFT regulatory system

83. Assessing the regulatory maturity of the AML/CFT regime examines the extent to which the regime takes a whole-of-system, proactive, collaborative, and long-term approach, that can anticipate, and respond to, change over time. This assessment allows us to understand whether the regime is functioning as intended and whether there is a risk of regulatory failure. We used an assessment tool developed by the Ministry of Business and Innovation (MBIE) (the tool), which provides a framework for agencies to self-review their regulatory practices and performance.

84. We note that assessments are normally conducted by an independent group of assessors. However, we did not have the time available to stand up an independent review panel for this part of the review (*see* Limitations of the approach). Instead, we used this tool to design a questionnaire for employees involved with the AML/CFT regime across the different agencies, with the intention of seeking their views on the regulatory maturity of the regime. We consider that this approach would still provide insight as to the maturity of the regime as well as provide a foundation for future assessments of regulatory maturity.

85. The tool includes a four-point maturity scale (informal, defined and evolving, structured and proactive, or optimised) and is organised around three areas (leadership and culture practices, design and delivery practices and systems performance). Each of these areas are then divided into three further sub-areas. These areas and sub-areas reflect the key aspects of regulatory systems that are integral to a well performing regime. The tool also contains lines of enquiry for each sub-area which are designed to stimulate and enable reflection about current performance.

86. We adapted the areas, sub areas, and lines of enquiry into an online survey by turning them into statements reflecting key aspects of the regime and also added other statements we considered were relevant to understanding the Act's maturity. For each statement, we asked submitters to rate their level of agreement on a 6-point Likert scale that ranged from strongly agree to strongly disagree. We then assigned a number to each rating (from -3 to +3) to enable us to generate an average score across the responses.[2] We also provided respondents with the opportunity to include comments at the end of each sub-section. Each maturity level was then assigned a range of average scores in order to appropriately code the responses received:

Maturity level	Average score (-3 to +3)
Informal: Inconsistent systems and practices, outcomes are not shared and understood, the system is reactive, and change is challenging.	-3 to 0 (indicates general disagreement with the statement)
Defined and evolving: Recognition of the need for shared objectives/ outcomes and more consistent ways of working with work underway to support more coordinated approaches across the system.	0 to 1 (indicates neutrality or slight agreement with the statement)
Structured and proactive: Formal systems and practices are in place and used consistently, adaptive practice is encouraged, the impact of change is understood, and the system can respond in good time.	1 to 2 (indicates general agreement with the statement)
Optimised: Adaptive systems, practices and ways of working are part of the culture, the system anticipates and responds to the challenge of changing circumstances.	2 to 3 (indicates strong agreement with the statement)

[2] The scale and scores given were strongly disagree (-3), disagree (-2), slightly disagree (-1), slightly agree (+1), agree (+2), strongly agree (+3)

87. The questionnaire was sent out to managers in the DIA, FMA, RBNZ, Police, the FIU, Ministry of Justice, MBIE, and Customs for them to distribute amongst their staff. In total, we received 46 responses out of approximately 120 estimated to be working across the regime. We have used 120 as the total population size when calculating a 95 percent confidence interval, which we have reported along with the average score.

Assessing consistency with Te Tiriti o Waitangi

88. We considered the extent to which the operation and development of the AML/CFT regime is consistent with the principles of Te Tiriti o Waitangi, as expressed by the courts and the Waitangi tribunal. Specifically, we assessed the extent to which the Act's operation has been consistent with the principles of partnership, active protection, and redress.[3]

Part B: Determining whether any amendments are necessary or desirable

89. The second aspect of the review required the Ministry to consider whether any amendments to the Act are necessary or desirable. We approached this in three broad stages: identifying potential options for change, analysing those options to determine whether any were necessary or desirable, and then developing any required recommendations. We engaged in extensive consultation and collaboration with other agencies and the private sector at each stage of the review. The recommendations we make reflect a general consensus.

Identifying potential changes (March 2021 – December 2021)

Identifying issues and opportunities

90. We began identifying issues and opportunities for reform once New Zealand's Mutual Evaluation was adopted in February 2021. The two main sources for potential reforms were the Mutual Evaluation findings and recommendations as well as issues and opportunities agencies have identified through the Act's operation. However, in line with the Terms of Reference (*see* Developing the Terms of Reference), we also considered other potential drivers for change, such as addressing emerging risks, supporting other government priorities, and ensuring compliance costs are proportionate to risks for our economy. We also considered how to modernise the Act and our approach to reflect the digital economy, and how to avoid or mitigate unintended consequences.

91. Per the requirements of the review, the Ministry was technically only required to identify whether there should be any amendments to the Act. However, in line with Cabinet's Impact Analysis Requirements (*see* Cabinet Office Circular CO (20) 2), we have also considered whether there should be any changes to secondary legislation (e.g., regulations) or operational changes (e.g., guidance). We note that challenges may result from the secondary legislation itself, or actually be resolve through operational reform rather than legislative amendments.

Public consultation on issues with the Act

92. In consultation with agencies and the IAG, we produced a public facing Discussion Document, which outlined and summarised all the issues or opportunities we had identified and invited comment from industry. Publication of the Discussion Document, short summary document, factsheet, and list of frequently asked questions was delayed

[3] Waitangi Tribunal, He Tirohanga ō Kawa Te Tiriti o Waitangi – A Guide to the Principles of the Treaty of Waitangi as Expressed by the Courts and the Waitangi Tribunal. Available at: https://waitangitribunal.govt.nz/assets/Documents/Publications/WT-Principles-of-the-Treaty-of-Waitangi-as-expressed-by-the-Courts-and-the-Waitangi-Tribunal.pdf

until in October 2021 due to COVID-19 and resulting delays in seeking Cabinet agreement for its publication. Once the consultation material was published, the AML/CFT supervisors emailed all of their reporting entities to encourage them to engage with the review. The factsheet and frequently asked questions were translated into other languages, specifically Arabic, Hindi, Chinese (simplified and traditional), Māori, Tongan, and Samoan.

93. In total, 220 submissions were received via email or online form, with submitters commenting on a range of topics that were of interest. The topics that attracted the most comment was the discussion about the risk-based approach, purpose of the Act, address verification, Identity Verification Code of Practice, and mitigating unintended consequences. All submissions were read, analysed, and then summarised to produce the Summary Document. The Summary Document and all non-confidential submissions were released in March 2021 and should be read in conjunction with this report (particularly Part B).

Developing options for reform (January 2022 – March 2022)

94. We developed the following criteria to assess potential options to determine the best approach for the regime:

- **Effectiveness:** how effective is the option/recommendation at addressing the harm or risk that has been identified?
- **Workability:** how workable will the option/recommendation be for the government, reporting entities, or third parties to implement and maintain?
- **Cost Effectiveness:** are the costs of the option/recommendation for private sector, government, and the wider economy in proportion to the harm and/or risk being addressed?
- **International Standards: t**o what extent is the option/recommendation in line with the FATF recommendations and the suggestions made in New Zealand's Mutual Evaluation report?
- **Constitutionally appropriate: i**s the option/recommendation in line with the principles of Te Tiriti o Waitangi, human rights conventions, privacy interests, or other constitutional considerations such as rule of law?

95. These criteria are broadly consistent with the criteria used for other AML/CFT reform projects and reflect the principles outlined in the Terms of Reference (*see* Developing the Terms of Reference). The criteria were also shared with agencies and IAG for comment to ensure they would ensure we appropriately assessed and considered all perspectives. No suggestions for change were received.

96. We then developed and brainstormed options for reform that could address the issue or achieve an identified opportunity. Feedback and suggestions from the private sector were included and considered as part of this process. No options were discounted from the outset, with all options assessed against the criteria above to determine whether they were better or worse than the status quo (do nothing) option.

Developing recommendations (April 2022 – May 2022)

97. We developed initial recommendations based on the analysis of the options to determine the best approach(es) that the regime could take. In doing so, we considered which option or combination of options would deliver the best outcome, as well as how the option would be achieved (e.g., through amending the Act, issuing regulations, or developing guidance).

98. Based on stakeholder input, we identified issues that were of importance to other agencies and/or industry and prioritised developing recommendations for those issues.

These recommendations and underlying analysis were tested with DIA, FMA, RBNZ, New Zealand Police, and New Zealand Customs Service in a series of agency workshops to develop a consensus position across agencies.

99. Following agency engagement, we invited all people who submitted on the Discussion Document and the IAG to a series of targeted engagement workshops in the latter half of April 2022. The purpose of these workshops was to share the initial recommendations, invite views from attendees, and ensure that, as much as possible, recommendations reflected the consensus of the private sector and AML/CFT agencies. The workshops and the topics considered were as follows:

Workshop	Topics discussed
Purpose and approach to AML/CFT Regulation	Changes to the purpose of the Act, such as including preventing money laundering and terrorism financing; changes to the risk-based approach; exemptions; how unintended consequences could be mitigated; and the role of the private sector.
Supervision, regulation, and enforcement	The model for supervision in New Zealand; registration or licensing for AML/CFT; changes to the offences and penalty framework; and whether there should be any regulation for agents, auditors, and consultants.
Customer due diligence	Reducing duplication of CDD; improving the requirements in relation to beneficial ownership; and whether any changes should be made to the Identity Verification Code of Practice.
Prescribed transaction reporting and suspicious activity reporting	When prescribed transaction reports (PTRs) are required; who should be required to submit PTRs; whether there should be changes made to the wire transfer definitions; and how to improve the quality of suspicious activity and transaction reporting.
Politically exposed persons and sanctions	Whether the AML/CFT regime should be used to support businesses implementing targeted financial sanctions obligations and what, if any, changes should be made with respect to politically exposed persons.

100. We also conducted five sessions on certain topics that only impacted specific sectors, namely Virtual Asset Service Provider obligations, CDD for Real Estate Agents, Wire transfer obligations, Money or Value Transfer Service provider obligations, and obligations for High Value Dealers and Pawnbrokers.

101. The workshops were well attended, with between 20 and 80 people attending the workshops from a range of sectors. Our recommendations reflect the outcome of the workshops and were shared with all agencies a final time to confirm agency consensus across all recommendations.

Limitations of the approach

102. There are two key limitations to the approach we have taken to the review. The first is the length of time that we had available to conduct the review, as the Act mandates that the review must conclude no later than one year after it begins (section 156A(2)). This timeframe was also impacted by the delays in the release of the Discussion Document: public consultation was the first stage of identifying recommendations for change, but the release of the document was delayed going to Cabinet by two months (*see* Public consultation on issues with the Act).

103. The mandatory timeframe of a year (in practice, nine months) necessarily impacted the amount and level of consultation that could be conducted, and the level of detail included in recommendations for change, particularly legislative changes. This timeframe also precluded being able to engage with Māori and other ethnic groups in a manner fully

consistent with the Te Arawhiti's guidelines of engagement with Māori or DPMC's community engagement toolkit.

104. As such, many of the recommendations are less firm or specific than they could have been if more time was provided to conduct the review, as there is further work and engagement that needs to occur before a specific recommendation can be made or agreed to. In addition, approaches to assessing various aspects of the system, such as regulatory maturity, had to be tailored to the amount of time that was available (*see* Assessing the maturity of the AML/CFT regulatory system).

105. The second limitation was the scope of the review, which was also set by the Act and limited specifically to the operation of the Act and whether there should be any changes made to the Act. Importantly, the Ministry was not able to assess the performance of or identify whether any changes should be made to other aspects of the AML/CFT regime that are not contained within the Act, such as:

- the money laundering offence *(Crimes Act 1961)* or terrorism financing offence (*Terrorism Suppression Act 2002)*
- seizing or forfeiting tainted assets or illicit funds (*Criminal Proceeds (Recovery) Act 2009)*
- the formation and operation of legal persons and legal arrangements, including whether there is any verification undertaken of the identity of the parties to the company or trust (e.g., *Companies Act 1993, Trusts Act 2019)*
- general availability of identity verification requirements in New Zealand or access to verified identity information, such as RealMe or databases of passport information (e.g., *Passports Act 1992, Electronic Identity Verification Act 2012)*
- general registration and licensing requirements for businesses (e.g., *Financial Service Providers (Registration and Dispute Resolution) Act 2008)*.

106. These other Acts contain important parts of the overall AML/CFT regime, and their performance both impacts on and is impacted by the performance of the Act. For example, the fact that the identity of directors and shareholders of companies is not currently verified by the registrar necessarily weakens the overall transparency of beneficial ownership in New Zealand and means the register is potentially unreliable for customer due diligence purposes.[4] Conversely, issues with the identification and reporting of suspicious or criminal activity impacts how easily money laundering or terrorism financing can be investigated or prosecuted. As a result, the review has not been able to consider or make recommendations for change in other related regulatory frameworks, even where those changes could significantly improve the effectiveness of the Act and the overall regime

[4] Cabinet agreed to introduce a Bill in 2022 to make it harder for companies and limited partnerships to be misused for illicit activity, which includes some verification of the directors, shareholders, and beneficial owners of these types of legal persons.

Part A: Operation of the provisions of the Act

CHAPTER 1

Achieving the objects of the Act

Summary

107. In this chapter, we consider the extent to which the Act is achieving its objectives or purposes in order to assess how well it has performed since 2017. The purposes of the Act are outlined in section 3 and are to:

- detect and deter money laundering and the financing of terrorism
- maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force (FATF), and
- contribute to public confidence in the financial system.

108. Overall, we consider the Act is detecting and deterring money laundering to some extent, which is largely in line with the findings of the FATF in New Zealand's Mutual Evaluation. There are two main barriers to the Act being as effective as it could be: the lack of an up-to-date national assessment of risks, and a number of important gaps in the Act's measures to deter money laundering and terrorism financing. Furthermore, as discussed elsewhere in this report, the Act's ability to effectively detect and deter money laundering is heavily impacted by the level of resourcing for the regime as well as how easy it is for businesses to submit reports through to the FIU.

109. The Act is intended to be an inherently risk-based regime, in that efforts by government and businesses should be prioritised to areas of highest risk. Generally larger businesses have a better understanding of their risks, with smaller businesses or businesses that have not been in the regime for as long had a more developing understanding of their risks and New Zealand's risks overall. However, the out-of-date assessment of national risks means that the regime may not be responding to new or emerging threats that have not been identified by government. In addition, we received a large amount of feedback that the overall risk assessment framework can be improved in terms of how information is communicated to businesses as well as the nature of the information that is shared.

110. The Act generates a large amount of financial intelligence to be analysed and turned into intelligence products. Most of the reports come from larger and more sophisticated financial institutions, with generally low levels of reporting from DNFBP sectors and smaller financial institutions. The low level of reporting does not reflect the risks associated with those sectors, and likely results from the variance in risk understanding. The FIU in turn produces a large amount of intelligence products, but the FATF found that the FIU did not fully exploit the potential of financial intelligence being used to detect criminal activity by persons not already known to law enforcement. Nevertheless, several investigations and prosecutions have made extensive use of financial intelligence provided by the FIU.

111. Deterrence of money laundering and terrorism financing is undermined by gaps in obligations for businesses as well as gaps in the overall regulatory regime which leave many businesses vulnerable to being misused. These gaps are, in turn, further undermined by the AML/CFT supervisors lacking sufficient enforcement powers to respond to all instances of non-compliance with the Act and impose effective, proportionate, and dissuasive penalties. Notwithstanding this, we consider that law enforcement efforts will be having some deterrent effect through investigating and prosecuting this offending and being highly effective at recovering tainted assets.

112. While we have identified several gaps in the Act and many areas for improvement, we note that New Zealand was found to be relatively effective in its Mutual Evaluation compared to many other countries, including Australia, Canada, and the United States. Importantly, New Zealand was not found to warrant public identification by the FATF as a high-risk jurisdiction, which would have occurred with a weaker regime. As such, we consider that the Act has generally maintained and enhanced New Zealand's international reputation, but there is still more that could be done to prevent the misuse of companies and trusts.

113. Finally, we were not able to identify any negative impacts following AML/CFT reform in the levels of investor confidence, ease of doing business, and the rate of business registrations in New Zealand. We generally consider that the Act appears to have fulfilled its third purpose of contributing to public confidence in the financial system to the extent public confidence can be measured.

1.1. Detecting and deterring money laundering and terrorism financing

114. As outlined in the Methodology and approach, we have assessed the extent to which the Act has detected and deterred money laundering and terrorism financing by considering the findings of New Zealand's Mutual Evaluation and providing any relevant updates. We begin by outlining the extent to which New Zealand takes a risk-based approach (assessed by Immediate Outcome 1 in the Mutual Evaluation). Next, detection of money laundering and terrorist financing is assessed by reference to Immediate Outcome 6. Finally, deterrence is assessed by reference to Immediate Outcomes 3, 4, and 7-9.

1.1.1. Implementing a risk-based approach

115. FATF Standards require that, at its core, any AML/CFT regime should be risk-based: there should be an assessment of money laundering and terrorism financing risks at the national, sectoral, and business level, and regulation and resource allocation should be focused on mitigating the risks identified. This is reflected in the emphasis on national risk assessments in the FATF Standards. A risk-based approach helps ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified and that resources are allocated efficiently.

How well do we understand our risks

116. Risk assessments play a key part in New Zealand's efforts to detect and deter money laundering and terrorist financing. They guide the development of policies and controls, as well as directing resource across the regime.

117. The FATF concluded that as of early 2020 New Zealand had a good understanding of our risks through a three-tiered risk assessment system and that we have largely responded well to these risks. This was based on a comprehensive multi-tiered risk assessment process through the National Risk Assessment (NRA) undertaken by the FIU and Sector Risk Assessments (SRAs) undertaken by supervisors. These have been through several iterative revisions but was due for a major update after the Mutual Evaluation was completed to align with the original 2020 timeframe for the third NRA and to provide insights to be used by the review of the Act.

118. Due to the impacts of the pandemic and competing priorities in the FIU, work on the planned new NRA has yet to start. The existing NRA is now outdated and based on core data on money laundering methods from its last full iteration in 2013-15. In addition, the previous NRA predates (and thus does not consider) the impact of key regulatory changes such as the Phase 2 reforms and subsequent amendments to other related legislation (such as the *Trust Act 2019*). As such, we lack an informed understanding of how legislative settings have changed the risk environment. In addition, our understanding of money laundering threats and methods and risks from

dynamic factors such as emerging technology relies on outdated information in the NRA. Taken together, these limitations of current risk understanding mean we do not have assurance that the system is responding effectively to unidentified or developing risks, which would impact the detection and deterrence of money laundering and terrorist financing.

119. As the NRA informs the SRAs, three of the four SRAs similarly require updating. This directly impacts how businesses are assessing their risks and may mean they are focusing on the wrong areas as New Zealand's risk landscape evolves. It also means that our policy measures may not be effective and that resources are not being allocated appropriately across the regime.

New Zealand uses a three-tiered system to assess our risks, but NRAs are not required by the Act

120. New Zealand has a three-tiered risk assessment system to identify and assess its money laundering and terrorist financing risks, comprising of the NRA, four SRAs and reporting entities' own risk assessments. The 2015 core assessment of the current NRA was developed in alignment with the FATF methodology, led by the FIU, and coordinated by the working groups of the NCC. Relevant government agencies and certain reporting entities contributed to this process as well as subsequent minor updates. The NRA details risks at the national level, and consistent with the FATF expectations, assesses risks as a function of threats, vulnerabilities, and consequences and describes the scale and nature of the risks faced by New Zealand at the national level.

121. While the Act does provide a function to the Commissioner of Police to produce risk assessments to be used by the Ministry, supervisors, and the New Zealand Customs Service (section 142(k)), there are no provisions for an assessment to be produced at a national level or meet the standard or status of an NRA. In particular, there are no provisions to coordinate other agencies or private sector input, nor are their provisions for the role that the NRA should have on national coordination mechanisms to drive the AML/CFT system and any policy, resourcing, or operational changes. Further, there has been historically limited private sector involvement in the production of the NRA.

122. In line with their role in the Act (section 131(a)), the AML/CFT supervisors are required to produce more specific assessments that identify and communicate the money laundering and terrorism financing risks faced by their reporting entities. The supervisors fulfil this through producing SRAs, which are informed by the NRA and aim to provide sector-specific assessments of money laundering and terrorism financing threats and vulnerabilities. The four SRAs are:

- **Financial Markets Authority:** Sector Risk Assessment (December 2021; previous versions published in 2011 and 2017)
- **Department of Internal Affairs:** Financial Institutions Sector Risk Assessment (December 2019; previous versions published in 2011 and 2018); DNFBPs and Casinos Sector Risk Assessment (December 2019; previous version published in 2017)
- **Reserve Bank of New Zealand:** Sector Risk Assessment for Registered Banks, Non-Bank Deposit Takers and Life Insurers (April 2017; previous version published in 2011)

123. At the bottom tier, reporting entities are required by the Act to produce their own risk assessments (section 58(1)) and consider the risk assessments produced by government as part of this process. This means that reporting entities rely on up-to-date NRAs and SRAs to guide their risk assessments for their business but also as part of assessing the risk of a particular customer or transaction.

124. Although there is no provision in the Act for the NRAs and SRAs, or versions of them, to be made publicly available, authorities do so for transparency and in line with the provisions in the Act relating to the dissemination of guidance (section 152(d)). The FIU uses its secure message board system to advise registered reporting entities of

updates and changes to any risk assessments. The Financial Crime Prevention Network (FCPN), consisting of the FIU, five major banks, Customs, and RBNZ, is also used as an effective communication mechanism between the public and private sector

New Zealand had a good understanding of our risks at a national level

125. The FATF concluded that, as at the time of the onsite in early 2020, New Zealand had a good understanding of its risks. It evaluated the methodology of the NRA as sound, producing a multi-dimensional assessment of domestic and international threats, vulnerabilities, and the potential impact of these on the objectives of the Act. It also concluded that, through the SRAs, the AML/CFT supervisors maintain an overall good understanding of the inherent money laundering and terrorism financing risk profiles of their respective sectors. The FATF also considered it would be beneficial for the AML/CFT supervisors to further engage the private sector during the SRA processes.

126. The FATF agreed that New Zealand's major domestic proceeds-generating crimes are drugs, fraud, and tax offending, and noted that approximately NZD 1.35 billion is generated per annum, mostly from drug and fraud offending. Compared to drugs, the tax and fraud threat is more likely to comprise of individualistic, smaller value offenders who engage in self-laundering. However, fraud offenders may have access to more sophisticated methods of money laundering.

127. Several sectors in New Zealand have been identified as significant in terms of their scale, role, or vulnerability. These include the banking, money or value transfer service providers (particularly alternative remitters), real estate and professional services sectors, as well as the misuse of legal persons and arrangements.

128. The NRA considered the international and domestic terrorism-financing threat from lone actors, small cells, terrorism networks, identity-motivated and faith-motivated extremism. 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. This risk is reflected in the terrorist attack on Christchurch masjidain on 15 March 2019 and the New Lynn attack on 3 September 2021.

Businesses generally had a good understanding of their risks

129. The FATF considered that New Zealand has sound mechanisms to provide information in the NRA and SRAs to all relevant reporting entities. A public version of the NRA is published on the New Zealand Police website and the SRAs are similarly published on their respective supervisor's website, along with other guidance. Although there is no provision in the Act for the NRAs and SRAs, or versions of them, to be made publicly available, authorities do so for transparency and in line with the provisions in the Act relating to the dissemination of guidance (section 152(d)). The FIU uses its secure message board system to advise registered reporting entities of updates and changes to any risk assessments. The Financial Crime Prevention Network (FCPN), consisting of the FIU, five major banks, Customs and RBNZ, is also used as an effective communication mechanism between the public and private sector.

130. New Zealand's MER concluded that there is a better understanding in larger and more sophisticated reporting entities, and in sectors where AML/CFT obligations are better established. For example, banks and other large financial institutions demonstrated a good understanding of their risks, including the cross-border aspects of money laundering and terrorist financing. Larger MVTS providers demonstrated a more comprehensive understanding of risk, while smaller MVTS providers rely more heavily on third party providers to understand risk. Among non-financial sectors, casinos and some TCSPs have a good understanding of risks, while the newly supervised DNFBPs and VASPs are largely still developing their understanding of their risks and how AML/CFT obligations apply to their business.

However, the risk-based approach is currently undermined by out-of-date risk assessments

131. Two iterations of the NRA were conducted in 2010 and 2013-15 with updates made to some information the second NRA in 2016, 2017 and 2019. Critically, that the NRA is using core data on treats and methods from 2009-13, and many sections on significant vulnerabilities have either not been revised or still include information up to a decade or more old despite the subsequent updates. The NRA is intended to be iterative and includes recommendations for its review and updating within 18 months and for its full reassessment every five years.

132. As part of the AML/CFT National Strategy, New Zealand committed to completing its third NRA in 2020 which would have informed this statutory review and the 2021 update to the National Strategy. However, due to other FIU strategic priorities, along with the impact of COVID on the FIU, the deadline for the new NRA was revised until to December 2022 in the updated national strategy. Work to achieve the revised timeline is yet to commence.

133. The out-of-date assessments are a vulnerability in New Zealand's understanding of our risks. The FATF found that one of the key strengths of the private sector understanding of risk is that established reporting entities, such as banks, refresh their own risk assessments on an annual basis. However, since businesses use the NRA and SRAs to inform their own risk assessments, they may not be responding to their risks as well as they could if money laundering threats or methods have shifted since 2013. This would lead to focusing resources in the wrong areas. In addition, it means that we have not responded to any risks that have emerged following the NRA in the NRA at either a policy or operational level, or risks that have since become more significant. This threatens the effectiveness of New Zealand's broader policy levers and resourcing to combat money-laundering and terrorist financing as the NRA should inform potential changes to the regime and the prioritisation of resources by AML/CFT agencies

Businesses told us the risk assessment framework can improve

134. As part of consultation on the Discussion Document, we asked whether New Zealand is appropriately assessing our risks and sharing that information with businesses so they can properly assess and understand their risks. While some submitters thought New Zealand's current approach is sufficient, many submitters identified areas where the framework could be improved. This included greater sharing of risk information, intelligence, and feedback, including information about typologies and the data driving conclusions about risks. Other submitters said NRAs and SRAs could be more nuanced and targeted to industries or thematic areas, should have a standardised methodology and format, or be combined into one document to enable holistic understanding of risks.

135. Further, other submitters said the NRA and SRAs do not help people working in businesses to genuinely understand the nature of threats and vulnerabilities they are exposed to. Submitters noted that the NRA and SRAs could be kept more up to date to ensure continued relevance and accurate benchmarking for their businesses. Submitters also noted that the documents are generalised, quickly outdated or provide criminals and terrorists with a checklist to avoid raising suspicion and detection. In line with industry feedback, we make recommendations that will help avoid risk assessments being viewed or treated as a 'tick-box' exercise (*see* Recommendation R12) and help ensure they are produced more regularly (*see* Recommendation R9).

We have generally responded to and mitigated risks identified

136. The FATF concluded that our national AML/CFT policies and activities address identified money laundering and terrorist financing risks to a large extent. The Ministry develops and updates policy in response to the findings of each iteration of the NRA and other major events, and this was deemed an effective process in the MER. That said, the FATF did identify some gaps in how we addressed our risks. In addition, the

now outdated NRA and SRAs mean that we are not currently responding to unidentified or evolved risks.

137. Financial institutions, casinos, and some trust and company service providers have had obligations under the Act since 2013. Since then, agencies have progressed and implemented a number of policies and reforms to address risks as they were identified. The 2015 NRA led to several changes, including the extension of the AML/CFT regime to cover all non-financial sectors, ensuring law enforcement agencies (LEAs) have access to tax information to target money laundering, and the implementation of prescribed transaction reporting. Amendments were also made to the money laundering offence in the *Crimes Act 1961* and several policing initiatives were implemented (e.g., funding was secured for dedicated money laundering investigation teams and training was expanded). We also developed an enhanced regulatory regime for New Zealand Foreign Trusts.

138. Concurrent to the development of the 2019 update to the NRA, we developed an overarching AML/CFT National Strategy to help set the strategic direction for the regime. The Strategy was approved in December 2019 was led by the Ministry and coordinated by the NCC pursuant to its role in the Act (section 151) and includes an action plan with a series of actions that were to be completed between 2020 and 2021. This required conducting the third full NRA in 2020 and undertaking other risk assessments, the statutory review of the Act, expanding guidance on SARs for terrorist financing, and improving the cross-border cash reporting regime. The strategy has since expanded to included actions to be completed by the end of 2023. Since the third NRA has not been delivered (or started) within agreed timeframes, it any findings of the NRA have not been able to be considered as part of this review.

139. However, while the Act has enabled the development of the National Strategy, there are no provisions requiring agencies to carry it out, nor for the NCC to direct agencies to complete actions or report on progress in achieving its priorities. This limits accountability for the strategy and action plan.

However, the FATF identified several areas where more work is required

140. The FATF concluded that the above policy process has mostly addressed our identified money laundering and terrorist financing risks. The MER stated that we demonstrated our ability to respond to new and emerging risks, such as introducing most VASPs into the AML/CFT regime. However, the FATF did identify gaps in addressing some risks, particularly in the areas of beneficial ownership and unregistered MVTS providers. These included insufficient measures to ensure accurate and up to date beneficial ownership information of both legal persons and trusts, as well as unmitigated risks associated with the use of nominee directors and shareholders.

141. Other areas where the FATF identified gaps in addressing our risks included targeted financial sanctions, CDD obligations for trusts, licensing and registration of financial institutions and DNFBPs, implementation of PEP requirements, and monitoring of non-profit organisations. The statutory review has also identified the need to respond better to illicit capital entering the real estate market, the use of virtual assets for illicit purposes, high-value dealers, and trade-based money laundering (*see* Improving the Act's ability to combat high-risk areas).

1.1.2. Detection of money laundering and terrorism financing

142. New Zealand's ability to detect and investigate money laundering depends on the FIU's ability to collect information, create products and systems, and disseminate information and intelligence to law enforcement and regulatory authorities. In turn, this depends on the intelligence received by the FIU from businesses.

143. Under section 142 of the Act, the Commissioner of Police is responsible for receiving and analysing various intelligence reports and determining whether any report should be referred to investigative branches of the New Zealand Police or other law enforcement agencies for criminal investigation. The Commissioner is also responsible

for producing guidance material for businesses and developing risk assessments relating to money laundering and terrorism financing for other AML/CFT agencies to use. To support these functions, the Commissioner can order the production of or access to all records, documents, or information from any reporting entity that is relevant to analysing any information they have received (section 143(1)(a)).

144. In practice, these functions are carried out by the FIU, which is housed within the Police. Overall, the FATF considered that reports submitted to the FIU were broadly in line with expected risks, but some sectors were not found to be reporting as much as they should be (specifically DNFBPs and some FMA sectors). The FATF also found that the FIU is creating a range of intelligence products with the information they gather, primarily intelligence and strategic reports, which predominately comes from reports received under the Act. These products provide value to authorities and support criminal investigations and asset recovery efforts.

The Act generates a large amount of financial reporting for analysis

145. The FIU receives intelligence from businesses through three types of reports submitted under the Act:

- **suspicious activity reports (SARs)**, which businesses are required to submit no later than three working days after they have formed a suspicion that a transaction, activity, or inquiry may be relevant to the investigation or prosecution of any offence, including money laundering or terrorism financing (sections 39A and 40).
- **prescribed transaction reports (PTRs)**, which businesses are required to submit within ten working days where someone conducts an international funds transfer exceeding NZD 1,000 or large cash transaction exceeding NZD 10,000 through their business (section 48A).
- **border cash reports (BCRs)**, which every person is required to submit if they move more than NZD 10,000 in cash or certain cash-like equivalents into or out of New Zealand (section 68).

Suspicious activity reports

146. The number of SARs received by the FIU has increased over time as businesses mature in their understanding and implementation of the Act's requirements. The highest reporting is from banks, followed by MVTS providers, which is consistent with sector size and risk level.

147. However, the FATF and FIU consider that the level of reporting by DNFBPs was low, particularly by TCSPs, law firms, accounting practices, and real estate agents. This is notable given the risks that these sectors are exposed to. The same was true for some FMA sectors, particularly derivatives issuers.

Table 1 - Suspicious activity reporting by financial institutions 2017-2021

Sector	2017	2018	2019	2020	2021	Total
Banks	5,556	7,295	7,893	9,934	11,584	42,262
Brokers and custodians*	58	56	69	64	178	425
Derivatives issuers	12	46	77	122	167	424
Currency exchange	105	124	79	39	28	375
Life insurance	3	0	1	0	1	5
MVTS	2,727	2,892	3,578	7,637	9,702	26,536

NBDTs	258	373	648	683	578	2,540
Payment Providers	0	2	1	1	35	39
Securities dealers	8	3	10	110	56	187
Other FIs*	54	115	136	205	207	717
Total	**8,781**	**10,906**	**12,492**	**18,795**	**22,536**	**73,510**

Table 2 - Suspicious activity reporting by other than financial institutions, 2017-2021

Sector	2017	2018	2019	2020	2021	Total
Accountancy practices	**0**	**4**	**28**	**18**	**15**	**65**
Law firms and conveyancers	9	89	127	120	96	441
Real estate agents	1	1	166	108	100	376
HVDs	1	0	10	15	14	40
DNFBPs total	**11**	**94**	**331**	**261**	**225**	**922**
TCSPs	2	3	1	1	5	12
Casino	83	88	73	70	71	385
TAB NZ (Wager and Gaming)	36	31	26	57	70	220
VASPs	1	7	18	54	252	332
Total non-financial	**133**	**223**	**449**	**443**	**623**	**1871**

Prescribed transaction reports

148. PTRs help build an intelligence picture across the entire financial system, providing necessary statistics and useful intelligence on the flow of cash and money in to and out of New Zealand. They also help make certain money laundering and terrorism financing typologies even more difficult to hide, and improving the detection, and thus disruption, of organised crime, fraud, and tax evasion. Since 2017, 496,862 PTRs have been submitted to the FIU totalling NZD 6.14 trillion.

Table 3 - Prescribed transaction reports total volumes and values, 2017-2021

		2017	2018	2019	2020	2021	Total
International Funds Transfer	Volume	5,021	63,207	141,148	108,330	107,324	425,030
	Value (NZD million)	16,448	950,340	1,649,297	1,734,869	1,774,353	6,125,307
Large Cash Transaction	Volume	739	18,133	21,338	15,685	15,937	71,832
	Value (NZD million)	431	3,381	5,464	3,110	4,137	16,523

		2017	2018	2019	2020	2021	Total
Total	**Volume**	5,760	81,340	162,486	124,015	123,261	496,862
	Value (NZD million)	16,879	953,720	1,654,761	1,737,979	1,778,491	6,141,830

149. The FIU uses PTRs to develop strategic insights, such as how cash is used in New Zealand. However, the FATF considered that the technology available to the FIU at the time of the onsite visit in March 2020 limited its ability to proactively harness PTR information, including as part of prioritising SARs for analysis. The FIU has subsequently implemented sophisticated analytical tools to improve its analytical capability, but it is too early to assess how effective this change has been.

Border cash reports

150. The FIU receives a large number of border cash reports (BCRs) from Customs; however, these are provided in physical form and must then be manually introduced into the FIU's database. As a result, the FATF did not consider BCRs are providing as much analytical value as they could. However, the BCR requirements were recently changed to allow reports to be completed electronically and thus can be more easily used to generate valuable intelligence.

Table 4 - Numbers of border cash reports (BCRs) submitted, 2017-2021

Year	2017	2018	2019	2020	2021	Total
BCRs completed on arrival	3877	4850	4524	1313	790	15,354
BCRs completed on departure	870	815	951	363	377	3376
Direction not recorded	286	206	58	0	0	550
Total	**5033**	**5871**	**5533**	**1676**	**1167**	**19280**

151. In addition, BCRs also provided value in terms of allowing Customs to confiscate undeclared or falsely declared cash. Between 2016 and 2020, Customs seized a total of NZD 1.95 million of undeclared or falsely declared cash, and multiagency operations were taken against cash smugglers and cash controller networks.

Financial intelligence received is turned into a range of products

152. The FIU produces a range of qualitative and quantitative products to disseminate to authorities using the financial intelligence received. These products, as well as financial intelligence more broadly, is regularly used by a wide range of New Zealand authorities to support investigations into money laundering and related offences and to trace proceeds of crime. However, the FATF noted the current process does not fully exploit the available intelligence and information and could be better utilised to identify suspicious activity by persons otherwise unknown. 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 once prioritised).

Table 5 - numbers of reports produced by FIU, 2017-2021

Product	2017	2018	2019	2020	2021	Total
Information reports	831	968	995	1159	785	4738
Intelligence reports	146	102	61	61	84	442
Strategic reports	10	7	14	8	6	45

153. The FIU's two most common reports are Information Reports and Intelligence (analytical) Reports. Information Reports comprise responses to requests for information, proactive releases responding to issues identified in the SAR prioritisation process or are ongoing structured releases that support investigations. Intelligence Reports provide a more in-depth analysis by the FIU of specific tactical cases, accounting for 8 percent of reports disseminated since 2017. In addition, the FIU releases less in-depth intelligence, such as SAR spreadsheets, which are used to quickly disseminate information to authorities to meet their operational needs.

154. The FIU conducts strategic analysis on a range of themes, trends and emerging risks, 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 45 were produced between 2017 and 2022. The FIU also conducts the NRA, which informs the SRAs and reporting entities' own risk assessments. Without a third NRA and up to date SRAs, reporting entities are less equipped to identify and understand their risks (*see* How well do we understand our risks).

FIU products are requested and used by a range of agencies

155. Financial intelligence products are disseminated to a wide range of New Zealand authorities to support their AML/CTF operations. Law enforcement agencies are able to obtain a range of financial information from the FIU through intelligence products and via the FIU database. Between 2015 and March 2020, the FIU received 3,750 requests for information, including 3,369 requests from domestic agencies.

156. Authorities request information from the FIU and in some instances, 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 between 2015 and 2020, with 13,834 person lookups conducted in 2019 (compared to average of 37,000 person lookups by FIU staff per annum). We anticipate this would increase once a direct data access framework is established, which would in turn increase the value of financial intelligence overall (see Information sharing).

157. Sector supervisors use financial intelligence for strategic and tactical purposes. Prior to onsite visits, 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 and gain a more detailed understanding of the business' risk profile. The Ministry also requests information from FIU in relation to an entity applying for an exemption in order to inform whether an exemption should be granted or declined.

Financial intelligence also directly supports law enforcement efforts

158. There are no statistics gathered that measure the impact financial intelligence produced and disseminated has on the outcome of investigations. However, the FATF reviewed some cases triggered by the FIU's analysis and concluded it was of high quality and value, although also noted that only a relatively small number of investigations are initiated on the basis of FIU reports alone. Nevertheless, the FATF

considered that New Zealand was substantially effective at investigating and prosecuting money laundering.

159. The FATF determined that cases showed that financial intelligence is being used across a spectrum of investigations relating to a variety of predicate offences, including drug trafficking, fraud, tax crime, terrorism and terrorism financing, and labour exploitation. In 2016-2019, the FIU supported 291 ML investigations and 1,482 investigations into other offences. We have provided two case studies to demonstrate the intelligence value provided:

Operation Grand X

Operation Grand X is a 2019 investigation focused on money laundering, benefit fraud and tax evasion. This operation commenced following Operation Grand, an investigation that targeted a Paua and Sea Cucumber poacher in Wellington.

Financial analysis identified anomalies in evidence provided by an associate during the forfeiture hearing. As a result, Grand X commenced and a significant financial review involving multiple bank accounts identified hundreds of thousands of dollars being remitted into his accounts from China. The review has identified that persons are involved in the Daigou trading platform, where high-value products were purchased in New Zealand and shipped to China and sold at vastly higher prices. That money was then being returned to New Zealand via bank accounts and tax avoided.

The FIU released four reports detailing a total of 8 Suspicious Activity Reports and 16 Prescribed Transaction Reports to the investigation team. The FIU also facilitated an Egmont request for information from the investigation team to an international partner to obtain financial intelligence relating to one of the suspects believed to have a financial footprint overseas.

Operation Spectrum

Operation Spectrum was an MBIE led investigation that commenced following a series of meetings between FIU and MBIE. Both agencies were receiving reporting in relation to suspected migrant exploitation and visa fraud.

The FIU conducted network analysis of relevant SARs to identify key entities within associated financial networks. During the course of the operation, FIU disseminated 6 separate reports and intelligence products detailing the content of approximately 81 SARs involving the subjects.

The investigation identified use of shell companies, false identities, fraudulent documentation, and use of nominee directors and shareholders to facilitate offending which included using subcontractors who were unlawfully in New Zealand or working in breach of their visas. Based on one snapshot presented by MBIE, the estimated loss in tax revenue in one area of the investigation was estimated at around $5.4 million over a 5-year period.

1.1.3. Deterrence of money laundering and terrorism financing

160. The Act seeks to deter money laundering and terrorism financing by imposing a range of obligations on businesses that are vulnerable to misuse, which makes it harder for illicit financial activity to occur. The AML/CFT supervisors are then responsible for ensuring that businesses understand their risks and obligations and take appropriate steps to ensure businesses comply. The Act prescribes the functions of an AML/CFT supervisor to monitor and assess the level of money laundering and terrorist financing risk across reporting entities, to provide guidance, to monitor compliance and to investigate reporting entities and enforce the Act.

161. Supervisors have three core supervisory tools; producing guidance, education, and engagement to ensure businesses understand their obligations, conducting desk-based reviews and onsite inspections to assess compliance, and taking enforcement action against businesses that fail to comply. Although these tools are effective, there

are some shortcomings in the Act in detecting and deterring money laundering and terrorist financing. There is also no regulatory framework in New Zealand for the supervision of businesses for targeted financial sanctions obligations.

The gaps in preventive measures limit the Act's ability to effectively deter

162. The starting point for an effective AML/CFT framework is ensuring that there are adequate measures in laws and regulations. New Zealand's preventive measures are set out in the Act and in its associated regulations but are also found in several other pieces of legislation, such as the *Financial Service Providers (Registration and Dispute Resolution) Act 2008*, the *Companies Act 1993*, and the *Reserve Bank of New Zealand Act 2021.*

163. As part of New Zealand's Mutual Evaluation, the FATF identified several areas that need to be strengthened. This includes improvements to strengthen supervision and implementation of preventive measures, improve the transparency of legal persons and arrangements, and ensure targeted financial sanction implementation is effective. The FATF also identified the need to address gaps and in the overall registration and licensing framework, as well ensuring the AML/CFT framework aligns with the FATF Standards. In particular, the FATF recommended addressing shortcomings for politically exposed persons, MVTS networks, dealers in precious metals and stones and the supervision of targeted financial sanctions obligations.

164. We consider that the gaps in our laws and regulations limit the extent to which money laundering and terrorist financing can be detected and deterred effectively. We make recommendations to close these gaps in Part B of the report (*see* Preventive measures).

Supervisors work to promote understanding of obligations and risks

165. Although the FATF was critical about the extent of preventive measures, they nonetheless considered that New Zealand supervisors make a genuine effort to engage with their sectors proactively. This has generally had a positive impact on compliance.

166. A range of methods are utilised by supervisors to promote understanding of risks and obligations, including guidance, joint triple-branded guidelines, codes of practice, sector-specific guidelines, factsheets, FAQs, newsletters, outreach programmes, training videos and webinars. While guidance and codes of practice are anticipated under the Act, newsletters and outreach programmes are established by supervisors as their own initiative. Supervisors also provide direct feedback to reporting entities based on findings from onsite inspections and desk-based reviews. Feedback is also provided more broadly through publications such as RBNZ AML/CFT updates, FMA's AML/CFT Monitoring Report and DIA's Regulatory Findings Report.

167. Businesses interviewed by the FATF commented on the usefulness of supervisory documentation and outreach. However, issues raised included a lack of sector-specific guidance, compliance with prescribed transaction reporting requirements and implementation of targeted financial sanctions. Businesses noted a need for more high quality, practical and relevant guidance to assist apply a risk-based approach and better understand their AML/CFT obligations.

However, understanding across sectors is generally mixed

168. Overall, the FATF determined that sectors had a mixed level of understanding of money laundering and terrorist financing risks and obligations. Banks and other financial institutions demonstrated a good understanding of risks and obligations. The level of understanding by MVTS providers varied, with concerns raised around the distribution of responsibilities for MVTS providers that have agency models. Non-bank financial institutions demonstrated a good level of understanding of their risks and obligations, although for smaller entities this was still in development.

169. The FATF determined the level of awareness and understanding of risks and obligations by law firms, conveyancers, accounting practices, real estate agents and HVDs in its early stages. In part, the variability of performance across sectors is due to the provisions of the Act being too generalised and open to interpretation. As a result, the FATF recommended supervisors maintain up to date sector specific guidance and feedback to assist businesses understand their obligations under the Act.

170. Similarly, the FATF concluded that there was mixed implementation of policies, procedures, and controls by businesses. The FATF found that banks and other financial institutions are generally stronger at implementing appropriate controls, while the implementation by non-financial sectors and VASPs varied. In particular, real estate agents and conveyancers were identified as having a less sophisticated understanding of risk, while VASPs encountered challenges understanding and applying appropriate measures.

171. For enhanced measures in high-risk scenarios, the FATF found that the extent and effectiveness of measures varied across businesses dependent on size and international exposure. Larger businesses and those part of international groups were more likely to take additional steps which are not required by the Act due the parent organisation requirements (such as domestic PEP and designations screening). However, smaller businesses were more likely to conduct manual or delayed sanctions and PEP screening, which may not be effective. The implementation of enhanced CDD measures by DNFBPs was found to vary and generally be less sophisticated than financial sectors. HVDs do not have enhanced CDD obligations under the Act.

172. We recognise that some of the challenges businesses are having result from uncertainty about the scope and nature of some of the requirements in the Act. This includes requirements relating to beneficial ownership and identifying and verifying a customer's source of wealth or source of funds. The identification of source of funds is identified as a common challenge across sectors, but particularly for large law firms, casinos, and the real estate sector. Accordingly, we make a series of recommendations aimed at addressing these uncertainties and ensuring robust controls in Part B of this report (*see* Preventive measures).

Supervisors generally conduct effective inspections of businesses

173. Supervisory activity is risk-based, which means that supervisors focus their efforts on the areas of higher risk. The inherently risky sectors are initially identified through process of developing the SRA (*see* implementing a risk -based approach), but this understanding is then supplemented by other information (such as adverse intelligence or a history of non-compliance) to determine residual risk. For high-risk sectors or businesses this results in more frequent or more intensive inspections, with the reverse true for low-risk sectors or businesses. For example, life insurers (which are low risk) are only subject to desk-based reviews, while TCSPs (which are high risk) are subject to more frequent or intensive onsite inspections.

174. Supervisors generally assess whether a business is complying with their obligations through the following two measures:

- **desk-based reviews** are often the first step of monitoring compliance and are a paper-based exercise. A desk-based review typically involves the AML/CFT supervisor reviewing a reporting entity's independent audit report, compliance programme and/or risk assessment.
- **onsite inspections** involve the AML/CFT supervisor physically visiting the business' premises and inspecting their policies, procedures, and controls. Inspections can last up to a week for larger reporting entities and can cover a range of topics, such as risk assessments, CDD, transaction monitoring, and submitting SARs.

175. Since 2017, the AML/CFT supervisors have conducted the following numbers of onsite inspections[5] and desk-based reviews:

Table 6 - onsite and desk-based reviews, 2017-2021

Supervisor	Total number of reporting entities	Type	2017	2018	2019	2020	2021
RBNZ	83	Desk-based	0	9	0	1	0
		Onsite	18	17	11	2	4
FMA	842	Desk-based	58	71	35	50	35
		Onsite	19	27	75	7	5
DIA	5,420	Desk-based	115	74	148	304	129
		Onsite	34	33	48	115	50
Total	6,345	**Desk-based**	**173**	**154**	**183**	**355**	**164**
		Onsite	**19**	**27**	**75**	**124**	**5**

176. The FATF considered that the use of onsite inspections was broadly appropriate. but identified issues around the scope and depth of supervision across sectors and ensuring that sector-specific vulnerabilities specified in the SRAs are considered. The FATF noted particular risks in the banking sector, given their significance to New Zealand's financial system and the wide availability of vulnerable products and services. We consider that the FATF's findings are still generally accurate and note that the COVID-19 pandemic has prevented AML/CFT supervisors conducting onsite inspections in 2020-21.

177. One of the FATF's findings was with respect to RBNZ being limited in the scope and depth of onsite inspections in the banking sector due to having insufficient resourcing. We note that efforts are underway to increase RBNZ's supervision resource and also recommend generally increasing the amount of resource available for the regime, including RBNZ (*see* Ensuring there are sufficient resources to deliver the regime).

Available remedial actions are applied in a generally effective manner

178. Remedial actions are generally approached by supervisors in an effective manner, with remediation reports provided after onsite inspections and desk-based reviews. However, the FATF noted there are deficiencies in the range and use of available sanctions (*see* Comprehensiveness of penalty regime). The range of civil sanctions under the Act include formal warnings, accepting an enforceable undertaking, seeking an injunction, or applying for pecuniary penalty from the High Court. Criminal sanctions are also available. The FATF found that sanctions applied by supervisors are generally in line with the number of supervised reporting entities and the overall level of compliance of each sector.

179. Since 2017, supervisors have applied a range of civil and criminal sanctions under the Act:

[5] One onsite inspection can cover multiple reporting entities due to a Designated Business Group.

Table 7 - Enforcement actions taken by AML/CFT supervisors, 2017- 2021

		2017	2018	2019	2020	2021	Total
RBNZ	Remedial action	17	11	19	12	19	78
	Public formal warning	0	0	0	0	1	1
	Enforceable undertaking	0	0	0	12	19	78
	Pecuniary penalty (NZD million)					1 (3.5 total)	1 (3.5 total)
FMA	Remedial action	9	7	9	4	3	32
	Public formal warning	1	1	1	0	1	4
	Private formal warning	9	10	0	8	9	36
	Court proceedings	0	0	1	0	1	2
DIA	Remedial action	76	168	51	170	37	499
	Public formal warning	2	4	1	2	0	9
	Private formal warning	3	0	0	2	3	8
	Pecuniary penalty (NZD million)	1 (5.29 total)	1 (0.36 total)	1 (4.01 total)	2 (7.6 total)	0	5 (17.26 total)
	Criminal sanction	0	0	1	1	0	2
	Enforceable undertaking	0	0	0	1	1	2
	Restraining injunction[6]	0	0	0	1	0	1

180. Despite the availability and use of these sanctions, the FATF identified a need for New Zealand to have enhanced, proportionate, and dissuasive sanctions but also recognised that supervision generally has a positive impact on compliance. The FATF suggested increasing the range of pecuniary penalties for non-compliance and to provide supervisors with the ability to impose administrative sanctions. We consider the FATF's findings are still accurate post the Mutual Evaluation, although we note that RBNZ and FMA have both obtained their first pecuniary penalties from the High Court.

Law enforcement is effective at prosecuting people and recovering assets

181. Although it is not directly within the scope of the Act, we note that investigating and prosecuting money laundering, terrorism financing, and recovering criminal assets will also have some deterrent effect. Some of this law enforcement effort is directly supported by financial intelligence collected under the Act (*see* Financial intelligence also directly supports law enforcement efforts) but is also generally relevant to considering how effective the overall AML/CFT regime is at deterring illicit financial activity.

182. The FATF determined that New Zealand has good capacity to investigate, prosecute and obtain convictions for money laundering across different types of proceeds-

[6] While there were no restraining injunctions granted within the reporting period, one interim injunction was granted on 03 May 2021

generating crime, stand-alone and third-party money laundering, foreign proceeds laundering and complex money laundering operations. Between 2017 and 2021, agencies have successfully prosecuted and convicted 395 individuals for money laundering. The FATF considered that the figures until 2020 were broadly in line with New Zealand's risk profile but noted that the priority has been recovery of assets and pursuing prosecutions for the predicate offences.

Table 8 - money laundering prosecutions and convictions, 2017-2021

Year	2017	2018	2019	2020	2021	Total
Case files	50	103	193	177	133	822
Individuals charged with ML	50	96	166	160	120	313
Individuals convicted	27	77	64	143	84	395

183. While the FATF determined that New Zealand authorities demonstrated their ability to obtain convictions for a range of money laundering cases, there questioned whether penalties imposed in every instance were sufficiently proportionate and dissuasive. These concerns would likely be exacerbated given recent prosecutions where the penalty does not appear to be sufficiently proportionate noting the amounts laundered.[7] Nevertheless, the FATF determined that New Zealand pursues recovery of criminal proceeds, instrumentalities, and property of an equivalent value as a high priority policy objective. A significant amount of proceeds has been recovered in New Zealand, from both domestic and foreign offending.

Table 9 - Total (Estimated) Value of Assets Taken from Criminals (NZD million)[8]

Financial Year	2015-16	2016-17	2017-18	2018-19	2019-20	2020-21	Total
Proceeds Restrained	112	130	74	88	263	99	822
Proceeds Forfeiture	17	76	27	28	34	120	313
Instrumentalities	0.2	0.6	0.9	1.1	0.0	0.2	3.60
Restraint Abandoned	0.67	0.44	0.64	3.81	0.30	0.03	5.89

184. The FATF determined that New Zealand authorities had the capability and capacity to effectively investigate and prosecute terrorist financing if required. They noted that New Zealand authorities conducted a thorough investigation into possible terrorist financing links to the Christchurch Mosque attack. The FATF also noted that, to date, New Zealand has not prosecuted any terrorist financing cases which is in line with its risk profile in New Zealand's national risk assessment.

[7] For example, Yinghui Zhang was sentenced to 12 months' home detention after laundering an estimated NZD 8.4 million over a 20-month period (New Zealand Herald (13 February 2022) Auckland businessman sentenced after police target professional money launderers in cover Operation Menelaus). Another person was sentenced to 11 months' home detention and deported after being convicted for laundering NZD 330,000 (Stuff (22 June 2022) NZ resident deported to India after laundering $330,000 for drug dealers).

[8] The values provided in this table are subject to change, particularly in terms of asset value. In addition, the values provided differ to those reported in New Zealand's Mutual Evaluation: particular assets which had a status of 'currently restrained' in the 2016/17 financial year (for example) may have since been forfeited (since the stats were originally pulled) therefore having a change in status and thus increasing the forfeiture count.

1.2. Maintaining and enhancing New Zealand's international reputation

185. Section 3(1)(b) states that a purpose of the Act is to maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force. We have assessed the extent to which the Act has achieved this purpose by considering the results of New Zealand's Mutual Evaluation, and the impact that this has had on markers of reputation.

186. Overall, the indicators are clear: New Zealand's AML/CFT framework has maintained and enhanced New Zealand's international reputation. This is of value because of the increased prominence ascribed to having an effective AML/CFT framework when conducting global business. This purpose of the Act can be considered as performing well and will be enhanced by our recommendations in this report. Many of the recommendations we make will address deficiencies identified by the FATF in the Mutual Evaluation and improve the effectiveness of our AML/CFT regime.

1.2.1. Compliance with the FATF Standards

187. New Zealand's Mutual Evaluation Report, which was adopted by the FATF in February 2021, is broadly positive. As outlined in the background to the review, the assessment had two components (*see* New Zealand was assessed by the FATF in 2020-21):

- **a technical compliance assessment**, which looked at whether we have met all the technical requirements of each of the 40 FATF Recommendations in our laws, regulations, and other legal instruments to combat money laundering, and the financing of terrorism and proliferation.
- **an effectiveness assessment**, which looks at the extent to which we have an effective framework to protect our financial system from abuse in the context of the risks it is exposed to. The assessment team looked at 11 key areas, or immediate outcomes, to determine the level of effectiveness of our efforts.

188. Overall, the FATF has concluded that our measures to combat money laundering and terrorist financing are delivering good results, but we need to focus more on improving the availability of beneficial ownership information, strengthening supervision, and implementing targeted financial sanctions. The FATF assessed New Zealand as broadly effective overall, and particularly effective at confiscating and restraining criminal assets and cooperating with our international partners. In particular, the FATF determined our effectiveness as follows:

Table 10 - New Zealand Immediate Outcome results, 2021

Rating and description	Results for New Zealand (Act specific outcomes underlined)
Low effectiveness – The Immediate Outcome is not achieved or achieved to a negligible extent. Fundamental improvements needed	Nil
Moderately effective – The Immediate Outcome is achieved to some extent. Major improvements needed.	IO 3 – supervision; IO 4 – preventive measures; IO 5 -beneficial ownership; IO 10 – terrorism financing related targeted financial sanctions; IO 11 – proliferation financing related targeted financial sanctions

Rating and description	Results for New Zealand (Act specific outcomes underlined)
Substantially effective – The Immediate Outcome is achieved to a large extent. Moderate improvements needed.	IO 1 – risk, policy, and coordination; IO 6 – financial intelligence; IO 7 – investigation and prosecution of money laundering; IO 9 – investigation and prosecution of terrorism financing
Highly effective – The Immediate Outcome is achieved to a very large extent. Minor improvements needed.	IO 2 - International co-operation; IO 8 – confiscation

189. However, our laws are less compliant with the FATF's technical requirements compared to most FATF countries. Several of the areas where New Zealand is lagging in compliance are contained in the Act, but other legislation is also relevant to New Zealand's overall technical compliance. The FATF assessed New Zealand's laws as follows:

Table 11 - New Zealand technical compliance results, 2021

Rating and description	Result for New Zealand (Act specific requirements underlined)
Not compliant – There are major shortcomings.	Nil
Partially compliant – There are moderate shortcomings.	R.7 – Targeted financial sanctions related to proliferation; R.12 – Politically exposed persons; R.14 – Money or value transfer services; R.16 – Wire transfers; R.18 – Internal controls and foreign branches and subsidiaries; R.19 – Higher risk countries; R.22 – Designated non-financial businesses and professions (DFNBPS): customer due diligence. R.23 – DNFBPS: other measures; R.24 – Transparency and beneficial ownership of legal persons; R.25 – Transparency and beneficial ownership of legal arrangements; R.26 – Regulation and supervision of financial institutions; R.28 – Regulation and supervision of DNFBPS
Largely complaint – There are only minor shortcomings.	R.1 – Assessing risks and applying a risk-based approach; R.5 – Terrorist financing offence; R.6 – Targeted financial sanctions related to terrorism and terrorist financing; R.8 – Non-profit organisations (NPOs); R.10 – Customer due diligence; R.11 – Record keeping.; R.13 – Correspondent banking; R.15 – New technologies; R.17 – Reliance on third parties; R.27 – Powers of supervisors; 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; R.37 – Mutual legal assistance; R.38 – Mutual legal assistance: freezing and confiscation; R.39 – Extradition; R.40 – Other forms of international co-operation
Compliant – There are no shortcomings.	R.2 – National co-operation and co-ordination; R.3 – Money laundering offence; R.4 – Confiscation and provisional measures; R.9 – Financial institution secrecy laws; R.20 – Reporting of suspicious transactions; R.21 – Tipping-off and confidentiality; R.29 – Financial intelligence units; R.30 – Responsibilities of law enforcement and investigative authorities.

1.2.2. Impact on New Zealand's reputation

New Zealand is in the FATF's enhanced follow-up process

190. The FATF has three levels of follow up:

- **regular**: the default monitoring mechanism, based on a system of regular reporting,
- **enhanced**: a more intensive process of follow-up, for countries with deficiencies, or countries making insufficient progress, and
- **placed into International Co-operation Review Group review**: the most intensive process of follow-up, reserved for high-risk jurisdictions.

191. New Zealand is in enhanced follow up, however, as are many comparative jurisdictions, including Australia, the United States of America, and Canada. New Zealand is ranked fifth overall by the FATF for the effectiveness of our AML/CFT framework, but 56th in terms of our technical compliance.

192. In a May 2022 follow-up and technical compliance re-rating report, the FATF has upgraded Recommendation 25 from partially compliant to largely compliant.[9] This demonstrates the progress that New Zealand is making in addressing FATF recommendations. We anticipate that many of the recommendations provided in this report will improve both technical compliance and effectiveness. This could result in Recommendations 14 (MVTS Providers), 16 (Wire Transfers), 19 (Higher risk countries), 22 (DFNBPs: CDD) and 23 (DNFBPs: other measures) being upgraded and New Zealand likely exiting enhanced follow up (see Preventive measures).

Compliance with the FATF supports the adoption of other conventions and agreements

193. Both the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime assess aspects of AML/CFT measures. New Zealand is currently undergoing a review against both Conventions. We anticipate that our compliance with the FATF's recommendations will support a positive assessment of our adoption of the parts of those Conventions that relate to money laundering.

194. In 2018, New Zealand was assessed against the Organisation for Economic Cooperation and Development's (OECD) Standard for Exchange of Information on Request (EOIR). New Zealand was ranked compliant, meaning that the EOIR Standard had been met. New Zealand is one of the few countries who is ranked compliant, and this is likely a reflection of New Zealand's effective adoption of FATF Recommendations.

New Zealand continues to maintain a positive Basel Index rank

195. The Basel Index is an independent country ranking and risk assessment tool for money laundering and terrorism financing, produced by the Basel Institute on Governance. The Index provides holistic money laundering and terrorism financing risk scores based on data from 17 publicly available sources such as the FATF, Transparency International, the World Bank, and the World Economic Forum.

196. The Index assesses five elements and uses ten-point scale (0-10), with 10 indicating the most risk and 0 indicating the least risk. The five elements are:

- **quality of AML/CFT framework (65 percent)**, which is based upon an assessment of: FATF Mutual Evaluation Reports, Tax Justice Network Financial Secrecy Index, US State Department International Narcotics Control Strategy Report,

[9] Note that the FATF has subsequently upgraded New Zealand's compliance with Recommendation 25 from partially compliant to largely compliant: https://www.fatf-gafi.org/media/fatf/documents/reports/fur/Follow-Up-Report-New-Zealand-2022.pdf

- **corruption and bribery Risk (10 percent)**, which is based upon an assessment of: Transparency International Corruption Perceptions Index, TRACE Bribery Risk Matrix,
- **financial transparency and standards (10 percent)**, which is based upon an assessment of: World Bank Extent of Corporate Transparency Index, WEF Global Competitiveness Report – Strength of auditing and reporting standards, WEF Global Competitiveness Report – Regulation of securities exchanges, World Bank IDA Resource Allocation Index – Financial sector regulations,
- **public transparency and accountability (5 percent)**, which is based upon an assessment of: International IDEA Political Finance Database – Political disclosure, International Budget Partnership Open Budget Index – Budget transparency, World Bank IDA Resource Allocation Index – Transparency, accountability, and corruption, and
- **political and legal risk (10 percent)**, which is based upon an assessment of: Freedom House: Freedom in the World and Freedom in the Media, WEF Global Competitiveness Report – Institutional pillar, World Justice Project Rule of Law Index.

197. Overall, New Zealand has a Basel Index of 3.52, which indicates that New Zealand is a relatively low-risk jurisdiction. A Basel Index of this number ranks New Zealand as number one in the East Asia and Pacific region. Australia ranks third in this region. This is a positive indicator and demonstrates the strength of New Zealand's AML/CFT framework in relation to maintaining and enhancing New Zealand's international reputation. More generally, within all 203 jurisdictions assessed by the Basel Index, New Zealand ranks 13, with Estonia ranked number one with an index ranking of 2.34. Australia is ranked 18th, the United Kingdom 30th and the United States of America 49th

Table 12 - Basel Index scores for New Zealand, Australia, UK, USA (2022)

	Overall Score	AML/CFT Framework	Corruption and Bribery	Financial Transparency	Public Transparency	Political and Legal Risk
New Zealand	3.52	4.60	0.86	2.69	1.15	1.18
Australia	3.76	4.76	2.08	2.25	1.05	1.84
UK	4.04	4.98	1.94	3.11	1.50	2.20
USA	4.60	5.67	3.01	2.88	1.20	2.69

However, we continue to have some levels of financial secrecy

198. The Financial Secrecy Index (FSI) ranks each country based on the extent to which the country's financial and legal system allows individuals to hide and launder money extracted from around the world. The FSI grades each country's financial and legal system with a secrecy score out of 100 where a score of 0 is full transparency and a score of 100 is full secrecy. The country's secrecy score is then combined with the volume of financial services the country provides to non-residents to determine how much financial secrecy is supplied to the world by the country.

199. New Zealand was ranked 53rd in the 2022 Financial Secrecy Index with a score of 230, based on a fairly high secrecy score of 62.95, and a higher score and ranking indicates a worse performance overall. By comparison, the US ranked first (with a score of 1951), the UK ranked 13th (with a score of 547), Canada ranked 28th (with a score of 349), and Australia ranked 37th (with a score of 318).

Panama, Paradise, Pandora papers all show misuse of New Zealand structures

200. The leak of 12 million documents from the Panamanian law firm Mossack Fonseca (known as the Panama Papers) implicated a large number of New Zealand foreign trusts in tax avoidance and money laundering. More recently, a New Zealand formed company was connected to Aleksander Vinnik, who was arrested for money laundering by Greek authorities in 2017 at the request of the United States. New Zealand Police has restrained $140 million in an offshore bank account associated with Vinnik. This indicates that, despite positive progress, New Zealand legal persons and arrangements are still at risk of misuse.

1.3. Contributing to public confidence in the financial system

201. As outlined in the Methodology section, the extent to which this object has been achieved has been difficult to assess due to the lack of available data. Instead, we have assessed the delivery of this object by examining several proxy measures we anticipate would decline if there was a loss of confidence in the financial system. This enables us to determine whether any loss in public confidence has occurred following the AML/CFT reforms in 2009 and 2017.

202. We were not able to detect any significant impact on any of these measures following the 2017 reforms, negative or otherwise. Although none of these indicators directly measure the Act's impact on public confidence, this finding appears to support the conclusion that public confidence in the financial system is not significantly affected by the AML/CFT regime.

203. Further, the public's main exposure to the AML/CFT regime is likely for one of two reasons: a large penalty has been imposed against a business or the person has been asked to prove their identity. New Zealand regulators have not imposed significant penalties against businesses for failing to comply with the Act compared to other countries, including Australia (largely due to the low penalties available – see Comprehensiveness of penalty regime). The biggest penalty imposed against a bank was NZD 3.5 million against TSB Bank; this pales in comparison to AUD 1.3 billion imposed against Westpac by Australian regulators in 2020. It is possible that the public has maintained confidence due to the relatively low penalties in New Zealand, but we have not been able to test whether this is the case due to the lack of available data.

1.3.1. Investor confidence

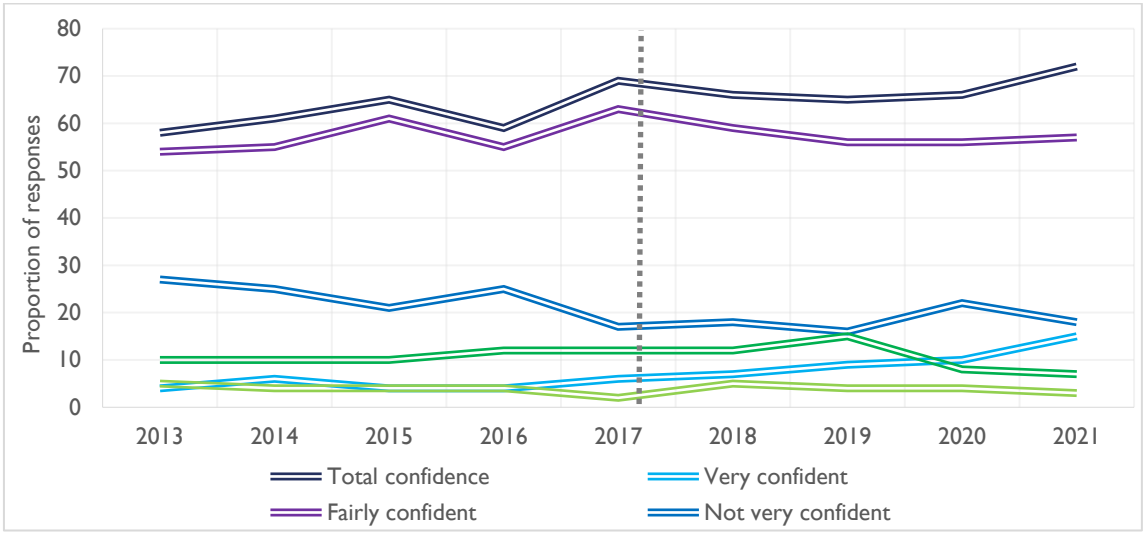


Figure 1 - Investor confidence (FMA) (2013 - 2021)

204. Investor confidence has been steadily increasing over time, with the result for 2021 finding that 72 percent of investors are confident in the country's financial markets. The top reasons people gave in 2021 for feeling confident was observing or experiencing a strong bounce back from COVID-19, having trust in the market, Government, or authorities responsible for regulation, and having high levels of knowledge of the market. Importantly, we cannot detect any significant decrease following the 2017 reforms – the average confidence level post-reform was 67.6 percent, while the average pre-reform was 60.75 percent. As such, we consider that the Act has not negatively impacted investor (and in turn, the public's) confidence in the financial system.

1.3.2. Ease of doing business

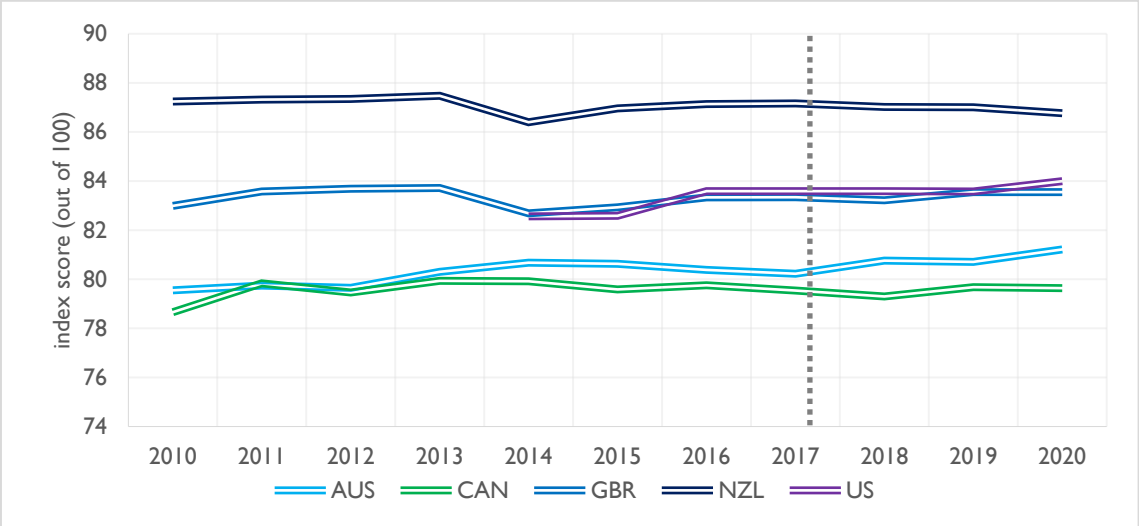


Figure 2 - Ease of Doing Business index (2010-2020)

205. New Zealand consistently ranked at or near the top of the World Bank's Ease of Doing Business index while it was measured, and higher than our close allies. As with investor confidence, we cannot detect a significant change in the ease of doing business following the 2017 reforms. This suggests that the 2017 amendments (and the Act more generally) has not negatively impacted the ease of doing business in New Zealand. As such, people who are confident in the financial system because it is easy to do business are unlikely to have that confidence impacted by virtue of the Act.

1.3.3. New and total business registrations per 1,000 people

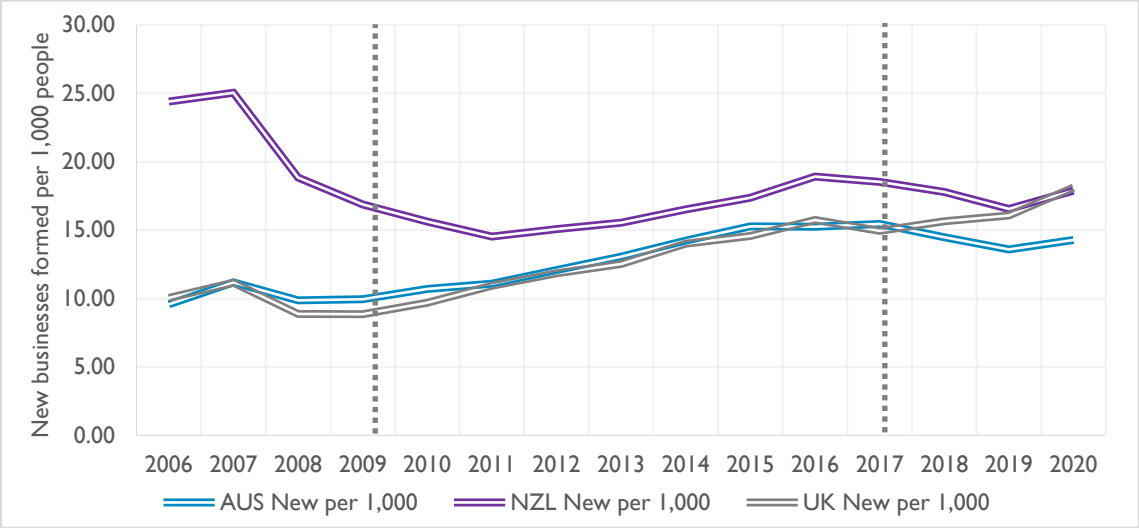


Figure 3 - New business registrations per 1,000 people

206. People continued to want to form businesses in New Zealand throughout the time the Act has been in operation, including post the 2017 reforms. While there was a noticeable decline in 2007-08, this is likely a result of the 2008 global financial crisis and predated the Act being passed in 2009. The rate of new business registrations also does not appear to have been impacted by either the Panama or Paradise papers in 2016 and 2017 respectively, despite both showing that New Zealand legal structures were involved in illicit financial activity. Further, we have not been able to identify a significant drop in the total number of businesses per capita throughout the lifespan of the Act, which could indicate businesses leaving New Zealand and a loss of confidence:

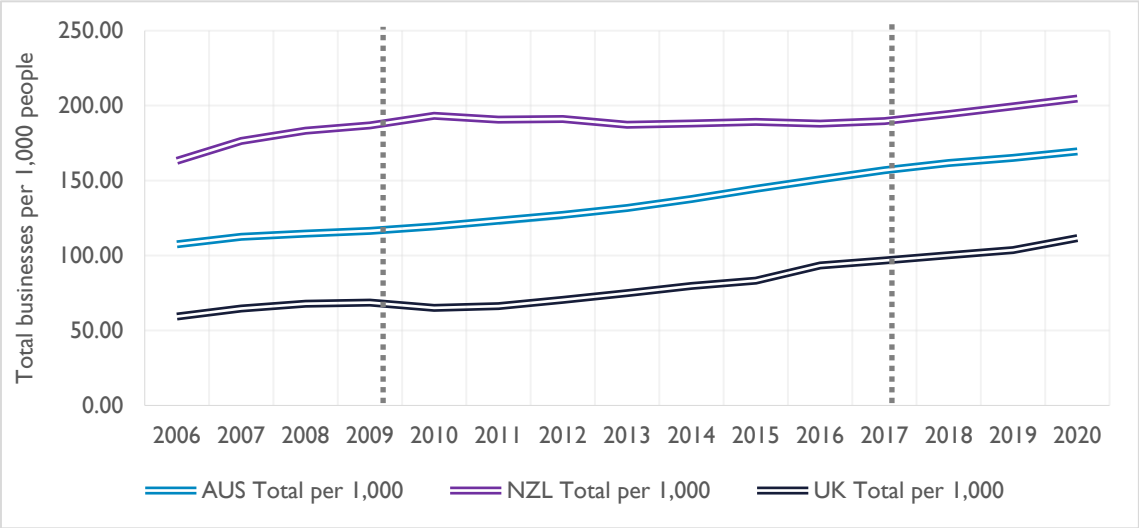


Figure 4 - total business registrations per 1,000 people

207. Accordingly, it appears that people continue to have sufficient confidence in the financial system to register businesses in New Zealand, and there has been no significant reduction in the total number of businesses throughout the lifespan of the Act.

1.4. Facilitating coordination amongst businesses, supervisors, and agencies

208. The final purpose of the Act is that it facilitates cooperation amongst reporting entities, AML/CFT supervisors, and various government agencies, in particular law enforcement and regulatory agencies.

1.4.1. Cooperation within the AML/CFT regime

209. The FATF considered that domestic coordination and cooperation are strengths of New Zealand's AML/CFT system. Agencies have a strong tradition of coordination and collaboration, and continually work to improve the flow of information between them. Authorities use a variety of mechanisms and fora to share information, coordinate efforts, and collaborate with partner agencies and the private sector.

210. The Act establishes the National Coordination Committee (NCC) as the central mechanism for coordinating AML/CFT policy and activity (section 150). The NCC consists of a representative of the Ministry, Customs, the AML/CFT supervisors, the Commissioner of Police, and other invited agencies, including Inland Revenue, the Serious Fraud Office, the Ministry of Business, Innovation and Employment, and the Ministry of Foreign Affairs and Trade. From time to time, the NCC has also established working or oversight groups to facilitate greater coordination and cooperation, such as supporting New Zealand's submissions and engagement on the Mutual Evaluation and conducting the statutory review of the Act. The NCC also developed a National AML/CFT strategy and action plan, which coordinates cross-agency efforts until the end of 2023.

211. The Sector Supervisors Forum (SSF) operates as a working group of the NCC and facilitates coordination and a consistent approach to supervision. The SSF meets fortnightly and considers a variety of issues such as operational policy, emerging risks, consistency issues raised by reporting entities, and development of AML/CFT guidance. The Forum also coordinates supervisors' relationships with other parts of government and international partners, joint supervision, joint onsite inspections, training, outreach, and technical assistance.

212. As part of the development of the AML/CFT Amendment Act in 2017, the NCC established a separate Oversight Committee that engages with strategic issues that may impact the AML/CFT system, as well as considering significant resourcing decisions. The Oversight Committee is comprised of senior leaders from the core AML/CFT agencies, and the NCC can refer strategic issues, significant resourcing decisions, and unresolved matters to the Oversight Committee for guidance as required.

213. However, we note that the existing coordination and cooperation mechanisms have been insufficient to address or resolve two key areas identified by submitters, namely delays to updating the NRA and inconsistent applications of the law from the AML/CFT supervisors. In addition, the coordination structure has not been successful at addressing underground remittances, which could be resolved through an operational project using the existing legislative powers and offences.

1.4.2. Cooperation with related regimes

214. The FATF also assessed the extent to which the AML/CFT regime coordinates and cooperates with other related regimes, such as the broader efforts to combat transnational organised crime, terrorism, and proliferation.

215. As money laundering is a facilitator of organised crime, there are strong linkages between the Transnational Organised Crime (TNOC) strategy and AML/CFT regime. The chair of the National Coordination Committee is a member of the governance bodies for the TNOC strategy.

216. The FATF stated that the operational cooperation and coordination by authorities on countering financing of terrorism is strong, flexible, and responsive to cases that emerge, working through informal coordination within New Zealand's highly inter-connected public sector. However, while individual agencies were effective in responding to terrorist financing risks they identify, the FATF determined that, based on discussions during the onsite visit, not all agencies were clear about the terrorist financing elements of New Zealand's broader counterterrorism efforts.

217. There are limited fora for coordination of AML/CFT and counter-terrorism work programmes. The Chair of the NCC and member agencies are also members of the Counter-Terrorism Coordination Committee (CTCC) and several of its working groups, although typically from different parts of the relevant agency. Apart from New Zealand Police, which is represented by the FIU but not business units responsible for counterterrorism, other key counter-terrorism agencies are not represented on the NCC. The Chair of the CTCC is not involved with the NCC and there are no mechanisms for coordination of the AML/CFT and counter-terrorism programmes.[10]

218. Counter-proliferation programmes face similar coordination challenges due to the governance structures mentioned above. All agencies working on counter-proliferation issues, including proliferation finance, are represented on a working-level forum, the Counter-Proliferation Forum (CPF), under the Officials Committee for Domestic and External Security Coordination which facilitates information sharing and coordination. The Ministry, the FIU, and members of the NCC participate in the Counter-Proliferation Forum. The Ministry of Foreign Affairs and Trade chairs the CPF and is represented in the NCC, and the New Zealand Police are represented in both fora, which can provide an opportunity for better coordination of counter-proliferation programmes.

219. Law enforcement cooperation occurs primarily through the free flow of information between agencies, including with the FIU and other agencies on a case-by-case basis. The *Privacy Act 2020* and related legislation enables lawful information sharing and access for money laundering and terrorist financing and associated predicate offences. The MER stated that that there is a very high degree of formal and informal cooperation among LEAs. This permissive environment has enabled LEAs to cooperate effectively against high-risk criminal targets.

[10] Note that we recommend additional agencies are invited to the NCC to ensure greater coordination between regulatory regimes, *see* Coordinating within the regime and between other regimes.

CHAPTER 2

How the regime has operated

Summary

220. This chapter considers how the regime has operated or delivered its outcomes in terms of the cost of the regime, overall regulatory maturity, and consistency with Te Tiriti o Waitangi. Reporting entities to were asked to complete a survey of their estimated costs for the financial year ending 31 March 2022, which was used to derive the estimated per-business cost as well as a total private sector cost of the regime. This was then combined with the actual costs from the public sector to determine the total per annum cost of the regime. We similarly assessed the regulatory maturity of the AML/CFT regime by sending a survey to everyone in government who works on the regime. Finally, we assessed the consistency of the regime with Te Tiriti by considering the extent to which the Crown has operated consistently with the principles of Te Tiriti as expressed by the Waitangi Tribunal.

221. We estimate that the AML/CFT regime costs New Zealand approximately NZD 260 million per annum, split between the private sector (NZD 246 million) and the public sector (NZD 14 million). In particular, we estimate that DNFBPs and high-value dealers spend approximately NZD 132 million per annum, which is roughly consistent with the cost estimates produced for Phase 2. While the amount spent a significant, we also estimate that the regime has significant monetary and non-monetary benefits, including disrupting NZD 1.7 billion worth of illegal drugs and fraud and NZD 5 billion of broader criminal activity over a ten-year period. We also note that not having an AML/CFT regime, or having a significantly weaker regime, would result in New Zealand being identified by the FATF as a high-risk jurisdiction, and result in an estimated reduction of capital inflows of between 4.6 percent and 10.5 percent of GDP.

222. In terms of regulatory maturity, the average scores from the survey suggest that the AML/CFT regime is generally defined and evolving, which indicates that there is recognition of the need for shared outcomes and more consistent ways of working with work underway to support more coordinated approaches across the system. However, given the regime has been in place for 12 years, we consider that this result is lower than it should be. A particular area of weakness identified was the low levels of resourcing of the regime, which appears to be causing underperformance in other areas (specifically the regime's efficiency, effectiveness, and durability). However, the regime does appear to be sufficiently mature with respect to its governance, leadership, and strategic direction.

223. Finally, we consider that the Crown can and should do more to satisfy its duty to be sufficiently informed about whether there are impacts for Māori or Māori interests in the operation of the Act. We note that there has been little, if any, engagement with Māori throughout the course of the Act's operation. This is despite there likely being some Māori interests in the Act resulting from impacts on the criminal justice, financial inclusion, data sovereignty, and the operation of post-settlement governance entities.

2.1. Cost of the regime

224. We have received a large amount of feedback from the public about the costs of the regime, both in general and to their business while it has been operational. This was reiterated as part of the public consultation process, with several submitters raising concerns about the cost of compliance. In particular:

- several submitters noted that the regime has had significant impacts on the profitability of their business or has had negative impacts on their business' productivity.
- others noted that the AML/CFT regime has meant that some transactions are no longer viable for their business or has led to the business declining to take on new customers or clients.
- a few submitters were concerned about the large amount of work that needs to be done to comply and understand what is required, which is particularly challenging for small businesses.
- finally, submitters noted that an AML/CFT service industry has emerged, that is able to charge large amounts of money to support compliance, but for questionable quality or value in the support provided.

225. In line with submitter feedback, we have examined the cost of the AML/CFT regime for businesses and compared that to estimates produced as part of developing AML/CFT reforms in 2009, 2015, and 2017. We have also reported on how much AML/CFT agencies have spent delivering their functions under the Act.

2.1.1. Private sector costs of the regime

Cost estimates for the reforms in 2009, 2015, and 2017

226. The Act was introduced and passed in 2009 and then substantively amended in 2017 (known as 'Phase 1' and 'Phase 2' respectively). In addition, the Act was reformed in 2015 following the *Organised Crime and Anti-Corruption Legislation Bill* requiring Prescribed Transaction Reports (PTRs) to be submitted. For each reform package, the Ministry conducted a cost-benefit analysis to estimate the costs of the policy changes for both the Government and for the private sector.

227. Prior to the Act coming into force, banks and other financial institutions had similar but more limited obligations under the *Financial Transactions Reporting Act 1996* (FTRA). Accordingly, for Phase 1, we estimated the additional costs these businesses would have from complying with the more stringent AML/CFT obligations. This estimate was an additional approximately NZD 97 million as start-up costs, with businesses incurring an additional NZD 21 million each year thereafter. Adjusting for inflation, this estimate would now be NZD 126.02 million as start-up costs and NZD 27.47 million per annum if implemented today. However, we are unable to provide total estimates for the Phase 1 reforms as we were unable to locate any cost estimates produced to support the FTRA.

228. For the introduction of PTR reporting, we estimated the cost of complying to be dependent on the extent to which a business had current record keeping and reporting systems that enabled electronic reporting through to goAML. We noted that the cost for a business lacking existing transaction reporting capabilities would indicate between NZD 0.85 and NZD 1 million. However, we did not estimate the total costs to the regime from this change.

229. For Phase 2, we contracted an external party (Deloitte) to conduct a business compliance cost study for lawyers, accountants, real estate agents, conveyancers, and high-value dealers. This assessment indicated the start-up costs for these sectors would range between NZD 71.9 million and NZD 313 million, with total ongoing costs between NZD 63.7 million and NZD 223.2 million. Adjusting for inflation, this estimate would now be between NZD 82.11 million and NZD 357.45 million in start-up costs, with ongoing costs of NZD 72.75 and NZD 254.89 million per annum if implemented today.

Table 13 – Estimated private sector costs of compliance - Phase 2 (2017)

Total	Establishment costs (Year 1) (NZD million)		Ongoing costs (per annum) (NZD million)		Average cost per client or transaction (based on high end cost) (NZD)	Estimated number of businesses within the sector	Estimated number of reporting entities
	Low	High	Low	High			
Lawyers and conveyancers	16.1	80.9	14.3	59.6	37.76 / client	1,919	1,572
Accountants	25.4	101.8	22.7	75.5	64.40 / client	2,433	2,223
Real Estate	13.3	35.0	11.8	23.1	355.88 / transaction	1,019	1,006
Motor Vehicle Dealers	13.9	66.8	12.1	45.7	77.65 / transaction	3,255	2,106
Jewellery	3.2	10.7	2.8	7.1	3.37 / client	640	229
Other	N/A	18.8	N/A	12.2	-	467	467
Total	**71.9**	**313.0**	**63.7**	**223.2**		**9,733**	**7,603**

230. This estimate was then used as part of a full cost-benefit analysis, which indicated that the total cost to Phase 2 businesses (such as lawyers) would be between NZD 0.8 to NZD 1.1 billion over 10 years, or approximately NZD 91.36 to NZD 125 million per annum after adjusting for inflation. Combined, these estimates indicate that the AML/CFT regime should cost the private sector between NZD 118.83 and NZD 152.47 million per annum in ongoing costs.

231. While the Phase 1, PTR, and Phase 2 estimates suggested potentially significant costs, we note each assessment indicated a likely positive return on investment:

- **for Phase 1,** the net quantifiable benefit was estimated to be between a net cost (no benefit) of NZD 17 million and net benefit of NZD 59 million, resulting from increased detection and deterrence of serious crime, improved international reputation, improved efficiency in the economy, improved risk management, and improved competitiveness. Adjusting for inflation, this estimate would suggest a net quantifiable benefit of between a net cost of NZD 22.14 million to a net benefit of NZD 76.84 million if enacted today.

- **for PTRs**, we estimated that the added value for improved law enforcement intelligence would be between NZD 12 and NZD 88 million per annum. We estimated this change would also reduce the harm to society from economic crime, reduce the impact of international wire transfers and cash deposits, lead to more assets being identified and restrained, and increase identification of victims of fraud.

- **for Phase 2**, the net quantifiable benefit was estimated to be between a net cost of NZD 20 million and net benefit of NZD 1.7 billion through disrupting illegal drugs and fraud over a ten-year period.

232. Over and above the specific benefits identified in previous assessments, we also note that the various reforms would lead to strategic benefits that are difficult to accurately assess. For example, for Phase 2, we estimated there would be a further NZD 5 billion in broader criminal activity disrupted (including because offenders would have less money to reinvest into illegal ventures or will be deterred from committing

crime). The change would also result in a reduction of an estimated NZD 800 million in social harm related to the illegal drug trade. These benefits were not included in the overall calculation as they are inherently difficult to quantify with any degree of certainty.

233. In addition, the costs of not having an AML/CFT regime or having a weak regime are significant. The FATF publicly identifies high-risk jurisdictions through what is informally known as its 'greylist', and this identification is typically based on how well a country does as part of their Mutual Evaluation. The International Monetary Fund estimates that being grey-listed results in an average reduction of capital inflows of 7between 4.6 percent and 10.5 percent of GDP, resulting from an overall reduction in investments in that country. If New Zealand had no AML/CFT regime or a weaker regime, we estimate that the resulting impact would be a loss of between NZD 15 and 35 billion of capital inflows.[11]

Estimated actual private sector costs for financial year ending 31 March 2021

234. We contracted a third-party research provider (Nexus Research) to survey reporting entities to assess whether the estimates in 2009 and 2017 are in line with the actual costs experienced by businesses. This survey was sent to all reporting entities between 31 March 2022 and 27 April 2022 and asked respondents to estimate their high-level cost pressures businesses experience, specifically labour, software, and tools, and third party or vendor costs for the past financial year (for full detail of methodology, see Understanding the costs of the regime)

235. The key finding of the survey is that, on average, businesses spent NZD 62,000 per annum managing their financial crime obligations for the financial year ending 31 March 2022. However, as noted in the Methodology and approach, "financial crime obligations" is inclusive of AML/CFT but also includes other obligations such as anti-bribery or corruption and complying with sanctions obligations.

236. Very small businesses (0 – 5 employees) on average spent NZD 25,000, while large businesses spent on average NZD 747,000 per annum. Labour was the predominant source of costs for businesses, followed by vendor costs and then software costs (although RBNZ reporting entities tended to spend significantly more on software compared with other sectors):

Table 14 – average costs by cost pressure and sector for FY ending 31 March 2022

Average cost by type	Proportion	Average costs (NZD 1,000)			
		Overall	DIA	FMA	RBNZ
Employee / labour	88%	51.5	43.9	69.6	716.4
Software	4%	2.1	1.7	3.7	306.1
Vendor, third party costs	8%	4.8	4.0	8.2	35.9
Sum of averages	100%	58.4	49.3	81.5	1,058.4

237. Respondents indicated that, on average, 63 percent of employee time was spent on AML/CFT obligations, indicating that AML/CFT is the majority of financial crime costs. Using the proportion of time spent on AML/CFT obligations to isolate the AML/CFT specific labour costs results in the following cost estimates:

[11] Mizuho Kida and Simon Paetzold (2021) *IMF Working Paper – the Impact of Grey-Listing on Capital Flows: An Analysis Using Machine Learning*, available at https://www.imf.org/-/media/Files/Publications/WP/2021/English/wpiea2021153-print-pdf.ashx. The approximately NZD 25 billion impact is based on the reported 2020 GDP of USD 212.5 billion or NZD 325.2 billion.

Table 15 – estimated AML/CFT costs for FY ending 31 March 2022 by supervisor

	Overall	DIA	FMA	RBNZ
Average per cost pressure (NZD 1,000)				
• AML/CFT specific labour costs	28.8	24.7	42.5	559.2
• Software	2.1	1.7	3.7	306.1
• Vendor, third party costs	4.8	4.0	8.2	35.9
Average total costs (NZD 1,000)[12]	38.8	32.9	58.1	921.8
Number of reporting entities	6,345	5,420	842	83
Total cost per annum (NZD million)	**245.9**	**178.5**	**48.9**	**76.5**

Table 16 – estimated AML/CFT costs for FY ending 31 March 2022 by type

	Overall	Financial Institution	DNFBP	HVD	Casino, TAB
Average per cost pressure (NZD 1,000)					
• AML/CFT specific labour costs	28.8	54.1	22.3	23.2	1,110.6
• Software	2.1	6.1	1.3	3.6	76.0
• Vendor, third party costs	4.8	9.6	3.3	5.3	233.0
Average total costs (NZD 1,000)	35.7	69.8	26.9	32.1	1419.6
Number of reporting entities	6,345	1,892	4,343	106	4
Total cost per annum (NZD million)	**245.9**	**144.4**	**128.2**	**3.9**	**5.7**

238. We recognise that the estimated total costs based on the survey are significantly more than the combined estimates from 2009 and 2017. However, this is largely due to the Phase 1 estimate focusing on the additional costs experienced by businesses, rather than the total costs of complying with the Act compared to the FTRA. Further, PTRs were introduced in 2015 following Phase 1, which could be the reason why RBNZ respondents are spending significantly more on software compared to other sectors. The 2017 estimate appears to be more accurate: the total cost per annum for DNFBPs (including high-value dealers) is NZD 132.04 million, which equates to approximately NZD 1.3 billion over 10 years.

239. In terms of comparison to previous years, a large majority (77 percent) of respondents indicated that last year's costs were either very similar or fairly similar to previous years. This appears to be consistent with another finding of the survey, where only a small proportion (approximately 18 percent) of respondents noted that there was a significant development in the past year that impacted their obligations and costs. The significant developments were typically updating AML/CFT

[12] Note that the average total costs do not equal the sum of the average costs for each cost pressure. This is a result of using trimmed averages: *see* Understanding the costs of the regime.

programmes or risk assessments, but also included remediation work or changing business activities, products, or delivery methods which impacted risks.

240. While the survey was unable to break down the specific costs associated with each obligation, it did ask respondents to identify the most and least expensive obligations overall. Most respondents indicated that risk assessments and compliance programmes were the most expensive obligation, followed by section 59 audits, standard customer due diligence (excluding address verification), and enhanced customer due diligence for trusts. This finding likely reflects that these costs are experienced by almost every business in the regime irrespective of the size of the business or the nature of their activity.

Table 17 – six most expensive compliance obligations by sector (2021)

Compliance obligation	Total	DIA	FMA	RBNZ
Risk assessment and compliance programme	22%	20%	28%	19%
Section 59 audits	21%	20%	25%	13%
Standard customer due diligence (excluding address verification)	17%	18%	11%	13%
Enhanced customer due diligence for trusts	16%	17%	13%	0%
Ongoing customer due diligence	9%	9%	7%	13%
Record keeping	7%	7%	7%	0%

241. In terms of least expensive obligation, respondents indicated that these were suspicious activity reporting, address verification, and PEP and sanctions screening. By contrast to the most expensive obligations, these obligations typically do depend on the nature and risk of the business. Some low or moderate risk businesses may never detect a suspicious activity report, and thus would never have to spend time submitting a SAR. The same is true for PEP and sanctions screening – businesses are not required under New Zealand law to conduct sanctions screening, but some multinational businesses typically do as it is required by their parent company's policy. Finally, we note that address verification is a small part of overall CDD, which similarly accounts for it being considered one of the least expensive obligations.

Table 18 – six least expensive compliance obligations by sector (2021)

Compliance obligation	Total	DIA	FMA	RBNZ
Suspicious activity or suspicious transaction reporting	53%	52%	58%	69%
Address verification	51%	51%	49%	44%
PEP and sanctions screening	46%	45%	55%	25%
Record keeping	43%	44%	39%	47%
Prescribed transaction reporting	38%	37%	43%	23%
Account/transaction monitoring	35%	36%	32%	0%

2.1.2. Public sector costs of the regime

242. The six agencies with responsibilities for delivering AML/CFT functions have spent the following between the 2017/18 financial year and 2020/21 financial year:

Table 19 – Public sector costs for AML/CFT (2017/18 - 2020/21) (NZD millions)

Agency	2017/18	2018/19	2019/20	2020/21
MOJ	1.83	1.07	0.67	0.33
DIA	4.00	7.77	8.35	8.45
FMA	0.69	0.54	1.11	1.19
RBNZ	0.63	0.58	0.68	0.66
FIU	2.86	3.56	3.20	3.50
Customs	0.09	0.10	0.11	0.09
Total	**10.09**	**13.62**	**14.13**	**14.21**

2.2. Maturity of the regulatory system

243. Assessing the regulatory maturity of the AML/CFT regime examines the extent to which the regime takes a whole-of-system, proactive, collaborative, and long-term approach, that can anticipate, and respond to, change over time. This assessment allows us to understand whether the regime is functioning as intended and whether there is a risk of regulatory failure. We used an assessment tool developed by the Ministry of Business and Innovation (MBIE) (the tool), which provides a framework for agencies to self-review their regulatory practices and performance.

244. We wanted to generate an initial current state view of the performance of the AML/CFT regime across various components to provide greater context to the review and indicate any areas that may be underperforming. We were limited by time as to how thoroughly we could assess the regulatory performance of the regime (see Limitations of the approach), but the findings nonetheless indicate areas of further work to improve the performance of the regime.

245. The responses to the questionnaire are themed around nine aspects of regulatory stewardship practice and performance, which each fall under one of the following three umbrella areas: leadership and culture practices, design and delivery practices, and systems performance. We developed a system for scoring each response so that we could compare each area and sub-area against a four-point maturity scale (*see* Assessing the maturity of the AML/CFT regulatory system).

2.2.1. Summary of results

Performance area	Informal	Defined and evolving	Structured and proactive	Optimised
Governance, leadership, and strategy			✓	
Culture		✓		
Resourcing		✓		
Insights and foresights			✓	
Regulatory review and design		✓		
Delivery and decision-making			✓	
Effectiveness		✓		
Efficiency		✓		
Durability		✓		

246. Overall, the average scores suggest that the maturity of the regime can generally be considered defined and evolving, which indicates that there is recognition of the need for shared outcomes and more consistent ways of working with work underway to support more coordinated approaches across the system. However, given that the regime has been in place for 12 years we consider that average scores should be in the ranges of structured and proactive and optimised, and the overall results suggests that the regime is not as mature as it should be. We consider there has been sufficient time for, at minimum, formal systems and practices to be put in place and used consistently, adaptive practices encouraged, impact of change understood and for the system to be appropriately responsive (which are indicators of a structured and proactive regime).

247. Of the 57 statements about the regime that we asked respondents, only one was considered optimised, while seven were considered informal, 30 were considered defined and evolving, and 19 were structured and proactive. The average score across all questions was 0.7 (out of a range of -3 to +3), which indicates that there is significant room for improvement. The lowest performing area was the regime's efficiency, which was considered informal overall with a score of 0.1. Resourcing also performed poorly with an overall score 0.29 (third weakest overall) and was reflected in respondent comments as underlying areas of weaknesses throughout other parts of the maturity assessment, particularly those that were found to be informal. The one area of strength was the regime's governance, leadership, and strategy, which was considered to be structured and proactive overall.

248. We note that several of the recommendations we make in Part B seek to address the issues and areas of weakness in the regime. In particular, we recommend increasing the amount of funding available for government agencies including through exploring the development of a hybrid funding model (Recommendation R29); providing additional powers to the NCC to ensure that risk assessments are produced with appropriate frequency (Recommendation R9); enhancing the role of the private sector in the regime (Recommendation R27); and providing for improved information sharing between agencies (Recommendation R46) and with the private sector (Recommendation R10). Finally, the findings of this assessment would provide a useful foundation to explore and assess the relative merits or drawbacks of any alternative institutional structures (Recommendation R30).

2.2.2. Leadership and culture practices

Governance, leadership, and strategy

Statement	Rating	Score (-3 to +3)
1. The leadership and governance arrangements of the regime are well defined and reviewed periodically	Structured and proactive	1.04 ± 0.24
2. The AML/CFT roles and functions within your agency are clearly articulated and understood	Structured and proactive	1.43 ± 0.23
3. The regime's objectives and outcomes are well defined	Structured and proactive	1.26 ± 0.24
4. The regime's performance is monitored and evaluated effectively	Defined and evolving	0.37 ± 0.35
5. You are motivated, engaged and invested in the AML/CFT regime's purpose and outcomes	Structured and proactive	1.91 ± 0.21
6. Your colleagues are motivated, engaged and invested in the AML/CFT regime's purpose and outcomes	Structured and proactive	1.43 ± 0.27
7. You have a good understanding of what you are trying to achieve and what you are contributing to the AML/CFT regime	Structured and proactive	1.83 ± 0.23
8. The AML/CFT Strategy is relevant to my work	Optimised	2.07 ± 0.19
Overall	**Structured and proactive**	**1.42 ± 0.24**

249. Overall, the governance, leadership, and strategy section was the strongest performing area with an overall rating of structured and proactive, indicating that formal systems and practices are in place and used consistently, adaptive practice is encouraged, the impact of change is understood, and the system can respond in good time. It was also the only area which received an optimised rating for any of the underly statements. This indicates that this area of the regime is largely formalised but that it may not yet be able to anticipate and adapt to changing circumstances.

250. The relevance of the AML/CFT Strategy to participant's work was the strongest performing aspect of this section (statement one), receiving a score of 2.1, indicating an optimised part of the system. The weakest element was the monitoring and evaluation of the regime's performance (statement 4) which was given an overall score of 0.4, consistent with a defined and evolving practice. Other aspects of this section, including the articulation of the roles and functions within agencies (statement 2), clarity around the regime's objectives and outcomes (statement 3), and motivation and engagement with the regime's purpose (statements 5 and 6) received scores consistent with structured and proactive practices and performances.

251. Respondent's comments on this section indicate that there should be more focus on understanding the effectiveness and efficiency of the regime (*see* System performance), with one respondent commenting that to achieve this we need more resources for monitoring (*see* Resourcing). Several respondents also commented that they wanted to see better alignment between the different agencies involved in the regime and more understanding of each other's roles. For example, one respondent felt there was a disconnect between regulators and enforcement officers. On the other hand, another respondent commented that the collaborative approach of the AML/CFT working group for the statutory review has been efficient for producing results and utilising the subject matter expertise of various agencies.

Culture

Statement	Rating	Score (-3 to +3)
1. AML/CFT agencies work effectively together to facilitate alignment and coordination across the regime	Defined and evolving	0.91 ± 0.29
2. You are encouraged and enabled to have good connections with your counterparts in other agencies	Structured and proactive	1.2 ± 0.28
3. You are encouraged and enabled to have good connections with the private sector/reporting entities	Structured and proactive	1.5 ± 0.23
4. Māori-Crown partnership obligations are embedded in your work	Defined and evolving	0.02 ± 0.31
5. There are plenty of opportunities to consider different approaches, share lessons learned and speak up about risks	Defined and evolving	0.52 ± 0.3
6. There are good processes in place to work through and overcome challenges in the regime	Defined and evolving	0.41 ± 0.31
7. Learning and evaluation is embedded in the practices of the regime	Defined and evolving	0.35 ± 0.3
8. When issues or concerns are raised, they are taken seriously by agencies	Defined and evolving	0.93 ± 0.29
Overall	**Defined and evolving**	**0.73 ± 0.29**

252. The culture section did not perform as well as the governance, leadership, and strategy section, with an overall score of defined and evolving. This indicates that the culture of the regime is not yet formalised but that there is work underway to support more coordinated approaches across the system, including trying to find more consistent ways of working and building shared objectives and outcomes.

253. Respondents indicated that the facilitation and encouragement of employees to build good connections with counterparts in other agencies (statement 2) and with the private sector (statement 3) were the strongest performing aspects of the regime's culture, receiving scores of 1.2 and 1.5 respectively in line with a structured and proactive practice. However, the embedding of Māori-Crown partnership obligations (statement 4) and learning and evaluation in employee's work (statement 7) stood out as being low performing, with scores of 0.0 and 0.3, just meeting a rating of defined and evolving but bordering on being informal. We note that the finding regarding Māori-Crown relationships appears to be in line with our findings regarding the consistency of the Act with Te Tiriti o Waitangi (*see* Consistency with Te Tiriti o Waitangi). Other low scoring areas concerned agencies having processes in place to overcome challenges in the regime (statement 6) and having opportunities to consider different approaches, share lessons, and speak about risks (statement 5).

254. Respondents commented on different aspects of the regime's culture. One respondent considered that agencies openly discuss feedback and new ideas but that there is little transparency around what is being done about issues. Another respondent commented that lack of resources can prevent issues from being dealt with properly. Further, respondents commented that there is too much emphasis on administrative work, for example using templates that are incoherent, rather than actual compliance and regulatory work. Another respondent also commented that relationships between the regulators and the Police appear to be primarily based on personal relationships and that there needs to be a coordination body straddling the AML/CFT agencies to ensure a collective approach is taken to risk, and to improve

information sharing. The suggestion that there needs to be a coordination body suggests that the existing coordination structures (e.g., NCC) may not be adequately fulfilling their role or visible to all in the regime.

Resourcing

Statement	Rating	Score (-3 to +3)
1. Overall, the AML/CFT regime is appropriately resourced	Informal	-0.7 ± 0.32
2. There are enough resources available to carry out your role to a high standard	Informal	-0.41 ± 0.32
3. Resources are prioritised to areas of highest risk across the regime	Defined and evolving	0.59 ± 0.28
4. Resources within my agency are prioritised to areas of highest risk	Structured and proactive	1.24 ± 0.2
5. Agencies ensure the regime has the skills and diversity to achieve its purpose	Defined and evolving	0.22 ± 0.3
6. People capability is planned for and developed in my agency	Defined and evolving	0.28 ± 0.33
7. The people working in the regime have the capabilities to carry out the regime's functions	Defined and evolving	0.8 ± 0.27
Overall	**Defined and evolving**	**0.29 ± 0.29**

255. Resourcing was one of lowest performing section of the regime, receiving an overall rating of defined and evolving but with several aspects considered informal. This indicates that some practices and performances around resourcing are inconsistent and struggle to adapt to change, but that overall work is underway to support a more coordinated approach to resourcing across the system.

256. The weakest area was the overall resourcing of the regime, which respondents indicated was not appropriately resourced (statement 1), and that this prevented them from carrying out their roles to a high standard (statement 2). Both these aspects of resourcing received a negative score in line with an informal system and highlight areas that need urgent attention. Other weak areas include agencies abilities to ensure the regime has the skills and diversity to achieve its purpose (statement 5) and planning and developing people capability within their agency (statement 6). The highest performing area was the prioritisation of resources by agencies towards areas of highest risk (statement 4) with a score of 1.2 indicating that this practice is structured and proactive. However, risk-based allocation of resources is a core aspect of any AML/CFT regime, and this result is arguably weaker than it should be. We also note that regime-wide resource allocation performed worse than intra-agency allocation.

257. A key issue reflected in the comments was the need for more dedicated resourcing across the regime, noting that supervision populations are growing, and that agencies are having to make trade-offs, and focus on urgent and high-risk areas. Respondents also commented that lack of resourcing is creating high staff turnover as the pressure on stuff is unsustainable which creates issues around continuity. Further, respondents noted that new recruits lack the right level of expertise, particularly in manager roles, and that the regime needs to recruit specialist knowledge rather than generalists. It was also raised that there needs to be better development once people are in the job. Finally, one respondent commented on the need to better utilise technology as each agency uses its own systems which creates inefficiencies and limits outcomes.

2.2.3. Design and delivery practices

Insights and foresights

Statement	Rating	Score (-3 to +3)
1. Effective and efficient data stewardship and information sharing practices are promoted and encouraged across the regime	Structured and proactive	1.02 ± 0.26
2. Agencies carry out horizon and environmental scanning activities to integrate insights on emerging needs, trends, issues and risks	Defined and evolving	0.85 ± 0.27
3. Agencies use insights to drive understanding of risks and regime effectiveness so they can adjust policies and processes where needed to ensure the delivery of optimal outcomes	Structured and proactive	1.02 ± 0.23
4. Insights from the FIU, such as the National Risk Assessment or other intelligence products, are useful and relevant to my work	Structured and proactive	1.8 ± 0.19
5. Insights from the supervisors, such as the Sector Risk Assessments, are useful and relevant to my work	Structured and proactive	1.93 ± 0.17
6. Work is carried out to understand the needs of reporting entities	Defined and evolving	0.52 ± 0.29
Overall	**Structured and proactive**	**1.19 ± 0.24**

258. The use of insights and foresights in the regime received an overall rating of structured and proactive. This suggests that formal systems and practices are in place to use information to inform system improvement but may not yet be able to anticipate and adapt to changing circumstances. However, the AML/CFT regime is designed to be driven by strategic insights about risks; as such, we would expect to see optimisation occurring regarding insights and foresights with adaptive systems, practices and ways of working are part of the regime's culture, with the system anticipating and responding to the challenge of changing circumstances.

259. The usefulness and relevance of insights from Sector Risk Assessments (statement 5) and intelligence products such as the National Risk Assessments (statement 4) were the strongest performing areas of this section, receiving scores of 1.9 and 1.8 in line with a structured and proactive performance. However, as we were not able to interrogate the responses further, we have not been able to ascertain whether this view would still be held if respondents were asked to consider that the NRA and several SRAs are out-of-date (see How well do we understand our risks). Carrying out work to identify the needs of reporting entities (statement 6) and identifying emerging issues and risks (statement 2) received lower scores of 0.5 and 0.6 in line with a defined and evolving practice.

260. Respondents' comments on this section indicated that the lack of resourcing is limiting agency's abilities to turn data and information into intelligence-driven approaches and plan for the future. One respondent also noted that intelligence functions should be based in Auckland rather than Wellington as this is where high-risk reporting entities and activities are located, and that we need to invest more in technology to ensure efficient data sharing across regulators and Police. Another key theme from respondents' comments was the need to focus more on engaging with reporting entities and assisting them with compliance. Again, respondents identified that resourcing is limiting their abilities to carry this out, which is further compounded by

the lengthy delays associated with the process for producing joint supervisory guidance. One respondent did note that the IAG has provided significant value to the review in terms of determining the scope of issues, which reinforces the value that private sector insights could provide.

Regulatory review and design

Statement	Rating	Score (-3 to +3)
1. High quality and evidence-based insights are frequently collected and used to inform improvements to the regime	Defined and evolving	0.46 ± 0.28
2. Where gaps or issues are identified in the regime, plans are developed to address them effectively and promptly	Defined and evolving	0.13 ± 0.3
3. The right tools and processes are in place to effectively deliver the regime	Defined and evolving	0.22 ± 0.31
4. There are no significant barriers within the regime to achieving the optimum outcomes	Informal	-0.5 ± 0.29
5. Planning for regulatory change considers the resources and time needed to implement the proposed changes by both agencies and reporting entities	Defined and evolving	0.65 ± 0.31
6. Evaluation is considered in early thinking about regulatory review and design	Defined and evolving	0.59 ± 0.31
7. When changes are considered, other agencies and reporting entities are effectively consulted	Structured and proactive	1.37 ± 0.25
8. Alignment with international regulatory approaches or cooperation with international counterparts and the FATF Standards are considered in the design of new regulations or changes to the regime	Structured and proactive	2 ± 0.13
Overall	**Defined and evolving**	**0.61 ± 0.27**

261. Overall, regulatory review and design came out with the lowest scores of the design and delivery category with an average rating of defined and evolving. This indicates that the regime's approach to regulatory review and design is not yet formalised but is in the process of trying to establish more consistent and coordinated systems.

262. Respondents' responses indicated that the regime is most successful at encouraging innovative and novel approaches to designing changes (statement 8), receiving a score of 2.0 and one of the few aspects of this area that was considered structured and proactive. However, the results indicate the presence of significant barriers within the regime that prevent optimal outcomes from being achieved (statement 4), in particular resourcing. Other low scoring areas were the effectiveness and promptness of the regime to address gaps or issues once they are identified (statement 2), and the presence of the right tools and processes to effectively deliver the regime (statement 3).

263. Respondents' comments indicated that time constraints are the biggest barrier to achieving effective regulatory review and design system. For example, they noted that time constraints mean that little time is given to continuously reviewing and improving our system, that the easiest option is often chosen rather than the one that has the potential to be most effective when making improvements, and that legislative and regulatory changes are rushed through without meaningful consultation. One respondent considered that time constraints have impacted the quality of the

statutory review. Respondents also suggested that technology could assist in carrying out regulatory review and design and that there should be a centralised pool of funding for investment in innovation across the AML/CFT agencies. Another commented that too much emphasis is placed on FATF Recommendations rather than what is best for the New Zealand environment.

Delivery and decision-making

Statement	Rating	Score (-3 to +3)
1. Agencies effectively support reporting entities to comply	Structured and proactive	1.33 ± 0.2
2. Guidance and support from supervisors is proportionate to the risks or harms being managed and informed by data and evidence	Defined and evolving	0.72 ± 0.27
3. There are opportunities for review of the regime's settings	Structured and proactive	1.22 ± 0.25
4. You know what decisions you can make and where you can go for guidance	Structured and proactive	1.61 ± 0.19
5. Consistent decisions are promoted through good processes	Defined and evolving	0.61 ± 0.3
6. Operational decisions are supported by knowledge of risk, regulated parties and changes in the regulatory environment	Structured and proactive	1.2 ± 0.23
Overall	**Structured and proactive**	**1.11 ± 0.24**

264. Overall, delivery and decision making received a rating of structured and proactive. This indicated that delivery and decision making is formalised in the regime but that it may not yet be able to anticipate and adapt to changing circumstances. The strongest aspect of this section was people in the regime knowing what decisions they can make and where they can go for guidance (statement 4). This received a score of 1.6 indicating this practice is structured and proactive. The weakest aspects were the promotion of consistent decisions through good practices (statement 5) and guidance and support from supervisors being delivered to reporting entities proportionate to the risks or harm being managed and informed by data and evidence (statement 6).

265. Respondents' comments on this section raised several different issues regarding decision-making, including that it is inconsistent, slow, and top-down, and that there is a lack of consultation, transparency, and consistent procedures in place. One respondent noted that some of these issues mean there is a reliance on key members of agencies for decision-making. Another respondent considered that there is strong framework in place to ensure consistent decision-making on compliance matters. Other comments raised the need for more guidance for reporting entities, more resources to effectively regulate non-compliant entities, better quality SARs, and more focus from supervisors on detection through intelligence and law-enforcement, rather than compliance.

2.2.4. System performance

Effectiveness

Statement	Rating	Score (-3 to +3)
1. The regime is effective in achieving its intended outcomes – the detection and deterrence of ML/FT	Defined and evolving	0.5 ± 0.28
2. There is a strong level of public confidence in the regime	Defined and evolving	0.07 ± 0.29
3. The regime is proportionate, fair and equitable in the way it treats regulated parties	Defined and evolving	0.93 ± 0.3
4. The regime is transparent and provides clear guidance to reporting entities	Defined and evolving	0.41 ± 0.31
5. The regime supports people from marginalised communities	Defined and evolving	0.15 ± 0.31
6. The regime encourages and supports stakeholder feedback and participation in regime improvement and regulatory review	Defined and evolving	0.98 ± 0.28
Overall	**Defined and evolving**	**0.51 ± 0.29**

266. Overall, the effectiveness of the regime's system performance was rated as defined and evolving. This indicated the effectiveness of the regime's performance is not yet formalised in the regime but that it is heading towards establishing more consistent and coordinated ways of achieving effectiveness, fairness, and accountability.

267. No aspect of this section received a particularly strong score. Statements 6 and 3 received scores of scores of 1.0 and 0.9 respectively, indicating that respondents slightly agreed that the regime encourages and supports stakeholder feedback and participation in improvements and regulatory review (statement 6), and that the regime is proportionate, fair and equitable in the way it treats reporting entities (statement 3). The weakest aspects concerned the level of public confidence in the regime (statement 2) with a score of 0.5, and the regime supporting marginalised communities (statement 5) with a score of 0.2. However, we were not able to interrogate responses further to understand why respondents considered there to be low levels of public confidence in the regime.

268. Respondents commented that the effectiveness of the regime is not well measured making it hard for agencies to know whether it is achieving its intended purpose. One respondent raised that our inability to demonstrate effectiveness undermines the public's trust in the regime. Another respondent considered the difference in maturity across industries that have been complying with the Act for less time is a factor in the regime having mixed effectiveness. Several respondents also raised the systems for providing feedback, with one respondent considering that use of feedback has improved in recent times while another did not think the regime made the most of feedback received. Other comments considered that the regime needs to consider its approach towards cultural diversity, allow the time and resourcing for monitoring and producing guidance, and clearly articulate the Act's obligations so that there are no ambiguities preventing obvious breaches from being enforced.

Efficiency

Statement	Rating	Score (-3 to +3)
1. There is a good understanding of the costs (direct and indirect, regime-wide) of regulation, where costs are incurred and how they are affected by changes in activity	Informal	-0.09 ± 0.3
2. Process and delivery practices support regime efficiencies. It is easy for reporting entities to comply with the regime	Informal	-0.13 ± 0.27
3. It is easy for agencies to administer the regime	Defined and evolving	0.13 ± 0.28
4. Regime governance ensure efficiencies are balanced against effectiveness considerations	Defined and evolving	0.48 ± 0.27
Overall	**Defined and evolving**	**0.10 ± 0.28**

269. Overall, the efficiency of the regime received a marginal defined and evolving rating but with areas of informality. This indicates that practices to minimise costs and burdens and maximise benefits are largely inconsistent and not well understood. The weakest areas, both receiving scores of -0.1, indicating general disagreement that there is a good understanding of the costs of regulations (statement 1) and that process and delivery practices support regime efficiencies (statement 2). Performing slightly stronger at 0.4 was the regime's governance ensuring that efficiencies and effectiveness considerations are appropriately balanced (statement 4).

270. Respondents' comments indicated that they consider there is too much emphasis placed on compliance without having enough regard for mitigating actual risks. One respondent also considered that the emphasis on FATF Recommendations leads to unnecessary measures that increase compliance costs, particularly around the customer due diligence settings. Another respondent commented that the use of unregulated auditors decreases the efficiency of the regime due to poorly undertaken audits while one noted that inefficiencies are unavoidable in any regulatory regime and the key is finding a balance with compliance. They considered there is space for large reporting entities to invest more in compliance and that costs could be scaled to businesses.

Durability

Statement	Rating	Score (-3 to +3)
1. The regime copes with changing circumstances and pressures	Defined and evolving	0.48 ± 0.3
2. The agencies engaged in the regime have the resources and capabilities to deliver now and, in the future,	Informal	-0.2 ± 0.33
3. Insights are being used to generate foresight and anticipate changing needs, particularly in regard to the digital economy	Defined and evolving	0.17 ± 0.28
4. The regime is agile in responding to unforeseen challenges and demands	Informal	-0.02 ± 0.31
Overall	**Defined and evolving**	**0.11 ± 0.3**

271. The durability of the regime also performed poorly, receiving a marginal defined and evolving rating overall but with informal elements. This indicates that the regime's ability to cope with changing circumstances and pressures is working towards being more coordinated but is still inconsistent in some areas and not well understood.

272. The weakest aspects of this section, receiving scores of -0.2 and -0.02 were with respect to agencies having the resources and capabilities to deliver now and, in the future, (statement 2), and the agility of the regime to respond to unforeseen challenges and demands (statement 4). Performing marginally better with scores of 0.2 and 0.5 is the regime's ability to cope with changing circumstances and pressures (statement 1) and the use of insights to generate foresights and anticipate changing needs, particularly around the digital economy (statement 4).

273. Several respondents commented that the regime is slow to react to changes, with one respondent noting this creates unfavourable conditions for the private sector. Respondents commented that durability would be improved through more experienced staff, better resourcing, practical training, and business continuity plans. Another respondent raised there is very little focus on both what is happening now and, in the future, and that the regime is are behind advantages in the digital space. One respondent also commented that Police and regulators cannot keep up with the criminal environment, particularly the use of technology, and that regulatory and legislative pathways are slow to keep up. They further commented that outcomes need to be supported through well-defined and flexible approaches and clear goals.

2.3. Consistency with Te Tiriti o Waitangi

274. We have assessed the extent to which the operation and development of the AML/CFT regime is consistent with the principles of Te Tiriti o Waitangi, as expressed by the courts and the Waitangi tribunal. Specifically, we have assessed the extent to which the Act's operation has been in consistent with the principles of partnership, active protection, and redress.[13] Overall, we consider the Crown needs to do more to satisfy its duty to be sufficiently informed and recommend that agencies work to develop relationships with relevant Treaty partners to identify and understand the extent of Māori interest in the operation of the AML/CFT regime.

2.3.1. Principle of partnership

275. The principle of partnership is well established in Treaty jurisprudence. The Waitangi Tribunal conceptualises the duty to act reasonably, honourably, and in good faith as being derived from the principles of reciprocity and mutual benefit, as well as ensuring that decision makers are sufficiently informed before making a decision.

276. The Tribunal identifies the principle of reciprocity in Articles I and II of the Treaty, in that these articles capture the 'essential bargain' agreed to by Māori and the Crown: the exchange of kāwangatanga for the guarantee of tino rangatiratanga. Similarly, the Tribunal has found the principle of mutual benefit as a cornerstone of the Treaty partnership, requiring that the needs of both cultures must be provided for and compromise may be needed in some cases to achieve this objective.

277. We consider that the regime provides significant benefits to both the Crown and Māori. Money laundering is the lifeblood of organised crime, and by detecting and deterring this activity the regime seeks to make it harder for organised criminals to conduct their business in New Zealand.[14] Similarly, New Zealand is not immune from devastating terrorist attacks: by making it harder for terrorism to be facilitated through the raising, movement, or use of funds, the regime helps prevent future

[13] Waitangi Tribunal, He Tirohanga ō Kawa Te Tiriti o Waitangi – A Guide to the Principles of the Treaty of Waitangi as Expressed by the Courts and the Waitangi Tribunal.

[14] This objective has been further enshrined in the Government's Transnational Organised Crime strategy, which has as its vision New Zealand becoming the hardest place in the world for organised criminal groups and networks to do business:

attacks from occurring. Furthermore, having an adequate regime (by the FATF's standards) avoids a significant dis-benefit which would result from New Zealand being greylisted (*see* Cost of the regime).

278. However, we recognise that the Crown must exercise its kāwangatanga responsibilities reasonably and in the utmost good faith.[15] One requirement of good governance is that the Crown takes reasonable steps to be properly informed of the effect of AML/CFT laws on Māori, and of any broader Māori/Treaty interest.[16] The level of Māori interest is relevant to determining the steps the Crown must take in this regard.

279. Overall, there has been limited engagement with Māori throughout the operation and development of the regime. We could not identify any submissions from Māori or Māori organisations on either the *AML/CFT Bill* in 2009[17] or the *AML/CFT Amendment Bill* in 2017.[18] Further, the departmental reports produced by the Ministry for each Bill did not identify any Māori interests that should be considered. This suggests that the Crown did not take sufficient steps to engage with Māori about the Act and its operation to identify and understand whether there are any Māori interests that should be considered as part of policy reforms.

280. This historical lack of engagement also impacted the ability of this review to identify and consider Māori interests, particularly as there have been no relationships established with iwi, hapū or Māori organisations within the regime. Due to the limited time available to conduct the review (*see* Limitations of the approach), we were unable to take the time to engage with Māori properly and in a manner fully consistent with the guidelines published by Te Arawhiti. We instead relied on general consultation approaches (i.e., publishing the Discussion Document and factsheet about the review in Te Reo Māori) and conducting direct outreach with a small number of Māori organisations. However, these efforts were unsuccessful as we received no submissions from Māori organisations.

281. Nevertheless, we have conducted our own analysis and have identified that Māori may have potentially significant interests in the following areas that are impacted by the Act:

Potential interest	Likely nature of the interest	Recommended reforms to protect interest
The extent to which the Act leads to Māori overrepresentation in the criminal justice system	We do not have any data about the extent to which the AML/CFT regime's operation differs depending on the ethnicity of the people involved (e.g., the customer, the subject of an intelligence report). This is due to the fact that there is no requirement on businesses to identify a person's ethnicity as part of customer due diligence, nor is there a corresponding requirement to indicate a person's ethnicity when submitting a suspicious activity report (SAR). As such, we cannot determine whether disproportionately more SARs are filed in respect of Māori as compared with other ethnicities, nor whether disproportionately more intelligence products are generated in respect of Māori. That being said, we anticipate that there would be some level of disproportionate treatment given the overrepresentation of Māori in the broader criminal justice system. A consistent message from Māori	We recommend reviewing the legislative requirements for submitting SARs, PTRs, and producing further guidance. This could provide an opportunity to consider whether there are disproportionately more SARs filed in respect of Māori compared to other ethnic groups (*see* Suspicious activity reports). Collecting this data would allow agencies to determine whether there is any overrepresentation or bias, and then work with businesses to address any bias in the system.

[15] *Te Runanga o Wharekauri Rekohu Inc v Attorney-General* [1993] 2 NZLR 301 (CA) (Lands) at 664

[16] See *Te Runanga o Wharekauri Rekohu Inc v Attorney-General* at 683

[17] Ministry of Justice (2009) Anti-Money Laundering and Countering Financing of Terrorism Bill – Report of the Ministry of Justice.

[18] Ministry of Justice (2017) Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill – Departmental Report for the Law and Order Committee

Potential interest	Likely nature of the interest	Recommended reforms to protect interest
	when engaging with Te Uepū Hāpai I to Ora – Safe and Effective Justice Advisory Group was that racism is embedded in every part of the criminal justice system. As of 2019, Māori comprised 16 percent of the general population, but made-up 38 percent of people proceeded against by Police, 42 percent of adults convicted, 57 percent of adults sentenced to prison.[19]	
The extent to which the Act supports or inhibits the ability of Māori to engage with the formal financial system and their access to legitimate capital	As we noted in the Discussion Document, some of the requirements of the Act make it harder for some people to engage with the formal financial system. This has been identified internationally by the FATF, which noted that "disadvantaged and other vulnerable groups […] are more likely to be excluded from the formal financial sector."[20] The FATF further notes that strict documentary requirements may exclude segments of society who have formal proof of their identity or address. As we note in Part B, the Act goes beyond the requirements of the FATF to require address information to be verified. We consider that the Act is likely to inhibit the financial inclusion of Māori to the extent that they are represented in vulnerable groups that tend to lack necessary documentation. We also note that Māori access to capital was identified as a primary concern by RBNZ in their Te Ōhanga Māori – Māori Economy Report 2018,[21] which may be driven by AML/CFT identity and verification requirements.	We recommend repealing and replacing the Identity Verification Code of Practice with a new code of practice that aligns with the incoming Digital Identity Services Trust Framework (*see* Identity Verification Code of Practice), relaxing the requirements to verify address information (*see* Verifying address information), and exploring whether any further regulatory exemptions are required to address financial inclusion challenges (*see* Financial exclusion). These changes should help improve financial inclusion for all New Zealanders, including Māori.
The extent to which the Act supports or undermines that ability of post-settlement governance bodies or Māori trusts to operate effectively and efficiently	A large amount of land is held in Māori trusts established under *Te Ture Whenua Māori Act 1993*, such as Whānau trusts, Ahu Whenua trusts, or Māori incorporations. In addition, many governance structures established following a Treaty settlement operate as a trust. The Act requires higher levels of scrutiny for customers that are trusts, such as verifying the source of wealth of the trust and the identity of the beneficiaries. For Māori trusts this requirement is likely to present a significant barrier that is unlikely to be justified by the money laundering and terrorism financing risks associated with these structures. In turn, the requirements for enhanced scrutiny are likely making it hard for these arrangements and structures to access or operate in the financial system, receive non-financial services, and deal with or dispose of interests in land.	We recommend relaxing the mandatory requirements to conduct enhanced scrutiny of customers that are trusts, including Māori trusts (*see* Mandatory enhanced CDD for all trusts), providing further clarity about the definition of a beneficial owner (*see* Definition of beneficial owner), and providing for alternative sources of information to verify some information about legal persons and legal arrangements (*see* Unavailability of independent verification sources). These changes should make it easier for trusts, including trusts established under *Te Ture Whenua Māori Act 1993,* to open and operate bank accounts and access the formal financial system.

[19] Te Uepū Hāpai I te Ora — Safe and Effective Justice Advisory Group He Waka Roimata; Transforming Our Criminal Justice System (June 2019, at 23).

[20] Financial Action Task Force (2017) *Anti-money laundering and terrorist financing measures and financial inclusion,* page 39

[21] BERL (2020) Te Ōhanga Māori 2018 – the Māori Economy 2018.

Potential interest	Likely nature of the interest	Recommended reforms to protect interest
The extent to which the Act supports or undermines Māori data sovereignty, particularly where data is sent offshore	The Act requires businesses to collect and store large amounts of information about the public, and in some instances, share the information with Government agencies or other businesses offshore. The Waitangi Tribunal has noted that Māori data may be a component of mātauranga Māori (Māori knowledge) or may, in combination with related data be (or have the potential to be) taonga.[22] As such, Māori are likely to have an interest to the extent that requirements for data collection and sharing impact on Māori data sovereignty. This interest is likely to be particularly acute with respect to businesses that, by virtue of their operation, share information with related businesses in other countries (e.g., subsidiaries sharing with offshore parent companies).	We recommend amending the Act to require groups of businesses to develop group-wide compliance programmes to ensure sharing of customer information to offshore businesses is consistent with the *Privacy Act 2020* (see Group-wide programme requirements). The process for developing and implementing this change could provide an opportunity to consider Māori data sovereignty interests.

282. To ensure the Crown is fulfilling its duty to be sufficiently informed, we consider that more efforts should be made to directly engage with Māori parties and interests as part of future AML/CFT reform work. In particular, agencies should look to develop relationships with relevant Māori stakeholders and continue to be involved with ongoing work regarding Māori access to capital or financial inclusion to resolve any issues caused by the Act or its operation. We also note that upcoming Waitangi Tribunal inquiries may identify areas where the Act is disproportionately impacting Māori, specifically the inquiry into the justice system and the inquiry into economic development.[23] These inquiries could provide a useful avenue for the Crown to be sufficiently informed as to Māori interests in the operation of the Act.

2.3.2. Principle of active protection

283. The Crown's duty of active protection is a central Treaty principle, which was first raised by the Waitangi Tribunal in its early reports, and affirmed by the Court of Appeal in 1987, in the *Lands* case. The principle encompasses the Crown's obligation to take positive steps to ensure that Māori interests are protected. The Courts have considered the principle primarily in association with the property interests guaranteed to Māori in Article II of the Treaty. The Waitangi Tribunal has also emphasised the Crown's stated aims in the preamble of the Treaty and in Article III.

284. As with the duty to be sufficiently informed, the Courts and the Waitangi Tribunal have both found that the extent of the duty depends on the nature and value of resources in question. As per the above discussion, we have identified areas where there may be Māori interests in the operation of the Act, but the nature of that interest (and whether they would be considered taonga) is unclear due to the historical lack of engagement with Māori. Nevertheless, we note:

- the Waitangi Tribunalin *Tū Mai Te Rangi!* noted that disproportionate reoffending and reimprisonment rates had serious impacts on thousands of Māori men, women and children and their communities, and that te ira tangata, the essence of life, is the ultimate taonga.[24] The extent to which the Act is contributing to disproportionate reoffending and reimprisonment rates is unclear, but likely to be limited as there are likely more significant drivers of this issue when compared with the Act.

[22] Waitangi Tribunal (2021) *The Report on the Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (*WAI 2522*)

[23] Waitangi Tribunal (2021) *Appendix B. The Kaupapa inquiry programme*

[24] Waitangi Tribunal (2017) *Tū Mai Te Rangi! Report on the Crown and Disproportionate Reoffending Rates*

- the *Te Mana o te Raraunga Framework* provides for when a data set may be considered taonga depending on the provenance, opportunity, and utility of the data. It is unclear whether the data held by the FIU would be considered taonga. However, we note that the data will not have come directly from a Māori source (but from businesses with Māori customers or Māori owned businesses), may not be able to support Māori aspirations for their people or their whenua and is limited in use to detecting illicit activity and producing financial intelligence products.[25]

285. However, despite the above uncertainty, we are recommending several changes to the Act and overall regime that should reduce the potential for Māori being disproportionately negatively impacted per the above table.

2.3.3. Principle of redress

286. The Court of Appeal has acknowledged that it is a principle of partnership generally, and of the Treaty relationship in particular, that past wrongs give rise to a right of redress. This acknowledgment is in keeping with the fiduciary obligations inherent in the Treaty partnership. In other words, where breaches of the Treaty had occurred, a fair and reasonable recognition of and recompense for the wrongdoing was required.

287. Despite identified shortcomings, the Act has not been found to breach the Treaty by either the courts or the Waitangi Tribunal. We further note that changes we recommend should significantly reduce the chance of a Treaty breach resulting from the Act. Accordingly, we consider that the Act has been consistent with the principle of redress.

[25] Māui Hudson et al (2017) "He Matapihi kit e Mana Raraunga" – Conceptualising Big Data through a Māori lens. In Whaanga, Keegan & Apperly (Eds.) "He Whare Hangaru Māori – Language, culture & technology" (pp. 64-73.

Part B: Whether any amendments are necessary or desirable

CHAPTER 3

Institutional arrangements and stewardship

Summary

288. This chapter makes a number of recommendations for changes to the fundamental components of the overall regime, such as the purposes of the Act, the approach the regime should take to regulation, and how the various agencies are structured and operate.

289. We recommend a number of changes to the purpose of the Act. One major change we recommend is that the Act should have the purpose of supporting businesses in their implementation of sanctions obligations under the *Terrorism Suppression Act 2002*, *United Nations Act 1946*, and *Russia Sanctions Act 2022*. We also recommend some smaller tweaks to the purpose of the Act, namely ensuring it refers to the Act taking a risk-based approach, accurately reflects its broader societal outcomes, and also combats proliferation financing. We do not, at this stage, recommend that the Act's purpose be changed to include prevention of money laundering and terrorism financing, but nonetheless recommend that further prevention-focused obligations be explored and strengthened where appropriate.

290. We recognise that the Act and its implementation has not been sufficiently risk-based for a number of reasons, which has the net impact of not being as effective as it could be as well as more expensive for businesses. We recommend strengthening the framework for understanding and sharing risk information through creating a specific power for the National Coordination Committee (NCC) to request the production of a risk assessment, as well as further progressing the development of a framework for sharing dynamic and/or live risk information. We also recommend that further and more detailed guidance is provided to businesses to ensure they empowered to comply with their various risk-based obligations, and that further regulatory exemptions for low-risk products, businesses, and transactions are issued. Finally, we also recommend that more is done to make it easy for smaller and/or lower capacity business to comply with their obligations, such as through creating a centralised source of AML/CFT information or developing additional tools or resources for businesses.

291. In terms of the agency arrangements or structure, we broadly recommend that further analysis is conducted to determine whether an alternative approach to the structure of the regime is viable and addresses issues we have identified with the current structure. This could include creating a new agency to deliver policy, administration, and financial intelligence function, creating a single supervisory agency (instead of the current multi-supervisory model), or creating a combined supervisor and Financial Intelligence Unit (FIU). This further work should also include conducting a full analysis of the costs and benefits of any change, given that changing the agency structure would be disruptive to the regime. Irrespective of the agency structure, we recommend amending the Act to the FIU has the necessary independence to deliver AML/CFT services, formalising existing private sector advisory group models, and exploring a hybrid public/private funding model to ensure the regime is sufficiently resourced.

292. Finally, we recommend a series of changes to the powers or functions of agencies as well as improving information sharing within the regime. In particular, we recommend empowering the AML/CFT supervisors to supervise the implementation of targeted financial sanctions, to appropriately inspect businesses that operate from private

residences, and to inspect businesses remotely. Subject to developing appropriate privacy protections and safeguards, we also recommend providing powers to the FIU to request information from businesses that are not reporting entities, conduct ongoing monitoring of transactions and accounts in high-risk situations, and can freeze accounts and/or block certain transactions to prevent harm.

3.1. Purpose of the Act

3.1.1. Actively preventing money laundering and terrorism financing

293. The Act currently focuses on detecting and deterring money laundering and terrorism financing. However, this approach assumes that some illicit transactions occur, which are subsequently detected and responded to by law enforcement agencies. As such, we considered whether the regime could do more to actively stop or prevent illicit funds from entering and flowing through New Zealand's economy.

294. We have identified several options for how the Act could take more of a prevention focus, which are not mutually exclusive:

- **amend the purpose of the Act:** this option would involve amending the purpose statement in section 3 to include "prevention" or "disruption" in addition to detection and deterrence of money laundering and terrorism financing. This would then influence how the Act is interpreted by agencies, businesses, and the judiciary.
- **strengthen existing prohibitions:** the Act already includes various prevention-focused requirements in section 37, which prohibit transactions and business relationships where customer due diligence (CDD) is not conducted to the level required by the Act. These prohibitions could be further strengthened to prevent suspicious transactions by, for example, prohibiting transactions from occurring where a SAR has been filed.
- **introduce new prevention focused obligations:** this approach could include prohibiting or requiring enhanced CDD for particularly risky transactions, such as cash transactions over a certain threshold or cash deposits into third party accounts. These requirements would then serve as a disincentive for businesses and discourage them from allowing the transactions to occur due to the additional compliance costs.
- **create new agency powers to support prevention**, such as increasing information sharing frameworks or strengthening parts of the broader AML/CFT system such as asset recovery.

295. Most submitters were not supportive of the Act requiring businesses to prevent money laundering or terrorism financing. There was particular opposition to the option of amending the Act's purpose to include prevention, with submitters noting this could result in businesses being effectively required to act in the role of the Police, would be costly and difficult to implement, be contrary to a risk-based approach, increase risks associated with tipping off, and potentially offend principles of natural justice. However, a small number of submitters thought this change could enable a more efficient and proactive approach to combatting financial crime and that would align with consumer expectations. This feedback was reiterated during private sector engagement in April 2022 where attendees were generally opposed to the purpose being amended but were open to agencies exploring prevention-focused obligations.

296. We broadly agree with the concerns raised by the private sector regarding an amendment to the purpose of the Act. Therefore, we do not recommend this change at this stage. Instead, we recommend further strengthening the existing prevention-focused obligations to ensure that, where appropriate, suspicious or risky transactions are stopped. We consider this approach most aligned with the existing framework in the Act. It will help combat illicit financial flows while reducing the risk of significant compliance costs being imposed on businesses. Given the concerns of submitters, we

will need to carefully develop any changes or additional obligations to ensure they are workable and mitigate tipping-off risks.

297. We further recommend implementing further prevention-focused obligations following an assessment of the costs and benefits, such as requiring enhanced due diligence for particularly risky transactions (e.g., cash transactions over a certain threshold or cash deposits into third party accounts). We consider that there would be value in requiring enhanced CDD on specific risky transactions, which would require businesses to understand and verify the source of the money before the transaction could proceed and thereby prevent illicit money from entering into the system. This approach could also encourage businesses to cease accepting particularly large cash transactions in order to avoid compliance obligations. However, we recognise that any additional obligations require careful development and consideration and further assessment of the precise benefits this change would provide

Recommendations

R1. Existing prevention-focused obligations in the Act should be further strengthened to ensure that, where it is appropriate, suspicious or risky transactions are stopped to reduce the ability for illicit money to enter or flow through the financial system.

R2. Introduce, subject to a cost-benefit assessment, additional prevention-focused obligations, such as requiring enhanced customer due for certain types of high-risk transactions, such as cash transactions over a certain threshold or cash deposits into third party accounts.

R3. If it is necessary to implement any additional obligations or powers identified, consider changing the purpose of the Act to include prevention of money laundering and terrorism financing.

3.1.2. Supporting the implementation of financial sanctions obligations

298. All people in New Zealand have obligations to implement sanctions to combat terrorism (through the *Terrorism Suppression Act 2002*), sanctions imposed by the United Nations Security Council (through the *United Nations Act 1946*), as well as sanctions against certain Russian individuals and entities (through the *Russia Sanctions Act 2022*). Broadly speaking, the various sanctions place requirements to freeze the assets of designated persons and entities and prohibit people and businesses from providing further funds or services to a person or entity following their designation.[26] They may also place restrictions on the export of goods and provision of services to sanctioned entities outside New Zealand. There are several offences for failing to implement sanctions which can be punishable by between 12 months and seven years imprisonment.

299. Further, the FATF further expects that countries ensure businesses are appropriately implementing targeted financial sanctions to combat terrorism financing and financing the proliferation of weapons of mass destruction. These requirements are outlined in Recommendations 6 and 7 of the FATF Standards and include requirements for promptly communicating listings and de-listings and providing clear guidance to businesses on their sanctions obligations. The FATF found that New Zealand only partly complies with these obligations, which in turn undermines how effectively we are implementing these types of targeted financial sanctions.

300. We note that there is significant overlap between the existing AML/CFT framework and a regulatory framework to support the implementation of sanctions. However, we also note that there are different approaches taken to AML/CFT versus sanctions – the former should be risk-based (*see* Risk-based approach to regulation), while the latter is rules-based and focused on prohibiting and restricting activities in every instance. Nevertheless, we considered whether the Act could or should be leveraged

[26] For example, section 9 of the *Terrorism Suppression Act 2002* makes it a crime to knowingly deal with a designated terrorist entity's property while section 24 of the *Russia Sanctions Act 2022* makes it a crime to breach a sanction knowingly or recklessly without lawful justification or reasonable excuse.

to support businesses in implementing their sanctions obligations, as well as whether it could aid in the detection of sanctions breaches (e.g., through detecting prohibited exports). However, leveraging the Act in this way would necessitate amending the purpose of the Act as this does not explicitly include supporting the implementation of financial sanctions. It would also require consideration of whether businesses should be supervised or have additional obligations to ensure they are appropriately implementing sanctions without delay (*see* Supervising the implementation of targeted financial sanctions).

301. We identified two options for how the Act's purpose could be amended to support the implementation of sanctions. Ione option would be to amend the purpose to include supporting the implementation of sanctions as a general purpose, which would cover terrorism and UN sanctions, as well as the current sanctions against specific Russian individuals and entities. Alternatively, the purpose could be amended to focus only on a specific type or types of sanctions, e.g., only terrorism or proliferation related sanctions. However, we note the Government is still considering a possible future role for autonomous sanctions and there may be the opportunity to leverage any future sanctions framework to support businesses in implementing their sanctions obligations.

302. Submitters were split on whether the Act should be used to support sanctions, with slightly more supporting the proposal than were opposed to the idea. Submitters who were supportive noted this would ensure New Zealand meets our international obligations as well as enabling a more holistic implementation of financial crime risk management. Submitters who were opposed thought the existing approach to financial sanctions was sufficient and that AML/CFT and financial sanctions should be kept separate. Submitters were also concerned about the potential for additional obligations being imposed on businesses. These views were reiterated during the engagement we conducted in April 2022, with the private sector generally preferring that Government develop a bespoke and comprehensive regime for implementing financial sanctions rather than use the Act for this purpose.

303. We recommend amending the Act's purpose in section 3(1) to include supporting the implementation of sanctions in general. We consider that leveraging the Act for this purpose is likely to be more efficient than establishing a wholly separate framework. In addition, the outcome for reporting entities is the same whether the Act or a separate framework is used as any framework is likely to involve additional obligations for businesses as well as active supervision of those obligations.

304. We agree with the point made by submitters that the Act does not apply to all businesses that have sanctions obligations and that, as such, it is not a perfect solution for supporting the implementation of financial sanctions. However, we note that the Act likely covers the vast majority of those businesses by explicitly applying to financial institutions and DNFBPs, but that any other business or sectors could be included within the scope of the Act through regulations. Depending on the outcome of the assessment of risks in the trade finance system, this could include businesses involved in importing and exporting goods, which is also exposed to sanctions risks (*see* Combatting trade-based money laundering). This approach would improve New Zealand's compliance with international obligations and the FATF Standards and address a recommended action in New Zealand's Mutual Evaluation.

305. Finally, we do not consider that any further amendment to the Act is required to enhance detection of sanctions breaches. Businesses are already required to submit a SAR if they have reasonable grounds to suspect that the transaction or activity is relevant to the investigation or prosecution of an offence against the *Terrorism Suppression Act 2002, United Nations Act 1946*, and *Russia Sanctions Act 2022*. However, we consider that any additional guidance regarding SAR obligations (*see* Recommendation R200) could include information about how to detect a potential sanctions breach. In addition, further types of transactions could be declared as requiring PTRs if there is a risk of a sanctions breach occurring through that transaction (*see* Types of transactions requiring PTRs)

Recommendation

R4. Amend the purpose of the Act to include "supporting the implementation of financial sanctions".

3.1.3. Countering proliferation financing

306. The proliferation of weapons of mass destruction is a global threat and has increasingly become part of the FATF Standards and international expectations, particularly with the FATF amending its standards to require countries to assess and mitigate their proliferation financing risks. Proliferation financing threats emanate predominantly from two countries (Iran and the Democratic People's Republic of Korea (DPRK)), although could also emanate from non-state actors as well as other countries in the future. The Act does not have an explicit purpose of countering proliferation financing and therefore cannot be used to support New Zealand's efforts in this regard.

307. Amending the purpose of the Act to include countering proliferation financing would enable obligations to be created to combat these threats. In addition to their money laundering and terrorist financing risks, this could include requiring businesses to assess their proliferation financing risks. This could be a narrow purpose (i.e., only combatting the threats emanating from Iran and DPRK) or a more general purpose, which includes DPRK and Iran as well as any future threats that may emerge from state and non-state actors.

308. Most submitters were supportive of including combatting proliferation financing as a purpose of the Act, and almost all supported a more general purpose rather than a focus only on DPRK and Iran. Submitters noted that this would bring New Zealand in line with international expectations and developments and align with our moral responsibility to combat weapons of mass destruction. By contrast, submitters who were opposed were concerned about the compliance burden and did not consider proliferation financing a risk in New Zealand.[27]

309. In line with industry feedback, we recommend amending the Act to include combatting proliferation financing as a general purpose. While the priority would be on addressing risks emanating from DPRK and Iran, a general purpose would allow us to respond to proliferation financing risks wherever they occur. A more general purpose also ensures that the Act can continue to be useful in the event that other proliferation financing risks emerge beyond Iran and DPRK. We note that concerns regarding any compliance costs resulting from this change depends on the extent of any additional compliance obligations, which may only extend to requiring businesses to assess their proliferation financing risks (*see* Business risk assessment requirements)

Recommendation

R5. Amend the Act to include "combatting proliferation financing" as a general purpose.

3.1.4. Ensuring a risk-based approach is taken

310. The risk-based approach is core to the implementation of the Act, in that both government and businesses should be identifying areas of highest risk and taking steps to mitigate those risks (*see* Implementing a risk-based approach). A risk-based approach is at the centre of the FATF Standards and its general approach to

[27] Although there has not yet been a formal assessment of New Zealand's proliferation financing risks, we consider that New Zealand companies and other legal structures or arrangements are vulnerable to being misused to evade sanctions against DPRK and Iran as this has occurred previously. For example, SP Trading Limited (a New Zealand incorporated company) was used to lease an aircraft registered in the Republic of Georgia. This aircraft was forced down while travelling over Thai airspace and found to contain 35 tonnes of North Korean with an estimated total value of USD 18 million. See *Zhang v Ministry of Economic Development* HC Auckland CRI-2010-404-000453, 17 March 2011 at [5].

AML/CFT policy. However, despite being a core concept, the purpose of the Act does not reference a risk-based approach. We could amend the Act's purpose to include this concept. This would then ensure that both the public and private sector take a risk-based approach to implementing the Act.

311. While we did not consult specifically on this topic, many submitters stated the Act does not achieve the right balance between a risk-based approach and prescriptive requirements. This indicates that further changes may be desirable. During targeted engagement workshops in April 2022, attendees were supportive of clarity regarding the need for a risk-based approach. We therefore recommend amending the Act to include reference to a risk-based approach as a purpose of the Act.

Recommendation

R6. Amend the purpose of the Act to include explicit reference to implementation of the Act using a risk-based approach.

3.1.5. Contributing to public confidence in the financial system

312. The Act currently includes "contributing to public confidence in the financial system" as a purpose. As we note in Part A, it is almost impossible to assess the extent to which this purpose is being achieved by the regime in any comprehensive way, as confidence in the financial system is influenced by a wide variety of factors, almost all of which are beyond the influence of the AML/CFT regime (*see* Contributing to public confidence in the financial system).

313. We consider that the purpose of detecting and deterring money laundering and terrorism financing is, and should be, the primary focus of the regime. If a regime is effective at achieving this purpose it will ultimately achieve the outcome of contributing to public confidence in the financial system. However, we consider it is inappropriate for this to be an explicit purpose of the Act given the inherent difficulties with measuring the Act's impact in this regard.

314. Accordingly, we recommend removing public confidence as a purpose and as we consider this purpose misrepresents the Act's function. Instead, we recommend amending Act to include a statement of its intended outcomes in addition to its purposes. This statement should recognise that, by detecting and deterring money laundering and terrorism financing, the Act will contribute to public confidence in the financial system as well as maintaining and enhancing New Zealand's reputation and combatting serious criminal activity.

Recommendations

R7. Insert a new subsection that outlines the intended outcomes of the Act. This section should state that the outcomes of the Act are that it contributes to combatting financially motivated crimes, maintains and enhances New Zealand's international reputation, and contributes to public confidence in, and transparency of, the financial system.

R8. Remove "contribute to public confidence in the financial system" as a purpose of the Act and remove "maintain and enhance New Zealand's international reputation" from section 3(1)(b).

3.2. Risk-based approach to regulation

315. At its core, any AML/CFT regime should be based on assessment of risk: there should be an assessment of money laundering and terrorism financing at the national, sectoral, and business level, and regulation should be focused on mitigating any risks identified. A risk-based approach should also ensure that an AML/CFT regime is flexible and adapts to changes in risks, and that resources are allocated efficiently and in proportion to levels of risk. Given the importance of taking a risk-based approach,

we considered how the Act is working in this regard, including whether businesses are empowered to understand their risks and the appropriate response.

3.2.1. Framework for understanding and sharing risk information

316. The current framework for ensuring everyone in the regime understands their money laundering and terrorism financing risks has three separate but complementary components (*see* How well do we understand our risks):

- the FIU assesses national and international risks as they relate to New Zealand, and publishes this in a National Risk Assessment (NRA)
- the AML/CFT supervisors assess how national risks impact the sectors they supervise and the extent to which those sectors are more or less vulnerable to money laundering and terrorism financing. These findings are then published in the various Sector Risk Assessments (SRAs)
- businesses are required to assess the risks they are exposed to, based on the factors outlined in section 58. As part of this, businesses are required to consider any applicable guidance material produced by the FIU and supervisors, including the NRA and SRAs (section 58(2)(g)).

317. Most submitters considered that the framework requires improvements to the amount, quality, and frequency of risk information shared by agencies with the private sector. In particular, submitters did not consider that the current assessments are useful for businesses. Submitters considered that nuanced, targeted, or thematic assessments would be more useful, particularly if agencies made better use of the experience of businesses operating in those sectors. Submitters were also critical of the fact that several of the risk assessments, including the NRA, are now out of date resulting in businesses not having a current understanding of risks. Submitters further identified a lack of dynamic information about risks, threats, and typologies being shared by the FIU.

318. We identified several options that could be progressed to address industry criticisms of the current framework. These options are not mutually exclusive, and include:

- **introducing legislative requirements for producing risk assessments:** this could be achieved by amending the Act to require assessments to be produced according to a statutory timeframe. Alternatively, the Act could provide the ability for a decision-maker (such as the National Coordination Committee (NCC)) to commission the production of a risk assessment by a specific date, including specifying requirements for the risk assessment such as scope, approach, and methodology.
- **review and update the content of risk assessments to improve usability:** agencies could review and update their risk assessments with a business-focused lens to ensure they are sufficiently nuanced and detailed and analyse relevant thematic or industry areas. This approach could be supported by increased involvement of the private sector in the development of the assessments, e.g., through establishing an advisory committee or seconding experts into agencies.
- **establishing a framework for dynamic and/or live risk information:** this framework could enable the sharing of information between private sector entities and/or between the public sector and private sector. It would need to have sufficient protections and safeguards in place to ensure privacy is protected and any information is used appropriately.

319. Given the foundational importance of understanding and sharing risk information, we recommend progressing all the identified options for improving the current framework. In the long term, we recommend amending the Act to provide the ability for a decision-maker, such as the NCC, to commission the production of risk assessments to ensure that they remain current and relevant for businesses. We do not consider the ability to commission a risk assessment undermines the operational independence of any agency, as the agency would still be able to independently

assess and report on the risks within the requirements set by the relevant decision-maker.

320. Despite a commitment to Cabinet to produce the next full version by 2020,[28] the most recent NRA was completed in 2015 and had its most recent update to some of its information was in 2019. The underlying assessment is still based on the original 2015 assessment drawing on data about money laundering threats and methods from 2013. While information on the terrorism financing threat and many vulnerabilities was updated in 2019, some of these updates cannot be relied on as being current given the change of the regulatory environment (inclusion of DNFBPs in the regime, changes to forming legal persons) and changes to technology (virtual assets).

321. Without a current NRA we cannot be certain that the regime is combating areas of greatest threat as these have not been assessed and communicated to agencies or industry. We also lack the key foundation for policy development and system stewardship. We consider that the ability for risk assessments to be formally commissioned will help to ensure that risk assessments are kept up to date and to ensure the regime is able to effectively respond to dynamic risk.

322. We also recommend amending the Act to provide a framework for sharing more dynamic information about current threats and risks, akin to efforts made in the United Kingdom and Singapore. The Financial Crime Prevention Network makes some progress towards achieving this outcome, however its membership is limited to the New Zealand Police, New Zealand Customs Service, and five banks and there is no legislative framework for public-private partnerships of this kind. We consider that establishing an information sharing framework of this kind has potential for significantly improving the effectiveness of the regime, given it would allow businesses to maintain a dynamic, rather than static, understanding of risks. It would also allow the system to respond to any emerging trends or typologies more easily. However, we also recognise the need for carefully considering privacy interests as part of developing any framework and ensuring that it is used appropriately.

323. Given that our other recommendations would involve legislative changes, we also recommend that agencies review and update the content of the various risk assessments to ensure they are useful and relevant for businesses. Agencies should consider the structure and format of the assessments, as well as whether they are sufficiently focused on the themes or topics of most importance to the various sectors. Agencies should also explore whether there are opportunities for increasing private sector involvement in the production or review of risk assessments, such as through establishing a private sector advisory committee or seconding staff from the private sector into agencies.

Recommendations

R9. In the long term, amend the Act to provide for the National Coordination Committee to request that an agency produce a risk assessment with the specific requirements for the risk assessment, including scope, approach, methodology, and timeframes for completion.

R10. Develop a framework for sharing more dynamic and/or live risk information with the private sector and/or within the private sector, such as through establishing an information sharing mechanism with appropriate safeguards and protections.

R11. In the interim, agencies should review the content and format of risk assessments with a business-focused lens and explore opportunities for increased private sector involvement in the production of risk assessments.

[28] National AML/CFT Strategy 2020-2023, agreed to by Cabinet in 2019 [DEV-19-MIN-0270 refers].

3.2.2. Business risk assessment requirements

324. We considered whether the current requirements for business risk assessments in section 58 are fit-for-purpose and provide value to all businesses, as well as whether businesses should be required to assess any additional risks. For example, the FATF recently updated its standards to require businesses to assess and mitigate their proliferation financing risks, but the Act does not currently require businesses to assess this type of risk as part of their section 58 assessment.[29] However, requiring businesses to assess these risks would arguably require amending the Act's purpose (*see* Countering proliferation financing).

325. Most submitters considered the current requirements appropriate, but some indicated there are aspects of risk assessment requirements that are unclear and may not be relevant to all businesses. Some submitters noted that this could result in risk assessments not being taken seriously and treated as 'tick box' exercises. In particular, submitters thought that some of the requirements were overly burdensome and provided little value to their business or compliance programme. Submitters also thought there should be better distinction between customer and business risk assessments, as well as between factors relevant to some businesses versus those relevant to all.

326. In line with industry feedback, we recommend amending section 58 to provide clarity to businesses, including distinguishing between factors relevant to some businesses versus those relevant to all businesses. This will help ensure that risk assessments are directly relevant to businesses and avoid their treatment as a 'tick-box' exercise.

327. In addition, we recommend amending section 58 to require businesses to assess their general exposure to a potential breach, non-implementation, or evasion of sanctions obligations. As we recommend amending the Act's purpose to support the implementation of financial sanctions in general, we consider that any risk assessment obligation should similarly have a general focus, which will include assessing proliferation financing risks. This change will ensure that the Act aligns with the updated FATF Standards, as discussed above.

328. As these recommendations require legislative changes, we also recommend in the interim that supervisors update the risk assessment guidance to address any areas of uncertainty or ambiguity. The supervisors should also consider including examples of best practices in the guidance where appropriate. While businesses need to be assessing their unique risks, we received a large amount of feedback that examples of best practice will greatly assist businesses, particularly small businesses, to understand and comply with their obligations (*see* Capacity of smaller and larger reporting entities). Improved guidance and examples could also reduce the compliance costs for businesses if they were doing more than is required due to their current uncertainty about the obligation.

Recommendations

R12. Amend section 58 to improve clarity and distinguish between factors relevant to some businesses versus those relevant to all businesses.

R13. As part of amending section 58, require businesses to assess their general risk of sanctions evasion, including proliferation financing sanctions.

R14. Supervisors should further update risk assessment guidance to address areas of uncertainty and ambiguity and consider including examples of best practices where appropriate.

[29] Proliferation financing risk is defined in the FATF Standards as referring strictly and only to the potential breach, non-implementation or evasion of proliferation financing related targeted financial sanctions obligations.

329. We also considered the following minor change regarding the requirements in section 58:

Issue	Recommendation
Businesses are required to "have regard" to the factors set out in section 58(2) when conducting a risk assessment. This includes any applicable guidance material produced by AML/CFT supervisors or the Police, such as the National Risk Assessment or the various sectoral risk assessments. However, the language of "have regard to" could allow businesses to consider, but ultimately reject, government advice about national or sectoral risks and therefore fail to implement appropriate controls.	Amend section 58(2) to ensure that a business' risk assessment reflects government advice about national and sector risks.

3.2.3. Balancing prescription with risk-based obligations

330. The Act should strike the right balance between two contradictory concepts – a prescriptive approach and a risk-based approach. While some obligations should be tightly prescribed or have minimum standards (such as SAR obligations), others should be implemented "according to the level of risk" to ensure they are effective. We asked whether the Act achieves the right balance, as well as whether some areas require minimum standards. We also sought views about the role that guidance should play in implementing a risk-based approach.

331. Almost all submitters supported a risk-based approach being taken instead of a prescriptive approach. However, most did not consider that the Act currently has the correct or appropriate balance between prescriptive and risk-based approach. While some recognised that a more risk-based approach may be challenging for businesses, others noted this would support greater adoption of innovation and technological solutions and help ensure the system is resilient and dynamic.

332. Some submitters considered the requirements on low-risk businesses and products are disproportionate and inconsistent with a risk-based approach. Most submitters considered that prescription is sometimes appropriate, but only where minimum and consistent standards are required regardless of the type of business or associated risks. Some considered a significant challenge not with the requirements themselves, but how they are applied by supervisors or auditors, noting a tendency for supervisors to take the most conservative interpretation.

333. We recognise that there are several areas where the Act has taken an overly prescriptive approach, particularly CDD relating to obligations, and that this is not aligned with the risk-based approach. We consider specific CDD obligations and make recommendations regarding the balance between a risk-based and a prescriptive approach (*see* Customer due diligence). In addition to those changes, we recommend agencies explore opportunities for issuing further regulatory exemptions to tailor obligations for low-risk products, businesses, and transactions. This should include exploring opportunities for greater use of simplified CDD and building on suggestions already made for further exemptions (*see* New regulatory exemptions).

334. Many submitters identified a need for improved guidance and assistance from supervisors in general, but in particular for assessing risks. Submitters noted that more high-quality, practical, and relevant guidance would greatly assist businesses apply a risk-based approach, as well as understand their obligations. Given this, we recommend issuing further and more detailed or granular guidance to support businesses to take an appropriately risk-based approach. Agencies should, in consultation with the private sector, work to identify areas where more guidance is needed and prioritise their efforts accordingly. This ensure that the guidance being produced meets the needs of industry and improves the overall effectiveness of the system.

Recommendations

R15. Issue any further regulatory exemptions to tailor obligations for low-risk products, businesses, and transactions, as well as opportunities for making greater use of simplified CDD, provided these exemptions apply only in situations of proven low risk.

R16. Agencies should issue further and more detailed or granular guidance to empower businesses in applying a risk-based approach. Agencies should, in consultation with the private sector, identify areas where more guidance is needed and prioritise their efforts accordingly.

3.2.4. Capacity of smaller and larger reporting entities

335. We asked whether the regime appropriately reflects the size, complexity, and resources available to the range of businesses. In particular, we considered whether more could be done to ensure that compliance requirements under the Act are proportionate to the size and risks of a business.

336. Most submitters did not consider the Act strikes the appropriate balance, with several noting it takes a largely "one size fits all" approach, particularly in relation to obligations such as CDD. While several submitters noted the impact on small businesses or businesses that only provide a small number of captured activities, others noted that some large and complex entities may also have low risks. Submitters stated more could be done to support low risk businesses engaging with one another.

337. As for the cause of the imbalance, some submitters attributed this to an overly complex approach taken to implementing the regime. Submitters noted the large number of agencies, obligations, regulations, and guidance material, with no central source of information to make it easier for businesses to understand what is required. Submitters noted the significant challenge for small businesses to understand what is required, let alone how to comply with their obligations. Several submitters also identified the significant number of 'minimum level' compliance obligations that apply to all entities regardless of their size, complexity, or risk.

338. In line with feedback, we recommend agencies take further steps to make it easier for all businesses, but particularly small businesses, to comply with the Act. In particular, this should include:

- **creating a single centralised online source** of AML/CFT information and resources to reduce the challenges in understanding the various aspects of the regime
- **reviewing guidance material** to ensure it is accessible, including for people for whom English is not their first language or for people who are disabled, and
- **develop further tools and resources** to assist small businesses to comply with their obligations, as well as using different tools or platforms that are easier for the end user (e.g., goAML, *see* Ensuring the FIU receives high-quality and accurate).

339. We recognise the potential for technology to improve the effectiveness of the regime overall, and in particular for small businesses. We also asked what barriers businesses have to using technology, with submitters noting that the biggest barrier was whether it was reputable and helped them comply with the Act. As such, we further recommend that agencies explore amending the Act to provide for an accreditation or certification process for technological solutions. We consider that an accreditation or certification process will make it easier for businesses to identify what products will be useful for their business but note that impact of any accreditation on enforcement would need to be carefully considered. In the interim, AML/CFT supervisors should issue guidance about technological solutions and how businesses can get assurance about using a particular product.

Recommendations

R17. Create a centralised source of AML/CFT information and resources that consolidates all information from the Ministry, AML/CFT supervisors, and FIU.

R18. Develop further tools and resources designed to assist small businesses in complying with their obligations and that are accessible to a range of audiences (e.g., translating guidance, ensuring simple language is used, complying with accessibility standards).

R19. Explore amending the Act to provide for an accreditation or certification process for technological solutions to make it easier for businesses to identify what products will be useful. In the interim, the AML/CFT supervisors should issue guidance about how businesses can use technology.

3.3. Agency structure or model

340. The administration, application, and enforcement of the Act involves six agencies:

- **Ministry of Justice** is responsible for administration of the Act. The role of the Ministry is set out in section 149 and includes advising the Minister of Justice as to whether any changes should be made to the regime.
- **Department of Internal Affairs, Financial Markets Authority**, and **Reserve Bank of New Zealand** are designated as AML/CFT supervisors. The functions and powers of the AML/CFT supervisors are set out in sections 131 and 132.
- **New Zealand Police** is responsible for a variety of financial intelligence functions (set out in section 142) and powers (set out in section 143), including receiving SARs and disseminating financial intelligence products.
- **New Zealand Customs Service** does not explicitly have its functions outlined in the Act, but it is responsible for managing movements of cash across New Zealand's borders.

341. We consider that the agencies involved, the powers they have, the role they play, and the resources they have at their disposal are strong predictors of whether the regime is effective and can operate efficiently. Ensuring that the appropriate agencies are involved, with suitable powers and sufficient resources, will lay a strong foundation for the Act to continue to be effective in the future.

342. We initially considered whether the current multi-agency supervisory model is the best for New Zealand, particularly as there are areas where the AML/CFT supervisors have taken inconsistent approaches. However, due to a large amount of public feedback, we have subsequently taken a broader look at the overall regime. This includes considering whether any changes should be made regarding administration of the Act and the role and position of the FIU. We also considered how the regime can be appropriately resourced, as well as the role the private sector could or should play in the regime's governance and administration.

3.3.1. Coordinating within the regime and between other regimes

343. The Act establishes an AML/CFT Coordination Committee known as the National Coordination Committee (NCC) (section 150), which is chaired by the Ministry of Justice and attended by Customs, the Police, and the AML/CFT supervisors. In addition, the Act allows for other persons to be invited to join the NCC, provided they are from another government agency. In practice, this power is used to invite Inland Revenue, Ministry of Business, Innovation and Employment, Ministry of Foreign Affairs and Trade, and the Serious Fraud Office to attend NCC meetings, given these agencies have general interest in the operation of the AML/CFT regime.

344. The functions of the NCC are set out in section 151, and include facilitating necessary information flows between agencies, the production and dissemination of information about risks, and providing a forum for examining any operational or policy issues that have implications for the effectiveness and efficiency regime. The functions also include facilitating cooperation among the AML/CFT supervisors, a consistent and coordinated approach to the development of guidance, and good practice and consistent approaches to supervision.

345. The FATF generally considered that domestic coordination and cooperation are strengths of New Zealand's system, which is supported by the operation of the NCC. However, they noted that there were weaknesses with respect to how the AML/CFT regime coordinates and engages with other regimes, such as the broader counterterrorism regime, counter-proliferation regime, sanctions regime, and international trade regime (*see* Cooperation with related regimes). We also note that several of the concerns raised by submitters indicate that the NCC may not be adequately fulfilling its functions of facilitating the production of information about risks (*see* Framework for understanding and sharing risk information) or consistent supervision (*see* Supervisory structure).

346. To enhance the coordination of efforts with complementary regimes, we recommend inviting further agencies to join the NCC. In particular, we recommend inviting other law enforcement or regulatory authorities (such as Ministry of Social Development, Ministry for Primary Industries, and the Commerce Commission) and other intelligence agencies (such as the New Zealand Security Intelligence Service and the Government Communications Security Bureau). We also make various recommendations to enhance the functioning of the NCC, such as providing it an ability to commission risk assessments (*see* Recommendation R9) or ensure consistency of supervision (*see* Recommendation R22).

Recommendation

R20. Invite further regulatory, law enforcement, and intelligence agencies to join the NCC to enhance the coordination of efforts with complementary regimes.

3.3.2. Supervisory structure

347. A core component of the AML/CFT regime is that it needs to enable effective supervision and regulation of businesses. The supervision and monitoring of businesses should address and mitigate money laundering and terrorism financing risks in the economy, in part by promptly identifying, remedying, and sanctioning (where appropriate) businesses that do not adequately comply with their obligations.

348. We have identified several challenges with the current supervisory model. The first is that this structure can make it difficult to ensure that supervisory resources are allocated in accordance with a risk-based approach, as there is no ability to direct how resources are allocated between AML/CFT supervisors. This was a finding in New Zealand's Mutual Evaluation and can result in some medium risk sectors being supervised more intensively than higher risk entities. This issue can be further compounded by the fact that AML/CFT supervision is resourced within existing agency priorities, which may make it difficult for AML/CFT supervisory functions to be given enough resource as they compete with other functions, including prudential supervision. Furthermore, we note that there is generally limited supervisory resource available in New Zealand, no cross-agency workforce plan, and inconsistent pay bands between supervisors, meaning that the AML/CFT supervisors can sometimes compete with one another (and the private sector) for the same people. Finally, having multiple AML/CFT supervisors necessarily results in duplication of corporate functions and requires additional resource to be used for coordination.

349. The second challenge identified is that the current model can sometimes result in inconsistencies of approaches, interpretation, and guidance between the three supervisors. While some inconsistency may be justified due to the inherent differences in the nature of the sectors being supervised, submitters indicated that

there are some instances (e.g., prescribed transaction reporting) where the inconsistency is unwarranted. This issue is compounded by the fact that there is no ability for another agency (e.g., the Ministry) or the NCC to direct how other agencies should be interpreting or applying the law in a way that is consistent with the purpose of the Act; the only power that the NCC has is to *facilitate* good practice and consistent approaches to AML/CFT supervision (section 152(e)). This power has not been sufficient to overcome situations where the AML/CFT supervisors are applying differing interpretations of the Act with some sectors being required to comply (or not) with an obligation by virtue of who they have as an AML/CFT supervisor.

350. The final challenge is that there is no ability for reporting entities to complain or seek reviews in appropriate circumstances about the conduct of the AML/CFT supervisors beyond seeking a judicial review (e.g., where there are issues of inconsistency or unfair treatment). This can mean that, outside expensive legal proceedings, the AML/CFT supervisors are not being appropriately challenged by businesses and can mean that some businesses are complying out of fear and are not able to properly engage with their AML/CFT supervisor. This challenge can also be compounded by the extent to which the private sector is involved in the operation of the regime – many submitters considered that there could be greater involvement of businesses in the production of guidance and risk assessments to ensure they will be fit-for-purpose (*see* The role of the private sector)

There are several potential options to improve AML/CFT supervision

351. We have identified several options for changing the framework for AML/CFT supervision to ensure a consistent and risk-based approach to supervision:

- **establish a single AML/CFT supervisor:** this agency would be responsible for supervising all reporting entities and allocating resources appropriately. Only one agency would need to make resourcing decisions, and if it was a new (rather than existing) agency, there would be no risk that AML/CFT supervision conflicts with other agency priorities. A single agency would also be able to resolve differences of interpretation internally, and there would be a consolidation of overheads and less resource required for coordination. However, a single separate AML/CFT supervisor would not be able to leverage off prudential supervisory activities and would result in businesses in those sectors having multiple regulatory agencies with which to engage.

- **establish a central administration agency:** this agency would be responsible for producing guidance, determining how agencies should apply the law. This agency could also be responsible for employing supervisory resources and seconding staff as required into RBNZ, FMA, and DIA to conduct supervisory activities. Alternatively, this agency could be responsible for having oversight of how supervisors operate, resolve complaints, and ensure appropriate consistency. As with having a single supervisor, a central administration agency would result in a single decision maker regarding how to apply the law as well as how resources are applied across the regime. However, this option would also result in an additional agency in the regime and thereby increase overall complexity of the system.

- **change how supervisory responsibilities are split:** for example, supervision could be divided between financial and non-financial supervision and split between two existing agencies rather than three. This would ensure there more of a risk-based approach taken within financial and non-financial sectors and would slightly reduce the complexity of the regime. However, by itself, this option would not be able to overcome any situations where inconsistent approaches are taken between the two AML/CFT supervisors where it is not justified by the differences in the nature of the sectors. It also would not overcome instances where AML/CFT supervision is not given the appropriate priority within the existing agencies.

- **enhance the powers of the NCC:** this could involve establishing a specific AML/CFT appropriation to fund supervisory resources and amending the Act to empower NCC to direct allocation of resources within each supervisor. NCC could also be given the explicit power to resolve issues of inconsistency (either on its own initiative or

following a complaint being raised) and determine how the AML/CFT supervisors should be applying the law.

352. In addition, some of the challenges identified may be able to be resolved by enhancing the current supervisory framework. In particular, some of the issues identified by the private sector and the FATF (e.g., timeliness and quality of guidance and the breadth and depth of supervision in the banking sector) could be resolved by ensuring that supervisors are appropriately resourced (*see* Ensuring there are sufficient resources to deliver the regime). A cross-agency AML/CFT workforce plan could also be developed to ensure appropriate resource allocation across the regime, and the supervisors could develop their own processes for reviewing and resolving complaints, such as establishing an ombudsman scheme. However, we also note that the current supervisory framework has not been able to resolve several of the challenges that have been identified, despite them being known for several years.

Submitters expressed a number of concerns with the current structure

353. A large number of submitters considered that the current model is slow, leads to inconsistent approaches and regulatory arbitrage, is not sufficiently risk-based, duplicates efforts, and does not foster sufficient collaboration between agencies as well as the private sector. Some submitters also did not consider that supervisors are sufficiently resourced, which limits the extent to which supervisors can engage with and properly understand their sectors as well as take a strategic approach to the regime. However, some submitters noted that the current model allows each supervisor to focus on specific sectors and build an awareness of how each sector operates.

354. Furthermore, most submitters considered that the current AML/CFT framework does not appropriately ensure consistency between the supervisors. Submitters noted different approaches taken with respect to regulatory action, interpretation, and supervision of similar sectors. However, a small number of submitters thought the supervisors did apply the Act consistently, with others noting there are areas where a consistent approach is not appropriate due to different sectoral needs.

355. Submitters were split over whether the supervisory model should be changed. A number of submitters thought the supervisory model should be changed while others preferred the current arrangement with some also noting the need for significant improvements. If the model were to change, most submitters supported having a single supervisor responsible for all entities with submitters considering this model would make the regime more consistent, clear, and efficient, and lead to higher quality supervision and guidance, provided the supervisor is sufficiently resourced.

356. Alternatively, some submitters suggested retaining three supervisors but having an additional agency responsible for oversight, administration, and interpretation of the Act and the functions of the supervisors, or splitting supervision between two agencies rather than three. Submitters thought greater consistency could be achieved under the current model through establishing an agency or committee that is responsible for reviewing the and clarifying the application of the law, engaging in more industry consultation, improving governance, and developing joint supervision plans.

357. During further consultation in April, the private sector expressed support for exploring alternative arrangements but wanted to see short-term changes that could ensure consistency of supervision without waiting until we have explored alternative approaches. The private sector also noted that any mechanism set up for complaints needs to sit independently of the AML/CFT supervisors.

Another model may be viable, but further analysis and engagement is required

358. We recommend further exploring whether an alternative approach to supervisory arrangements would address issues related to risk-based approach to supervision, supervisory consistency, and the ability for complaints to be resolved. Examples of what an alternative approach could look like is discussed further at the end of this section (*see* Potential alternative approaches to agency structure).

359. We consider that resourcing underlies a number of issues with the current institutional arrangements, particularly consistency of the AML/CFT supervisory framework, and most other aspects of the regime. Any option to improve resourcing will need to be considered alongside other changes (*see* Ensuring there are sufficient resources to deliver the regime). We also consider that while some level of non-uniformity is warranted due to different sectorial needs, the current supervisory model is producing inconsistencies that need to be addressed through changes to the institutional arrangements of the regime.

360. However, given the potential scale of the changes we consider further work is necessary to confirm the root causes of the problems before making a firm recommendation about a particular alternative approach. This would include conducting a full assessment of the costs and benefits of any alternative model (including an assessment of transition costs for the regime), which we have not been able to conduct as part of this review (see Limitations of the approach). This assessment would also consider whether there are changes that could be made within the status quo arrangements that would effectively address the issues identified. However, as noted, several of the challenges that have been identified have been long-standing issues that have not been able to be resolved within the current framework.

361. Given that our main recommendation is a potentially long-term change, we recommend exploring options for ensuring that NCC is able to resolve issues of inconsistency in the interim. This could include allowing the NCC to decide how the law should be applied by agencies given its statutory responsibility of facilitating good practices and consistent approaches to AML/CFT supervision (section 152(e)). However, this option would be limited to the current functions of the NCC outlined in the Act, which does not include the ability to make decisions about resource allocation or how the law should be applied.

Recommendations

R21. In the long term, explore whether an alternative approach to supervisory arrangements would address issues related to risk-based approach to supervision, supervisory consistency, and the ability for complaints to be resolved.

R22. In the short term, explore options for ensuring that NCC is able to resolve issues of inconsistency and decide how the law should be applied given its statutory responsibility of facilitating good practices and consistent approaches to AML/CFT supervision (section 152(e)).

3.3.3. Financial intelligence

362. The FIU is a central and fundamental part of the AML/CFT regime, responsible for receiving and analysing all reports submitted by businesses and producing timely and actionable intelligence for other agencies to use. The FIU is also responsible for producing strategic analysis about money laundering and terrorism financing risks, threats, typologies, and has to date led the production of the National Risk Assessment.

363. Section 142 of the Act vests a range of financial intelligence functions in the Commissioner of Police, including:

- receiving and analysing suspicious activity reports, prescribed transaction reports, and border cash reports, as well as financial intelligence from international authorities
- analyse reports received to assess whether anything should be referred to law enforcement agencies for investigation
- access relevant financial, administrative, and law enforcement information to support financial intelligence functions, including analysing reports

- produce risk assessments relating to money laundering and terrorism financing to be used by other government agencies
- produce guidance material, including information about typologies of money laundering and terrorism financing and guidance for how businesses can meet their obligations
- provide feedback to businesses on the quality and timeliness of their reporting and referring reports and feedback on reports to the AML/CFT supervisors.

364. The FATF determined that the FIU is well situated to understand law enforcement priorities and strategic objectives, and its collaborative relationships with LEAs is a key strength. They found that FIU produces and disseminates a wide range of financial intelligence products that generally support the operational needs of competent authorities. However, the FATF also noted that 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.

365. The FATF identified strengths in the FIU performance when providing intelligence to support Police's priorities. However, the FATF noted that while the FIU is responsive to feedback from law enforcement authorities (typically the Police), there was less financial intelligence produced on its own merits based on the FIU's own or the AML/CFT system's priorities. The FATF noted that this has resulted in the FIU not fully exploiting the potential of financial intelligence to detect criminal activity by persons not already known to Police and a relatively small number of investigations initiated on the basis of FIU reports alone.

366. As part of public consultation, many submitters from industry were critical of the extent to which the FIU provides value to businesses and is fulfilling its statutory functions. Submitters considered that the FIU could do more to support industry's effort to identify and report suspicious activities, by providing more dynamic risk information and making it easier for SARs or PTRs to be filed. Submitters were also critical of the limited feedback received about reports businesses have filed and whether the FIU is promptly acting on any intelligence in those reports (*see* Risk-based approach to regulation and). We have also noted that the lack of an updated NRA is potentially undermining its ability to detect and deter money laundering and terrorism financing (*see* Detecting and deterring money laundering and terrorism financing).

367. Given these concerns and feedback, we have examined the way the Act sets out the role, functions, and institutional arrangements of the FIU. By doing so, we have sought to determine whether there are any structural reasons contributing to the issues highlighted by submitters and to ensure the FIU can continue to be an effective part of New Zealand's AML/CFT framework.

Ensuring FIU independence to deliver AML/CFT services

368. The FATF Standards require FIUs to have the independence, authority, and capacity to carry out their functions freely including making the decision about who to target and what intelligence products to produce. The Egmont Group of Financial Intelligence Units has provided further guidance on constituting an independent and autonomous FIU as precondition for effectiveness.[30]

369. The New Zealand system is too small for to merit a standalone FIU. The functions of New Zealand's FIU are vested in the Commissioner of Police but delegated to the Head of FIU, who is a Police manager. Locating the FIU within the New Zealand Police provides for a number of benefits and efficiencies in terms of access to corporate services such as human resources, finance, and legal advice. The arrangement also

[30] Egmont Group of Financial Intelligence Units (2018) Understanding FIU Operational Independence and Autonomy

allows close cooperation with other parts of Police and other law enforcement agencies.

370. Many countries take a similar approach of locating the FIU within the structure of another authority. To assist countries in implementing such structures, the Egmont Group guidance noted factors that can pose unique issues or challenges, such as where:

- the hiring, firing, or replacing of staff requires approval from another rank within the organisation or that recruitment processes are directed by the overall organisation
- FIU staff may be tasked to perform other duties different from the FIU's core functions
- the FIU does not have its own budget, rather is embedded within the larger organisation's budget
- the FIU does not have complete authority to allocate its budget, for example the FIU requires prior approval to improve its infrastructure, including securing its facilities, or to hire new staff, and/or
- the FIU does not have the ability to obtain the resources necessary to independently perform its mandate.

The extent to which Egmont Group factors exist for the FIU

371. Although several of the factors identified by the Egmont Group may exist for the FIU, we note that the arrangement for the most part works well to deliver the core intelligence functions. The main areas for improvement relate to resourcing other AML/CFT system priorities.

372. As above, the FIU's location within Police provides economies of scale in terms of access to corporate services, such as human resources. The FATF findings indicate that this has allowed the FIU to access staffing and expertise to deliver its intelligence functions. Although the Head of FIU requires official sign-off from a higher Police manager to recruit within the allotted budget, this has not impeded FIU recruitment in practice. FIU intelligence staff also have access to the standard Police intelligence career structures and training, although this comes at the expense of the FIU having autonomy to specialise training or salary bands.

373. FIU staff may theoretically be redeployed for other Police priorities. Examples of this occurring was a major concern in the 2009 mutual evaluation, which led to the FIU being moved to the specialised Financial Crime Group. Since this move, redeployment of FIU staff has typically only been for exceptional circumstances, such as to support the Police operation following the Christchurch terror attacks.

374. The FATF noted that there is a New Zealand FIU budget within Police's overall budget, but this budget is controlled by the National Manager of the Financial Crime Group (within which the FIU exists). In addition, the FIU needs to follow a wider standard organisational budgetary process when changing its budget, and any changes are weighed against Police's key performance areas rather than the AML/CFT system priorities.

375. We note that the independence of an FIU budget appears to have some impact on the overall effectiveness of a country's financial intelligence system. Of the FATF assessments[31] where the FIU was found not to have sufficient budgetary independence, 75 percent were found to be moderately effective for Immediate Outcome 6, which relates to financial intelligence, while only 25 percent were found to be substantially effective. By contrast, 69.7 percent of FIUs where there was sufficient

[31] These assessments were for the following countries: Australia, Austria, Bahrain, Belgium, Canada, China, Denmark, Finland, Greece, Hong Kong, China, Iceland, Ireland, Israel, Italy, Japan, Korea, Malaysia, Mexico, New Zealand, Norway, Portugal, Russian Federation, Saudi Arabia, Singapore, Spain, Sweden, Switzerland, Turkey, United Arab Emirates, United Kingdom, and United States.

budgetary independence received a rating of substantially or highly effective for Immediate Outcome 6. We also note that the vast majority (74.2 percent) of FATF FIUs have an independent budget, including where they are hosted by another organisation.

376. Government investment has been provided to the FIU to match its expanded intelligence function from successive legislative changes. Since 2012 this has seen the FIU double, to around 30 staff, following investment for the commencement of the Act in 2013, prescribed transaction reporting in 2017, and the commencement of Phase 2 reforms in 2018. Police has also invested NZD 5 million in the FIU's information technology systems since the Mutual Evaluation. However, there are no provisions to ensure that these resources are retained so that the FIU is able to continue to effectively deliver its intelligence functions.

377. At the same time, the Act does not have provisions to ensure that other AML/CFT priorities for FIU services are resourced. AML/CFT priorities like guidance, a user-friendly portal for submitting reports, and producing actionable strategic intelligence for the regime are areas of long-standing weakness identified by submitters and other agencies. The FIU is in the process of rolling out changes to make the reporting portal more user-friendly using Police investment in FIU IT systems. However, the speed of changes has not met stakeholders' expectations and there is little that the AML/CFT system can do to influence this were AML/CFT priorities to not affect Police's core business.

378. We recommend amending the Act to independently constitute the FIU distinct from the Commissioner of Police. Independently constituting the FIU would not necessarily mean that the FIU would move from being housed within the Police. However, independently constitution would mean that the FIU has its own budget and the exclusive authority to make decisions about how the budget is spent to achieve AML/CFT system outcomes. We consider that this change would provide a range of benefits to the FIU and the regime overall and help improve the accountability of the FIU against its legislative functions. Note that we also recommend changes to resourcing the overall regime – as part of this work, we recommend exploring how to ensure stewardship functions are sufficiently resourced (*see* Ensuring there are sufficient resources to deliver the regime).

Recommendations

R23. Amend the Act to constitute the FIU as distinct entity from the Police to improve accountability against legislative functions subject to further engagement on the design and form of the FIU.

R24. As part of changing how the regime is resourced, agencies should explore how to ensure stewardship and strategic functions are sufficiently resourced (*see* Recommendation R29).

Position of the FIU within the regime

379. The FIU is currently housed within the Police due to the financial intelligence functions being vested in the Commissioner of Police. If changes to the AML/CFT supervisory framework are progressed there would be an opportunity to consider whether it should continue to be housed within Police as part of the broader changes to the structural framework of the Act (*see* Supervisory structure). Countries are free to choose how to structure their FIU, and there are several approaches that can be taken: most FATF countries have their FIU as part of a law enforcement agency, but countries also have their FIU as part of a supervisory authority or as an entirely separate agency. Overall, we are neutral as to whether any change should be made to the position of the FIU, and any change would require a detailed assessment of the costs and benefits before it is agreed.

Recommendation

R25. As part of exploring alternative approaches to the structure or framework of the regime, explore changing the position of the FIU within the regime.

3.3.4. Policy and administration

380. The Ministry of Justice is responsible for policy and administration of the AML/CFT regime. However, in most other jurisdictions, responsibility for administering the regime sits elsewhere, typically with the Treasury or Finance Ministry. We also note that other agencies have policy responsibility for other regulatory regimes that directly impact on the effectiveness and efficiency of the AML/CFT regime. For example, Ministry for Business, Innovation, and Employment (MBIE) is responsible for administering the Financial Services Provider Register and policies relating to forming legal persons, both of which directly impact on the AML/CFT regime.

381. Given other countries take a different approach to the one New Zealand has taken, we recommend exploring options for sharing administration of the regime with another agency, such as MBIE, as part of the general consideration of whether there should be a different institutional framework of the regime (*see* Potential alternative approaches to agency structure). We consider that co-administration of the regime could result in reforms being progressed more promptly, better linkages with complementary regimes as well as more policy advice that is better able to consider the overarching system. However, we also note that it is important to maintain the criminal justice focus of the regime, and therefore do not recommend shifting policy responsibility entirely to another agency.

Recommendation

R26. As part of considering an alternative institutional framework for the AML/CFT regime, consider options for co-administration if this would result in prompter reform, better linkages with complementary regimes and improved or more well-rounded policy advice.

3.3.5. The role of the private sector

382. Effective partnership between the public sector and the private sector is essential to combat financial crime. However, New Zealand will always be vulnerable to money laundering and terrorism financing if only some businesses are properly addressing their financial crime risks while others are not. Increasingly, businesses in other countries are taking an approach of 'not in my country' rather than 'not in my firm' and are actively cooperating to ensure that financial crime and dirty money has no place in their sector.

383. There is no formal mechanism in the Act that provides for a cooperation or feedback mechanism between the private sector and government except where some secondary legislation is being developed (e.g., section 154). The private sector is also unable to participate in the NCC due to the requirement that members are employed by the Government. Nevertheless, some AML/CFT agencies – including the Ministry – run their own forums and groups for public/private engagement and partnership and regularly conduct informal engagement with the private sector (*see* Establishing the Industry Advisory Group).

384. We considered how to increase the private sector's involvement in the operation of the regime and how to move towards the regime operating as a genuine partnership between the private and public sectors. One option is to generally increase the level of involvement in the development of guidance and policy reforms, such as through increasing the level of engagement or moving towards a co-design model. Another option is to create ways for the private sector to be directly involved in the governance or stewardship of the regime, such as amending the Act to allow the private sector to participate in the NCC or through formalising and consolidating existing advisory committee arrangements.

385. Submitters generally supported increased private sector collaboration and coordination within the regime, provided it was on a voluntary basis. In line feedback received, we recommend agencies formalise and potentially consolidate the existing advisory group arrangements that have been established. We consider this is the most efficient way for the private sector to directly engage in the operation and

governance of the regime and influence government decisions and could also be leveraged to support a hybrid funding model (*see* Ensuring there are sufficient resources to deliver the regime). As part of formalising these groups, agencies should ensure that the group is sufficiently representative and transparently operated so that he private sector can fully engage with the operation of the group.

Recommendation

R27. Formalise and consolidate the existing advisory group arrangements to increase the amount of private sector input into the operation and governance of the AML/CFT regime. Agencies should ensure that the regime-wide advisory group is sufficiently representative and transparently operated.

3.3.6. Ensuring there are sufficient resources to deliver the regime

386. Many submitters raised concerns as to whether the AML/CFT regime had sufficient resources to deliver the necessary functions. Submitters thought that insufficient resources could be responsible for some of their frustrations with the regime, such as unresponsive and inconsistent regulation, insufficient and out of date risk information, inadequate guidance and support, and lengthy and delayed reform processes. These concerns were reflected in the findings of the Regulatory Maturity survey (*see* Maturity of the regulatory system). The FATF also identified concerns regarding supervisory resourcing and recommended that there should be enough resources to ensure the appropriate scope and depth of supervision of all sectors, but particularly the banking sector.

387. We considered various options to ensure there are sufficient resources for the regime. One option would be to seek an increase to the baseline appropriations for the agencies involved to ensure there are enough resources. The last time AML/CFT resources were increased was in 2017 to those agencies impacted by including non-financial sectors in the regime (i.e., DIA, Police, and the Ministry), but there was no increase the funding available for rest of the regime. Agencies could seek changes to funding as part of considering any alterations to the overall agency structure, particularly as any changes that consolidates or centralises some functions would likely have the effect of lowering resourcing needs by reducing duplicated resources and overheads (*see* Supervisory structure).

388. In addition to an increase to baseline funding of the regime, another option is to introduce a hybrid public/private funding model for the regime through creating a levy. Some countries, such as Australia, entirely fund the operation of their AML/CFT supervisor and FIU through industry contributions. We have identified that charging each business a small amount could result in significantly more resources for the regime. For example, each business paying NZD 1,000 per annum would result in an additional NZD 6.4 million for the regime (a 45% increase) and help ensure there were enough resources for the regime. An industry contribution model would also enable the regime to be more dynamic and responsive without having to continually seek changes to baseline appropriations, which would ensure that it can address compliance challenges at a faster rate, produce more comprehensive guidance, and make it easier for businesses to comply and potentially reduce overall compliance costs.

389. However, given the existing costs of compliance for industry (*see* Cost of the regime), we recognise that a levy would need to demonstrate good value for money and deliver more responsive guidance, supervision, support, and reforms. This could be achieved by basing any contribution from industry on a forward workplan agreed to between the private sector and public sector. This workplan could outline the desired outputs from the regime (such as new guidance or tools being developed, new risk assessments, and legislative or regulatory reforms) with the private sector's contribution determined by the amount that cannot be met from existing or additional baseline funding. This is similar to the approach taken in the gas industry, where

industry participants fund the operation of the industry body through a levy based on an agreed work programme.[32]

390. Most submitters opposed the introduction of fees for three broad reasons: some businesses already pay licensing fees to another regime, the fee would be disproportionate to the risk in some sectors, and AML/CFT is a public benefit, and the costs should be borne by the government. However, attendees at the targeted engagement workshops in April 2022 expressed more support for the proposal for a levy determined by a collaborative work programme and thought this should be considered independently of any changes to the overall agency structure.

391. To ensure there are sufficient resources for the AML/CFT regime, we recommend seeking an increase to the existing agency appropriations as part of any changes to the regime, as well as exploring the creation of a hybrid funding model. We broadly agree with submitters that the government should bear most of the cost of administering the regime, particularly given that combatting illicit financial activity is a public good that all of New Zealand enjoys. However, we also recognise that a considerable amount of what the regime produces (e.g., guidance and technical policy reforms) are designed only to benefit businesses and make it easier for them to comply with their obligations. Accordingly, we consider that there is opportunity to create an innovative approach to funding that is responsive, resilient, and dynamic.

392. We anticipate that the details of the hybrid funding model would be developed as part of amending the Act to enable the levy to be charged. One key question that would need to be resolved is which businesses would be required to pay and how much businesses would be charged. Our initial view is that all businesses should be required to contribute some amount, but the amount charged is proportionate to the business' revenue. We also note that further work would be required to determine how a levy would be administered and governed. In particular, there would need to be clarity regarding how the levy amount is determined and how frequently it is set. If the levy is set based on a work programme, agencies would specifically need to determine how the work programme would be developed and agreed to by the private sector, as well as what happens if the items on the work programme are not delivered by the agreed date.

Recommendations

R28. As part of considering an alternative institutional framework for the AML/CFT regime, seek increases to the baseline appropriations for agencies. The necessary increase would depend on whether any changes are progressed to consolidate or centralise functions, as this would likely reduce the resourcing needs of the regime.

R29. Amend the Act to establish a hybrid public/private funding model to partially support the regime's operation, subject to further consultation on the viability of the model and how it would work in practice.

3.3.7. Potential alternative approaches to agency structure

393. This section outlines several possible models for the AM/CFT regime and combines options from the preceding sections. We intend this section to be indicative only, as any changes would require a comprehensive assessment of the costs and benefits of any change. Different models were considered in the process of developing the Act. We originally determined that using government agencies with existing regulatory relationships with sectors was the best approach in the New Zealand context as it was cost effective and would leverage the existing knowledge and relationships agencies had developed through their prudential regimes. That being said, we also note that the Select Committee report on the *AML/CFT Bill* expressed concern about the

[32] For further information see https://www.gasindustry.co.nz/our-work/work-programmes/levy/#overview

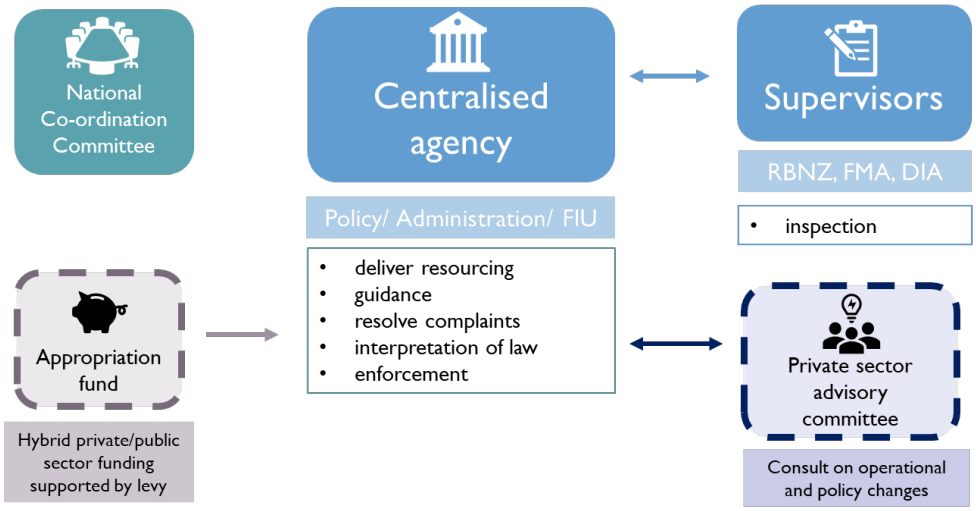
proposed supervisory model, noting that the Australian model of a single supervisor was preferable and that the proposed arrangement seems administratively untidy.[33]

394. We identified six alternative arrangements for the regimes that might address the issues identified in the review (including enhancing the status quo), specifically: (1) creating an oversight body; (2) creating a central administration body; (3) centralising administration and policy in one agency; (4) combining policy, administration, and the FIU in one agency; (5) having a single supervisor; and (6) combining supervision and the FIU in one agency.

395. We used these models as a reference point for the further engagement we conducted with the private sector in April 2022. As well as considering different agency arrangements, these models consider how different resourcing models and private sector engagement could feed into the structure (*see* Ensuring there are sufficient resources to deliver the regime). While these features could be progressed without changing agency arrangements, we considered that we need to consider how these different elements work together to create greater efficiencies.

396. The private sector singled out three models that they considered could provide a range of benefits. Consistent with feedback about the complexity of the regime (*see* Capacity of smaller and larger reporting entities), the private sector's preferences leaned towards models that simplified and brought together different functions of the regime. We have included the three preferred models below, along with our initial analysis, and recommend that further work is undertaken to fully assess the costs or benefits of these options as well as any alternative options that were not identified.

Option one: combined policy/administration/FIU

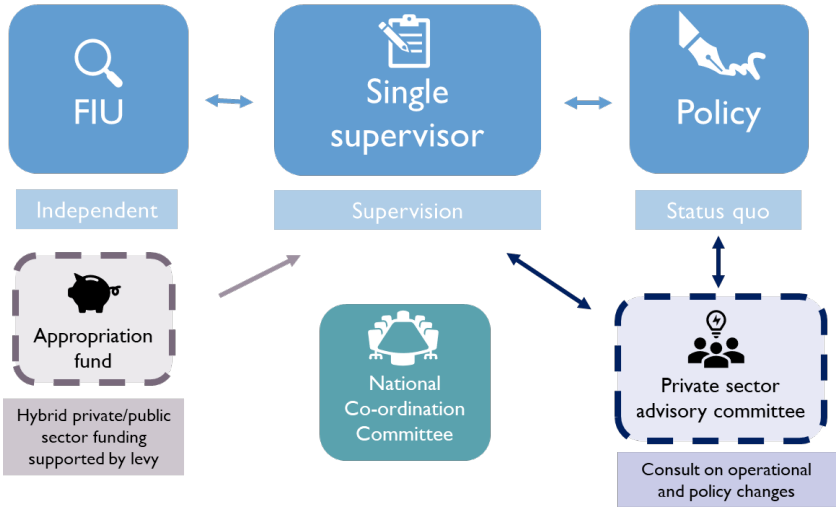


397. This option would see the policy and administration function combine with the FIU in a centralised, stand-alone agency. This agency could take responsibility for some of the tasks currently undertaken by the AML/CFT supervisors, such as producing guidance, providing a unified view of the Government's interpretation of the Act, and carrying out enforcement functions. Inspection could continue to be carried out separately by the existing supervisors, utilising their existing relationships with the private sector. However, the resourcing for supervision would come from the central agency with staff deployed staff deployed as required. This model could also consider splitting supervision between two agencies, divided between financial and non-financial institutions respectively, or even just one agency

[33] *Anti-Money Laundering and Countering Financing of Terrorism Bill*, as reported from the Foreign Affairs, Defence and Trade Committee on 14 September 2009: https://www.legislation.govt.nz/bill/government/2009/0046/19.0/096be8ed804522d5.pdf

398. This option also allows for the enforcement function to be separated from the inspection function. The private sector was supportive of this approach as they wanted more consistency in the way enforcement is undertaken as under the current model, different supervisors take different actions depending on factors such as resourcing and agency priorities. The private sector noted that bringing the intelligence function closer to the guidance aspect in the centralised agency could lead to better informed decision-making. They also considered that this option could speed up and simplify the process for producing guidance, noting that having a number of agencies involved slows the ability for guidance to be responsive to issues that arise.

Option two: single supervisor model

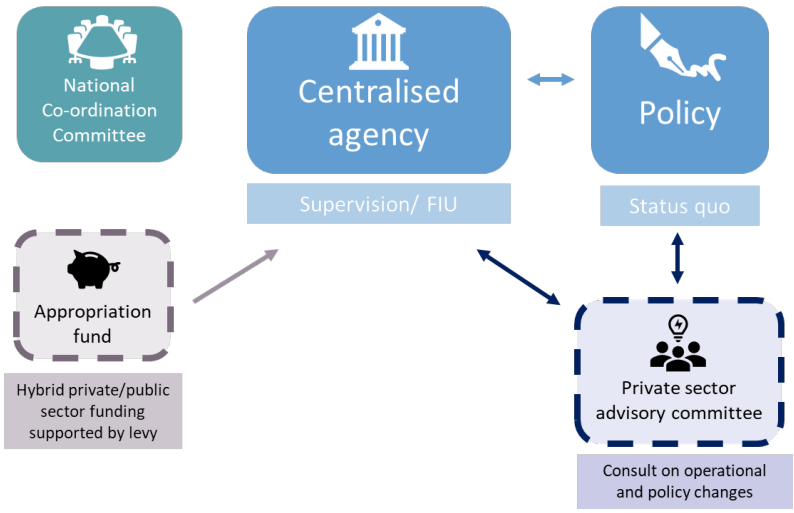


399. This model maintains the status quo for most functions but consolidates the three supervisors into a single supervisor. The single supervisor would retain the supervisory function under the Act but could also carry out some administrative functions currently undertaken by the Ministry, for example, processing exemptions applications. Under the current model, this would not be feasible as having these functions spread across three agencies would create challenges around consistent decision-making.

400. In terms of structure, the single supervisor could exist as its own agency, or it could be housed within an existing supervisor, i.e., DIA, FMA, or RBNZ. The benefits of its own agency would be that AML/CFT supervision would not have to compete with other agency priorities. However, this may not be a problem if supervision is kept within a sufficiently resourced existing supervisor, so long as enhancements could be made to operational independence. Attendees at the targeted engagement workshops we ran in April 2022 noted that it could be cheaper and simpler to consolidate resources within an existing supervisor.

401. A strength of this model is that a single supervisor would simplify the process for issuing guidance allowing the supervisor to be more responsive to needs and emerging risks. Attendees also noted the benefits of having guidance and inspections kept together under one agency, which would be more consistent in the interpretation and enforcement of the law.

Option three: combined supervisor/FIU



402. This model features a single supervisor with the FIU housed within it. This is the approach taken in Australia, where the Australian Transactions, Analysis, and Reporting Centre (AUSTRAC) is responsible for both supervising businesses as well as financial intelligence functions.

403. This model contains the same advantages as the single supervisor model in terms of more responsive and consistent guidance. However, a distinct advantage is that it could more closely align the intelligence function performed by the FIU with the inspection and enforcement function performed by the AML/CFT supervisor. The private sector considered this a particular strength of the model and generally preferred this option over the alternatives. However, moving the FIU from Police could result in different inefficiencies and challenges that would need to be avoided. Further, many effective FIUs operate as law enforcement style, although only administrative-style FIUs have been found to be highly effective by the FATF.[34]

404. Overall, submitters supported a model that would provide the following benefits:

- allow for greater simplification and consistency e.g., responsive guidance, consistent interpretation of the law and enforcement decisions.
- consolidate functions into fewer agencies leading to better informed decision-making and making it easier for businesses to engage. However, there were different views on which functions should be kept together e.g., policy and guidance, or supervision and guidance.
- enable a greater focus on AML/CFT within agencies, with more focused resourcing and greater expertise.

405. The private sector also noted that changing the model does not necessarily change the substance of what agencies do and that it is important that we also focus on ensuring the right people are involved and bring in more resources to support areas that are struggling. We agree that we cannot rely on changes to the model to fix the issues identified. However, we do consider that it is important to explore whether a different model could better facilitate improvement to these areas.

[34] The only FATF countries that have been found to be highly effective for Immediate Outcome 6 (which relates to the use of financial intelligence) are Israel, Russian Federation, and Spain, all of which operate administrative-style FIUs.

Recommendation

R30. Further explore alternative approaches to agency structure to determine whether any other approaches would result in the regime being more effective and efficient. This should include conducting a cost-benefit analysis of any alternative model(s) as well as an assessment of transition costs for the regime.

3.4. Agency powers or functions

3.4.1. Supervision

Supervising the implementation of targeted financial sanctions

406. No agency currently has the explicit authority to supervise whether businesses are complying with their existing financial sanctions obligations (*see Supervising the implementation of targeted financial sanctions*). This was identified as a significant gap in New Zealand's Mutual Evaluation that undermines our effectiveness in using financial sanctions to combat terrorism and the proliferation of weapons of mass destruction. We asked which agency or agencies should be empowered to monitor and supervise compliance with financial sanctions obligations, noting that it could be the AML/CFT supervisors or an entirely separate agency or agencies who could perform this role.

407. A large majority of submitters thought supervision of financial sanctions should fall within the scope of the AML/CFT regime with existing supervisors empowered to perform this function. However, some submitters were opposed to supervision of financial sanctions being included or thought another agency should be responsible for supervision (such as the Police, Ministry of Foreign Affairs and Trade, or a dedicated agency established for this purpose).

408. As we recommend amending the Act to include the purpose of supporting the implementation of financial sanctions (*see Recommendation R4*), we also recommend that the existing AML/CFT supervisors should be responsible for supervising financial sanctions. As submitters noted, the AML/CFT supervisors already have relationships with the businesses in question, and it is more efficient to leverage these relationships than establish a new agency and duplicate supervisory relationships. This change would also improve New Zealand's compliance with the FATF Standards and address a recommended action in New Zealand's Mutual Evaluation. However, we anticipate that additional baseline funding may be required for supervisors to carry out this role, which should be factored into any attempt to increase the resources of the regime (*see* Ensuring there are sufficient resources to deliver the regime).

Recommendation

R31. Include supervision of implementation of financial sanctions within the scope of the existing AML/CFT supervisor responsibilities (noting that additional funding would be sought to support this function).

Inspecting businesses that operate from home

409. Currently the Act prohibits onsite inspections of dwellinghouses. There are a small number of businesses operating from the owner's home, including in high-risk sectors, that cannot currently be subject to onsite inspection. We considered whether the AML/CFT supervisors should have the power to conduct onsite inspections of businesses operating from dwelling houses, and if so, what controls should be implemented to protect occupant's rights.

410. Overall, submitters largely supported allowing onsite inspections of businesses that operate from a person's home. Some submitters considered there would need to be

restrictions and some were not in support of allowing such inspections. Accordingly, we recommend amending the Act to allow supervisors to conduct onsite inspections of a business that operates from a person's home. This amendment will help ensure consistency of the application of the Act and that businesses operating from residential addresses are not advantaged. We recommend restricting these inspection powers to the part of the house used to provide the captured activity and, as with onsite inspection at places of businesses, inspections should be constrained to "any reasonable time".

Recommendation

R32. Amend the Act to state that an onsite inspection may be conducted at the part of a dwellinghouse (i.e., home office space) that is used to provide a captured activity.

Remote inspections

411. While supervisors have all the powers necessary to undertake their functions under the Act, there are no explicit provisions allowing remote monitoring or inspections (e.g., video conferencing). This is problematic in relation to online businesses that have no physical office, and the COVID-19 pandemic also highlighted the need to be able to conduct business or inspections remotely and the benefits of this approach. As such, we considered whether remote inspections would be useful for the regime.

412. Overall, submitters supported allowing inspections to be carried out virtually and considered this would provide efficiencies for both supervisors and businesses. Some submitters were concerned about how this would work in practice, raising administrative, technology and privacy challenges. Other submitters noted that a remote inspection may not provide the AML/CFT supervisor with a full picture of how the business operates.

413. We consider that remote inspections would be useful for the regime. However, we agree they would not substitute the need for an onsite inspection in some circumstances. We recommend amending the Act to explicitly allow supervisors to use virtual tools when it is appropriate to do so, and subject to relevant technical and data security considerations. This should include a requirement to caution the reporting entity's employees, officers, and agents consistent with onsite inspection requirements.

Recommendation

R33. Amend section 132 of the Act to explicitly allow supervisors to utilise virtual tools, such as video conferencing technology, when appropriate and subject to technical and data security considerations, as part of their supervision and monitoring a reporting entity's compliance with the Act. Employees, officers, or agents should be advised of the right not to answer a question if the answer would or could incriminate them (to align with the onsite inspection requirement of section 133(3)).

3.4.2. Financial intelligence

Allowing information to be requested from other businesses

414. Section 143(1)(a) of the Act currently enables the FIU to order production of additional information from reporting entities where it is relevant to analysing data and information they have already received. However, this does not extend to businesses who are not reporting entities. For example, airlines or travel agents may have information relevant to understanding potential terrorism financing threats. Providing the FIU with powers to request information from non-reporting entities would enable them to capture the data they need to understand the full picture and obtain relevant material in time sensitive situations, such as risks to national security.

415. We identified two options that could be progressed to enable the FIU to obtain information from non-reporting entities in a timely fashion, that are not mutually exclusive:

- **amend section 143 of the Act:** this option would introduce a new power enabling the FIU to require non-reporting entities to provide relevant information. This could be limited to a certain set of circumstances such as where the information is high risk and/or time sensitive.
- **issue guidance:** this option involves providing non-reporting entities with guidance on how to identify high-risk individuals and suspicious activity and how and when to report it. There would not be any requirement for a non-reporting entity to comply with a requires, but the guidance could offer advice on reporting suspicious activity to improve the quality of information.

416. Most submitters supported extending the current FIU powers to require information from non-reporting entities. Submitters considered the extension of powers to include non-reporting entities a powerful tool to combat money laundering and terrorism financing, and that it would support the FIU to prevent illicit activity from occurring. However, most submitters agreed that any power should be constrained so it is only exercised, when necessary, to balance competing interests, such as the *Privacy Act 2020*. However, some submitters were opposed to the introduction of a new power, indicating it would be an unjustified, overreach of power, given existing FIU powers.

417. We agree that a FIU power to request information from non-reporting entities would be beneficial in supporting the prevention of criminal activity. We also generally agree that powers should be constrained to certain circumstances to balance other concerns, such as privacy. Accordingly, we recommend amending the Act to provide this power subject to appropriate constraints, such as specifying who the power could apply to and how it could be exercised to balance competing interests. Further work should also include research around whether there are similar powers exercised in overseas jurisdictions. Additional powers would best support preventing financial crime as the power to obtain additional information would enhance and improve analysis of financial intelligence.

Recommendation

R34. Subject to further exploration of how such a power could be exercised appropriately, amend the Act to provide a power that enables the FIU to request information from non-reporting entities and requires them to supply the information.

Providing for ongoing monitoring of transactions and accounts

418. The FIU and investigators are able to obtain details of financial activities using powers in section 143 of the Act and *Search and Surveillance Act 2012,* but only a transaction or activity has occurred. However, the retrospective nature of the powers and the delay between identification of suspicious activity and making a request risks illicit funds being shifted to avoid detection of criminal activity or law enforcement action. Additionally, when investigating certain types of offending such as illegal drug trading or online exploitation, time can be critical to disrupt the activity or prevent harm.

419. We considered whether the FIU should have the power to order information on an ongoing basis could mitigate the risk associated with time delays. This would provide the FIU and law enforcement agencies with timely access to information on high-risk individuals to disrupt illicit activity. We identified several options for how this could be achieved, all of which involve amending section 143 of the Act to expand the FIU's powers and enhance financial monitoring functions:

- **allow direct access to information from reporting entities**, such as access to accounts related to persons of interest. This would greatly reduce the time taken to respond to illicit activity but raises significant privacy and human rights concerns.

Details around the workability of this option and how it could be implemented are still to be considered.

- **require reporting entities to provide ongoing information (at the request of FIU):** amend the Act to enable the FIU to request ongoing information be provided to them in certain intervals (e.g., daily, weekly, monthly) regarding persons of interest. This option may be more resource intensive for businesses but would support analysis of financial intelligence for high-risk individuals and allow the FIU to access real-time information. This could be in line with the UK model of account monitoring orders which provides a similar function. The privacy and human rights impacts would still be significant, but less than allowing direct access to reporting entity information.

- **mirror an extended Production Order:** this option would amend the Act to create a provision that mirrors Production Orders as set out in section 74 of the *Search and Surveillance Act 2012.* A Production Order requires that a person or organisation (such as a business) produce documents to enforcement agencies as evidential material of a specified offence. However, a new provision would differ by providing that the Order could be in force for a period longer than 30 days from the date the Order is made.

420. Submitters were mixed on whether proactive FIU powers should be extended. Most submitters supported the proposal, acknowledging that it could result in further investigations into complex and high-risk activity. Those opposed were primarily concerned with compliance costs and noted that businesses are already responsible for conducting ongoing monitoring of customer accounts and transactions meaning it may result in overlapping efforts. Submitters generally considered any power, should it be introduced, should be limited to only the circumstances of highest risk (e.g., terrorism financing and child exploitation) as well as require sufficient authorisation such as a warrant.

421. We agree that FIU powers should be extended as it would support the Act's purpose of detecting and deterring money laundering and prevent harm. We also agree that there should be appropriate constraints on any powers introduced to balance other competing interests such as privacy and human rights concerns. We recommend agencies explore what, and how, appropriate safeguards would need to be applied to provide FIU with ongoing monitoring powers. This could include consideration of time limits, limitations on the circumstances in which the power could be exercised, and a suitable authorisation process. In particular, we recommend further engagement with Privacy Commissioner to consider in detail the privacy implications of introducing a new power, and whether safeguards would provide an adequate balance to justify extended powers.

Recommendations

R35. Explore, in consultation with the Privacy Commissioner, what appropriate safeguards might need to be applied should the FIU be provided with the power to request ongoing information relevant to high-risk individuals.

R36. Subject to appropriate safeguards being available, amend the Act to allow the FIU with appropriate powers to request ongoing information.

Freezing or stopping transactions to prevent harm

422. Identifying and preventing criminals from using illegal funds to further illicit activity is crucial to preventing harm. However, there is currently a risk that illicit money can be transferred before law enforcement can respond to suspicious activity. We identified that an FIU power to freeze accounts and transactions, where there is suspicious activity, would enable enforcement agencies to act quickly to stop the transfer of funds before further harm can occur. This would help deprive funds used for harmful illicit activities such as child sexual exploitation, human trafficking, and national security matters such as terrorism offences.

423. The current powers available to respond to suspicious activity and prevent transfer of illicit funds are limited. The FIU can advise banks to freeze accounts and transactions pursuant to the standard terms and conditions and the Code of Banking Practice. The Asset Recovery Unit (ARU) can also direct reporting entities to freeze accounts in certain circumstances, such as when it is suspected funds have been obtained through proceeds of crime. However, ARU must obtain a court order to either freeze or seize an account or transaction, which can often take weeks, even when urgent, meaning funds can be transferred before the Order is obtained.

424. There were several options considered around powers to freeze assets, that are not mutually exclusive:

- **introduce constrained freeze powers:** this option would allow the FIU to freeze accounts/block transactions to act more promptly where there is suspicious activity. However, this would be limited to certain high-risk situations (e.g., suspected terrorism financing) and be constrained to freezing or stopping transactions for a specified time period.
- **introduce broad freeze powers:** this option would allow the FIU to freeze accounts/block transactions with a broader application than the above option and would be inclusive of all concerning situations (such as scams and other fraud).
- **provide guidance and support:** this approach would provide further support and training to reporting entities around reporting suspicious activity. This could potentially improve the quality and timeliness of reporting.

425. Most submitters agreed the FIU should have powers to freeze or block transactions, while some considering there should be appropriate constraints to ensure powers only be used in limited circumstances of particularly high risk. Others noted that there should be careful consideration of how freeze powers are managed as banks are already proactive in identifying and acting on potential fraud. Others noted they did not think the power should be applied in instances of scams and other frauds for similar reasons. Further, submitters noted the need for a clear framework for managing and communicating any freezes of customer accounts or transactions so that risks of 'tipping off' can be mitigated.

426. We broadly agree with the majority of submitters and recommend that agencies further explore a power for the FIU to freeze accounts or block transactions for the purpose of investigating whether there is criminal activity occurring. Providing a freeze power to the FIU would allow them respond to time-sensitive and high-risk situations, such as freezing funds so they cannot be used to further terrorist activity.

427. We agree that there should be further exploration of the appropriate constraints applied to any potential freeze power. This includes, but is not limited to, an appropriate time period for freezing, privacy concerns, human rights, consumer rights and what the freeze powers should cover (e.g., limited to highest risk or include frauds and scams). We recommend amending the Act to create a power to freeze or block transactions, subject to there being sufficient privacy and human rights protections identified and developed and a full assessment of the costs and benefits of the proposal. In line with our recommendation regarding a power for ongoing monitoring of accounts, we recommend further engagement with the Privacy Commissioner on this potential power.

Recommendations

R37. Explore, in consultation with the Privacy Commissioner, what appropriate safeguards might need to be applied should the FIU be provided with the power to freeze accounts and/or block transactions for the purposes of determining whether criminal activity is occurring.

R38. Subject to appropriate safeguards being available, amend the Act to provide the FIU with the appropriate powers to freeze accounts and/or block transactions in appropriate circumstances.

3.5. Secondary legislation making powers

428. The Act allows for a wide range of secondary legislation to be issued, including regulations (generally issued under section 153 and 154), Ministerial exemptions (section 157), and codes of practice (section 64). These powers are intended to allow the regime to be flexible and responsive and allow for changes to be made without amending the Act.

3.5.1. Secondary legislation making powers generally

429. The existing powers to issue regulations, exemptions, and Codes reflect the current institutional arrangements of the regime. In particular, the involvement of multiple agencies in conducting AML/CFT supervision and regulation has resulted in the current formulation of secondary legislation making powers and has limited other powers from being used. For example, it would be unnecessarily complicated with the current arrangements to delegate decisions relating to exemptions to the AML/CFT supervisors and would risk inconsistent decisions being made (*see* Supervisory structure).

430. Submitters generally supported the need for secondary legislation to provide further clarity and guidance for the system and considered the existing powers to be appropriate. Several submitters noted that the powers are not used as expediently or as efficiently as they potentially could be, with others suggesting that secondary legislation needs to be reviewed more frequently.

431. In line with submitter feedback and our recommendations regarding the institutional arrangements of the Act, we recommend adjusting the secondary legislation making powers to ensure that secondary legislation can be efficiently issued and administered. The extent to which this can be done will depend largely on whether there is any consolidation or simplification of the agencies involved in the regime, as some changes (e.g., rules or simplifying exemptions) would be viable only if there was a central administration body or single supervisor established. However, even if no changes are made to the institutional framework of the regime, we consider that existing powers need to be amended so that they are clear and can be used efficiently (*see* Challenges with existing powers).

Recommendation

R39. Adjust secondary legislation making powers to ensure that secondary legislation can be efficiently issued and administered. This adjustment should reflect any changes to the institutional arrangements of the regime and could result in new types of secondary legislation being issued (e.g., AML/CFT rules) or agencies being given new powers to make or amend secondary legislation.

3.5.2. Challenges with existing powers

432. We identified several changes that should be made to the existing secondary legislation making powers in the Act, specifically the ability to specify forms and reports, make and amend codes of practice, and for exemptions to be issued by the Minister of Justice. We consider that these changes should be made irrespective of the outcome of our overall recommendation to adjust secondary legislation making powers.

Forms and reports prescribed by the Act under section 153

433. The format of annual reports, formal warnings, and various other reports (e.g., suspicious activity reports) are prescribed in regulations. Prescribing forms via regulations limits the ability for agencies to quickly change the format of any reports

as all changes need to go through Cabinet and be provided to the Governor-General to be issued.

434. Most submitters thought it was appropriate for operational decision makers, such as Chief Executives, to be responsible for issuing or changing forms and annual reports. Submitters agreed that this change could make the regime more effective and responsive, provided sufficient consultation occurs and enough time for implementation. Submitters also noted the need for consistent approaches to be taken across forms and ensuring that agencies consider the compliance impact before making or amending a relevant form.

435. We recommend amending the Act to delegate the ability to make or amend the various forms to the appropriate operational decision makers within the regime. For example, the power regarding forms for SARs and PTRs could be delegated to the Commissioner of Police, while the power regarding forms for BCRs could be delegated to the Chief Executive of the New Zealand Customs Service. Alternatively, the ability could be delegated to a single decision maker, such as the Secretary of Justice or the NCC. We note that the powers will need to have the appropriate safeguards and oversight in place, which could include a requirement for consultation with industry before any changes are made.

Recommendation

R40. Amend the report and form making power in section 153(1)(b) to delegate the ability to make or amend forms to the appropriate operational decision makers with the appropriate safeguards and oversight.

Making or amending codes of practice under section 64

436. The Act allows for the Ministers responsible for the AML/CFT supervisors to issue a code of practice in respect of any compliance obligation. A code of practice sets out how a business can comply with specific obligations and provides a legislative 'safe harbour', in that businesses that meet a code's requirements are deemed to have complied with the relevant obligation. Businesses can choose to comply with the relevant obligation by another equally effective means and 'opt out' of a code by notifying their supervisor.

437. We considered whether codes of practice were a useful tool for businesses and whether the Act's current provisions and settings were appropriate. In practice, the process for issuing codes of practice is overly burdensome, and we also considered whether codes should be issued by operational decision makers such as the Chief Executives of the AML/CFT supervisors. We also considered if the Police should be able to issue codes, for example relating to SAR obligations.

438. Most submitters considered that opting out of a code was challenging due to current requirements to adopt equally effective means and to notify the AML/CFT supervisor, which ultimately stifles innovation. Other submitters noted a lack of clarity around how to demonstrate that alternative means are equally effective, and how to resolve a difference in opinion between an AML/CFT supervisor and a business. Most submitters supported the Police being able to issue codes of practice (in relation to reporting obligations), although a large minority were opposed.

439. Overall, we agree that codes of practice are of potential benefit to the AML/CFT regime given the current institutional framework. They are intended to offer assurance to businesses and set out a consistent standard to be met for the relevant obligation across the AML/CFT system. However, we also consider that improvements should be considered for the framework to ensure there is enough flexibility to allow for innovation and efficiency.

440. We therefore recommend amending the Act's framework for codes of practice to ensure the framework is useable, provides flexibility for meeting AML/CFT obligations, and mitigates risks. This change should also reflect any updates to the institutional

arrangements of the Act, which may mean that other types of secondary legislation, such as rules, could be issued that could fulfil the same function as codes.

Recommendation

R41. Noting the general recommendation regarding secondary legislation (*see* Recommendation R40), amend the Act's framework for codes of practice to ensure the framework is useable, provides enough flexibility and scope for innovation for businesses towards meeting AML/CFT obligations, while also providing assurance of minimum requirements and mitigating risks.

Applying for exemptions from the Act under section 157

441. Section 157 of the Act allows the Minister of Justice to wholly or partially exempt businesses or classes of businesses and transactions from AML/CFT obligations. The Minister must consider the factors in section 157(3), which include the intent and purpose of the Act, the risk associated with the business, and the level of regulatory burden, whether other reporting entities would be advantaged or disadvantaged, that would exist in the absence of an exemption.

442. The purpose of these provisions is to allow low-risk businesses to seek relief from various obligations and ensure that their regulatory burden is proportionate to risks to which they are exposed. New Zealand has granted approximately 120 individual exemptions, 33 exemptions for classes of businesses, transactions, or services, and issued regulations to declare 11 types of business not to be reporting entities for the purposes of the Act.

Stewardship of the Ministerial exemptions regime

443. Given that a number of exemptions have been issued since the regime came into force, we have taken the opportunity to consider the overall stewardship or governance of exemptions, including whether exemptions are still required for the regime to operate effectively and efficiently.

444. Most submitters were in favour of exemptions, noting that they ensure the regime operates effectively and flexible, but that several changes should be made to ensure the exemptions regime operates effectively. In line with substantial industry support for keeping exemptions, we recommend progressing recommendations in the following areas to enhance the stewardship of the exemptions regime:

- **reducing the volume of individual ministerial exemptions:** we could issue more regulatory and class exemptions, such as making amendments to the *AML/CFT (Definitions) Regulations 2011* to reduce the number of businesses that are unintentionally captured in the regime.
- **introducing some light-touch supervision of exempt entities:** e.g., by including conditions in exemption notices that allow for some oversight or retaining obligations such as annual reporting which could be tailored for exempt entities.
- **reviewing what obligations entities are exempted from:** for example, whether it is logical for businesses to have SARs obligations but be exempt from risk assessment obligations, given a risk assessment is usually required to determine whether something is suspicious.
- **reviewing the approach to expired exemptions:** this could include clarifying expectations for businesses when their exemption expires, i.e., that they are expected to comply with their obligations from the date of expiration.
- **providing avenues beyond judicial review** for applicants if the Minister decides not to grant an exemption, that could involve creating an ombudsman scheme (*see* Supervisory structure) or creating a process for the Ministry to formally review the decision.

445. We consider that progressing improvements to the stewardship of the exemptions regime, subject to further engagement with industry and agencies to ensure that exemptions are being used appropriately. In line with the high-level nature of the recommendation, further analysis and consultation will be needed to develop more detailed options for each of these areas. Further engagement with the private sector in April 2022 revealed broad support for the areas we identified for progressing changes. We note that other recommendations made as part of this review will impact on some of the areas we wish to explore. For example, changes to the scope of captured business will impact on the volume of exemptions, and similarly, the method for providing avenues beyond judicial review for applicants is tied to any changes progressed under the institutional arrangements section (*see* Institutional arrangements and stewardship).

Recommendation

R42. Subject to securing sufficient resourcing, progress options to enhance the stewardship of the Ministerial exemption regime (subject to further engagement), including identifying more regulatory and class exemptions, introducing some form of light-touch supervision of exempt entities, reviewing how obligations should be exempted and clarifying the approach to expired exemptions, and proving avenues beyond judicial review if an exemption application is declined.

Application process for Ministerial exemptions

446. Many submitters noted that the application process for exemption can be burdensome, costly, and confusing. Submitters also overwhelmingly commented on the long period of time that it takes for the process to be completed. We also note that reviewing and processing exemption applications can be difficult for agencies due to the lack of dedicated resources as well as applicants sometimes failing to provide all the necessary information.

447. We identified several ways where we could improve the application process to make it easier for businesses to apply while also improving the quality of information we receive:

- **publishing clear guidance to assist businesses** with the exemptions process, including the features of low-risk activities/entities to help businesses determine whether they may be eligible for an exemption, the information applicants need to provide for exemption applications, and an overview of the application process.
- **creating a standardised application process** and simplifying the reapplication process, which could include implementing an online portal which could also house relevant guidance. In addition, reapplications could focus on changes to the business and their activities rather than a fresh application.
- **set fixed timeframes by which exemptions must be processed** in legislation or on the Ministry's website to increase accountability for processing exemptions in a timely manner.
- **explore options for charging applicants a fee** which could go towards resourcing agencies to carry out exemptions but would need to be justified by a streamlined and timely process. We would also need to explore how to make this equitable for small businesses or non-profit organisations.

448. Most submitters thought the Act or guidance should specify what applicants need to provide as doing so would ensure clarity of process, improve accessibility and transparency, and promote consistency. Some disagreed that there should be further requirements prescribed in terms of what needs to be provided, with others also noting the need to retain flexibility in the process. Almost all submitters supported a simplified process when renewing an exemption, such as focusing on any changes since the original exemption, or on how the business has complied while subject to an

exemption. Submitters also noted that a standardised or online application process would assist. These views were reiterated when we conducted targeted engagement with the private sector in April 2022.

449. In line with feedback, we recommend progressing all the identified options to ensure a more streamlined and clear application process. We note that further analysis and consultation will be needed to further develop the changes and ensure they will be effective. We also note that the option to charge applicants a fee would follow on a longer timeframe and be dependent on sufficient improvements being made which justify the fee being charged. We would also need to conduct a significant amount of consultation and analysis to ensure any system would be implemented fairly. It is also important to note that if the recommendation to increase resourcing of the AML/CFT regime is progressed, we may not need to introduce a fee (*see* Ensuring there are sufficient resources to deliver the regime).

Recommendations

R43. Progress options to streamline and provide clarity to the application process for Ministerial exemptions including publishing clear guidance, creating a standard application process, simplifying the reapplication process, and setting fixed timeframes for processing exemptions.

R44. If it is required to ensure there are sufficient resources to process applications for exemptions, amend the Act to charge applicants a fee subject to further engagement and sufficient operational improvements being made.

How decisions are made to grant or decline a Ministerial exemption application

450. The Minister must consider the factors in section 157(3) when deciding whether to grant an exemption. These factors include the intent and purpose of the Act, the risk associated with the business, and the level of regulatory burden, whether other reporting entities would be advantaged or disadvantaged, that would exist in the absence of an exemption.

451. As part of New Zealand's Mutual Evaluation, the FATF found that it is not clear that all the exemptions granted were in cases where low money laundering and terrorism financing risks were proven. In addition, we note that it is unclear what 'risk' needs to be low, e.g., inherent versus residual risks, and the risk of the business versus the risk of the exemption. Further, the Act does not make it clear that the other factors (e.g., the business' compliance burden, whether there are any competitive advantages or disadvantages if an exemption was or was not granted) are only considered once low money laundering and terrorism financing risks are not themselves grounds for an exemption.

452. Most submitters thought the decision-making factors set out in section 157(3) are largely still appropriate (noting that there may nonetheless be changes if the purpose of the Act is changed – *see* Purpose of the Act). However, submitters agreed that the factors could be further clarified or updated, including how the criteria should be applied by the Minister. Further, most submitters thought exemptions should only be granted in instances of proven or assessed low risk. Some noted the Act or guidance should clearly articulate what would be considered low risk, with most favouring assessing the risk of the business rather than the risk of the exemption, or a combination of the two.

453. In response to the issues identified, we recommend amending the factors in section 157(3) to ensure they are clear and given the appropriate weight as part of decision making. This would include specifying what risk is assessed i.e., the business' risk or the risk associated with the exemption and clarifying that only low-risk entities can be granted exemptions. We consider this change could lead to more robust decision-making in line with FATF Standards, while also providing greater transparency to applicants regarding the decision-making process. Note that we generally recommend adjusting secondary legislation making powers to ensure that secondary legislation can be efficiently issued and administered (*see* Secondary legislation making powers generally). With respect to exemptions, this could result in making an operational

decision-maker responsible for making decisions, such as the Secretary of Justice, if this would lead to more efficient decision making.

Recommendation

R45. Review factors in section 157(3) to ensure they are clear and given the appropriate weight as part of making a decision. This would include specifying what risk is assessed i.e., the business' risk or the risk associated with the exemption and clarifying that only low-risk entities can be granted exemptions.

3.6. Information sharing

3.6.1. Direct data access to FIU information for other agencies

454. The FIU maintains a wealth of information that may be relevant to other agencies, including the AML/CFT supervisors, Customs, and other agencies not directly part of the AML/CFT regime (e.g., Ministry for Social Development, Inland Revenue). However, the FIU is currently only able to share information with other government agencies on a case-by-case basis. This is administratively burdensome for the FIU and means that the regime is unable to realise the full value of the information that the FIU holds to support better regulation, supervision, and law enforcement outcomes.

455. Section 139A of the Act allows for regulations to be issued that enable information sharing, which includes enabling direct data access arrangements. A direct data access arrangement would enhance the overall effectiveness of the regime and how the FIU operates. There are three options for how the change can be progressed:

- **introduce a narrow direct data access arrangement**, which would only encompass the AML/CFT supervisors and Customs. Other government agencies would not be included in the arrangement even where they may have a genuine need to access FIU information. This option would be the least resource intensive to implement as a result of there being fewer agencies involved, but the FIU would have to continue to service requests for information from other agencies on a manual basis.

- **introduce a broad direct data access arrangement,** which encompasses all agencies that have historically accessed FIU information or would have a need to access the information in the future. This would be the most resource intensive to implement and ensure that all agencies have appropriate and proportionate access to FIU information but would also mean that the FIU would only be required to manually service requests for information in limited circumstances.

- **combination of the two (i.e., narrow initially but expand overtime)**, which would begin with the AML/CFT supervisors under the Act and Customs and then potentially expand to any relevant government agency who can demonstrate a need for FIU data, in congruence with the purposes of information sharing as noted in section 139. Unlike the first option, this option allows other government agencies to establish direct data arrangements with the FIU, after a direct data arrangement has become embedded for the AML/CFT supervisors and Customs.

456. Most submitters were supportive of the proposals for direct data access for other agencies, but this was contingent upon the access and use of the information being tightly constrained and there being sufficient privacy and cyber-security protections. Many submitters also noted that the proposals would enable greater regime responsiveness and efficacy, but also highlighted the need for strong checks, balances, and oversight. Some submitters were not supportive of the proposals largely because of concerns around privacy and confidentiality.

457. We generally agree with the feedback provided by submitters, particularly around access being tightly constrained and only provided to those relevant government agencies who can demonstrate a need for FIU data. In particular, we recommend

taking a combined or staggered approach creating direct data access arrangements and begin with RBNZ, FMA, DIA and Customs. These agencies all have roles, responsibilities, and powers under the Act and currently request FIU data through current provisions. Once initial direct data access arrangement is embedded, we recommend considering extending the arrangement to other regulatory, intelligence, and law enforcement agencies who can demonstrate their need for FIU information.

458. We consider this approach strikes the appropriate balance between effectiveness and privacy concerns and would help realise the full value of FIU information for regulatory and law enforcement purposes.

Recommendations

R46. Issue regulations to support a direct data access arrangement for RBNZ, FMA, DIA and Customs, following consultation with the Privacy Commissioner.

R47. Once direct data access is embedded, consider extending the arrangement to other regulatory, intelligence, and law enforcement agencies who are able to demonstrate their need to access the information.

3.6.2. Minor changes to information sharing

459. We recommend making the following minor changes to information sharing provisions in the Act:

Issue	Recommendation
Several key acts are currently not included under section 140 of the Act, such as *Agricultural Compounds and Veterinary Medicines Act 1997, Animal Products Act 1999, Animal Welfare Act 1999, Biosecurity Act 1993, Child Support Act 1991, Commerce Act 1986*, *Corrections Act 2004*, *Defence Act 1990*, *Environment Act 1986*, *Fisheries Act 1996, Food Act 2014, Forests Act 1949, Gaming Duties Act 1971, Immigration Act 2009*, *Policing Act 2008, Student Loans Scheme Act 2011, Trusts Act 2019* and *Wine Act 2003*. The key agencies responsible for the listed legislation have observed money laundering and other harms but are currently unable to share information with the AML/CFT agencies.	Issue regulations to include additional acts within scope of section 140 to enable broader information sharing between key agencies that are well placed to observe money laundering and other harms.
There are two Acts (the *Non-Bank Deposit Takers Act 2013* and the *Insurance* (*Prudential Supervision*) *Act 2010)* which are not included in section 48(b) of the Act to enable the disclosure of personal information to another government agency relating to employees or senior managers for law enforcement purposes.	Add the following Acts to Section 48(b) of the Act: *Non-Bank Deposit Takers Act 2013*, and the *Insurance (Prudential Supervision Act 2010)*.
There are limited provisions explicitly allowing the DIA to share information internally for law enforcement purposes.	Amend the Act to clarify that the DIA is able to share information internally for law enforcement purposes on the same basis it is able to share information with other government agencies.
There is no explicit provision in the Act that allows supervisors to conduct enquiries on behalf of foreign counterparts. Section 132(2)(e) of the Act provides a general power to initiate and act on requests from overseas counterparts, but not specifically conduct enquiries.	Clarify in the Act that supervisors are empowered to conduct enquiries on behalf of overseas counterparts (i.e., to provide a general power to conduct enquiries).

Issue	Recommendation
The reasons for agencies to engage in data sharing are limited by Section 139 of the Act that notes information can only be shared in pursuance of 'law enforcement purposes.' The lack of clarity for the definition of 'law enforcement purposes' is opaque and means that reasons for sharing information is obfuscated.	Clarify that law enforcement purposes includes the investigation of any offence (per section 243(1) *Crimes Act 1961*) and repeal sub paras 5(a)(i), (ii), and (iv) of the Act to ensure that information can be shared to and from all other LEAs, such as the Commerce Commission.
The NZSIS and GCSB cannot current submit SARs under Section 39A of the Act, instead, submission of SARs by these agencies needs to be done under the *Crimes Act 1961*. There is a need for these agencies to be able to directly submit SARs to Police for reasons of efficiency.	Add a sub paragraph to Section 39A of the Act that reads "the enforcement of Parts 1 to 7 of the Intelligence and Security Act 2017."

3.7. Mitigating unintended consequences

460. While the AML/CFT regime aims to prevent harm, misapplying AML/CFT measures can have serious negative and unintended consequences which should be avoided or mitigated. These include making it harder for legitimate non-profit organisations to operate, closing accounts of risky customers or businesses, and excluding people from the formal financial system. This issue is not unique to New Zealand: internationally, the FATF has recognised a number of areas where implementing AML/CFT requirements has inadvertently caused issues and is working to resolve those challenges.

3.7.1. De-risking

461. One area where the AML/CFT regime has had unintended consequences with respect to making it harder for certain types of businesses, particularly money remittance and fintech businesses, is to open or maintain a bank account. Known as 'de-banking' or 'de-risking', this can result from other businesses preferring to avoid, rather than manage, the risk of having the risky business as a customer. De-risking ultimately hurts communities in New Zealand and overseas and increases overall risks. As such, we have considered whether the Act could do more to reduce the prevalence or likelihood of de-risking and thereby ensure legitimate businesses can operate.

462. We have identified three broad options that could be progressed regarding de-risking, including suggestions made by submitters:

- **make it harder, but not impossible, for businesses to de-risk customers**: the Act could require businesses to consider the impact that terminating the relationship would have on the customer's financial inclusion or demonstrate that terminating a relationship would not unreasonably impact the customer's financial inclusion. Alternatively, we could prohibit businesses from exiting customers if doing so would result in financial *ex*clusion or introduce a requirement for businesses to demonstrate that they have exhausted alternative risk management approaches before de-risking a customer.

- **provide for a dispute resolution mechanism in the Act,** which would empower customers to apply for a resolution if they feel they have been unreasonably exited or denied access to financial services. This mechanism would require an agency (or agencies) to be given the mandate to investigate and resolve complaints and potentially mediate a resolution or direct that a customer is onboarded.

- **provide regulatory assurance to businesses with risky types of customers**, such as remitters or VASPs. This could be achieved by issuing a code of practice that outlines

the steps the business needs to take to manage the risks of the customer but provide a regulatory safe harbour should the customer be involved in illicit activity.

463. Submitters agreed that de-risking is an area of concern and heavily impacts some sectors, such as remitters, and that this is driving people into riskier and ultimately more expensive situations to remit funds. Submitters identified that addressing the issues with de-risking could be achieved by the regime being more outcomes-focused to avoid legitimate business being lost or by making it harder (but not impossible) for businesses to deny basic banking services. Alternatively, submitters thought the central bank could offer exchange settlement accounts and allow entities who have been de-risked to still hold a bank account or provide some form of safe harbour to industry to ensure businesses do not de-risk entire industries.

464. We conducted further engagement on this topic and the options identified as part of targeted engagement workshops in April. Attendees were generally opposed to any option that would make it harder to exit or not onboard a customer, with some noting that this approach would conflict with general principles of competition law. Attendees generally preferred an approach of providing regulatory assurance to businesses, with others noting that this would be consistent with recommendations regarding licensing high-risk businesses (*see* AML/CFT licensing for some reporting entities).

465. In line with industry views, we recommend requesting that the AML/CFT supervisors create a code of practice for banks to rely on when onboarding high-risk customers, including remitters and fintech providers. Based on feedback we have received from the banking sector, we consider that this change would help reduce risk-averse behaviour and help banks more favourably view onboarding certain types of customers, such as remitters. In turn, this would help ensure that innovation within the financial sector is not stifled as a result of businesses not being able access banking services.

Recommendation

R48. Request that the AML/CFT supervisors develop a code of practice for businesses (particularly banks) to rely on when onboarding high-risk businesses and customers, including remitters.

3.7.2. Financial exclusion

466. Financial inclusion or exclusion refers to how well various groups of society, including low income, rural and undocumented persons, can access or be provided with an adequate range of safe, convenient, and affordable financial services (e.g., bank accounts). We recognise that the regime has negatively impacted financial inclusion for some people, either because they are viewed as being risky or because they lack the necessary documentation to prove their identity or address. This is particularly an issue for people without secure access to housing, as they are currently required to provide proof of address (*see* Verifying address information).

467. We consider that financial inclusion will be substantially improved as a result of our recommendations regarding certain CDD settings. In particular, we consider that relaxing requirements around address verification and requirements to treat trusts as high risk will improve financial inclusion, as will our recommendation to overhaul the Identity Verification Code of Practice (IVCOP) (*see* Identity Verification Code of Practice). However, there are two options that could be progressed in addition to broader changes to CDD settings, specifically:

- **issuing exemptions to relax CDD requirements in specific low-risk scenarios**, such as where customers lack appropriate identification documents due to being disabled, a new migrant, recently released from prison, or fleeing a domestic violence situation.

- **amending IVCOP** to expand the types of documents considered sufficient for low-risk circumstances and/or adjusting exception handling procedures. This could include expanding the types of documents that could be used as well as other parts of the Code, such as trusted referees

468. Submitters generally considered that the regime is too blunt and generic in its focus, particularly with some identity requirements that can be challenging for some demographics. Submitters suggested using exemptions to provide for *de minimis* levels below which CDD is not required, recognising alternative options for verifying a person's identity, and providing a centralised or more streamlined CDD process.

469. In line with submitter feedback, we recommend exploring further regulatory exemptions to address financial inclusion challenges in specific low-risk situations, particularly if the broader changes to CDD settings do not sufficiently improve financial inclusion. While IVCOP already has exception handling procedures to address instances of financial inclusion, feedback from industry indicates that these measures are not sufficient. Accordingly, we consider that regulatory exemptions should be explored to address specific challenges and ensure that CDD obligations are appropriately tailored.

Recommendation

R49. Explore whether there are any further regulatory exemptions needed to address financial inclusion challenges in the event that broader changes to CDD requirements still result in instances of financial inclusion.

CHAPTER 5

Scope of the Act

Summary

470. This chapter considers and makes various recommendations as to whether the Act is capturing the right activities and businesses to mitigate New Zealand's risks of money laundering and terrorism financing. It also considers whether the definitions and terminology for existing activities or services are fit-for-purpose, especially given technological advancements.

471. We have identified a number of ways the Act could be strengthened to combat areas of high risk. In particular, we are concerned that illicit capital is still able to enter the real estate market despite the inclusion of law firms, conveyancers, and real estate agents in the regime between 2018 and 2019. Similarly, we consider that the Act could (and should) do more to combat trade-based money laundering through potentially increasing obligations for some businesses and/or enhancing information sharing between agencies. However, we recommend conducting a thorough risk assessment to identify the particular ways in which real estate and the trade system are or could be exploited to ensure that any changes are appropriately risk-based. We also recommend a number of changes to clarify and strengthen obligations for virtual asset service providers and high-value dealers to order to protect against the use of virtual assets or high-value goods for money laundering and terrorism financing.

472. In terms of current terminology, we make a large number of recommendations to improve the clarity of the various capture points in the Act, particularly for designated non-financial businesses and professions (DNFBPs). We further recommend clarifying how the Act applies to stored value instruments, businesses which provide multiple activities, and the scope of "in the ordinary course of business". We also consider that there should be greater alignment between the definition of 'financial institution' in the Act and the definition of 'financial services' in the *Financial Service Providers (Registration and Dispute Resolution) Act 2008*, which could involve amendments to either or both Acts.

473. We generally do not recommend that any additional activities should be captured by the Act as did not consider there to be sufficient risks of money laundering or terrorism financing that would justify the changes. Specifically, we do not recommend capturing businesses which act as a secretary of a company or partner in a partnership, criminal defence lawyers, non-life insurance businesses, or non-profit organisations which are moderately vulnerable to terrorism financing. The one exception is with respect to businesses which could provide financial intelligence by virtue of the services they provide, such as fintech providers offering open banking solutions or marketplace operators. For these businesses, we recommend further exploring whether these businesses should be reporting entities, and if so, how obligations could be appropriately tailored.

474. We also make a number of recommendations to issue new exemptions for various low-risk sectors or products, in line with our general recommendations regarding taking a more risk-based approach. For example, we recommend issuing new exemptions for certain businesses which act as a trustee or nominee, provide low value loans, and various Crown-owned or controlled entities which provide certain captured activities using public funds. We also recommend reviewing and/or clarifying the scope of some existing exemptions, such as for internet auctioneers, special remittance card facilities and non-finance businesses which transfer money or value.

475. Finally, amending the Act to define its territorial scope to ensure that offshore businesses which provide captured activities to or in New Zealand have the same

obligations as businesses based in New Zealand. We consider that this approach will ensure an even playing field and that New Zealand businesses are not unfairly disadvantaged by being in New Zealand and having AML/CFT obligations. However, we do not have a firm recommendation for how the territorial scope should be defined and recommend that further analysis is conducted to identify the best approach that could be taken. In the interim, we recommend reviewing and updating the existing territorial scope guidance to ensure it is sufficiently clear, appropriate, and consistent with the approach taken in related regulatory regimes.

4.1. Improving the Act's ability to combat high-risk areas

4.1.1. Ensuring illicit capital cannot enter the real estate market

476. Real estate continues to be the asset of choice for money laundering. Despite the inclusion of law firms, conveyancers, and real estate agents in the regime between 2018 and 2019, the Police have continued to recover a large amount of real estate tainted by proceeds of crime. For example, in the financial year ending June 2021, 100 properties totalling NZD 73.7 million were seized by the Police, which was an increase from the previous year where 51 properties totalling NZD 55.7 million were seized. This suggests that large sums of illicit capital may still be able to enter the market, and also may be contributing to inflating property prices in New Zealand.

477. We are concerned that the current settings regarding real estate are not as effective as they could be at detecting or deterring illicit capital from entering the real estate market. As such, we considered how the system could be strengthened to better combat this significant threat. For example, in some circumstances real estate agents may have an opportunity to detect or deter proceeds of crime being used to purchase property, whereas other businesses concurrently involved (e.g., the bank or conveyancer) in the transaction may not have sufficient visibility to detect suspicious activity and vice versa. Consequently, one option may be to increase information sharing between the various businesses involved in a transaction to ensure they are all informed if one of the businesses detects something suspicious.

478. In addition, real estate agents are only required to conduct CDD on their client (usually the vendor), and on the purchaser in limited circumstances (e.g., if the purchaser pays the deposit in cash or by cheque). The current settings do not comply with the FATF Standards, which require AML/CFT obligations to be applied to both vendor and purchaser. This gap could be a vulnerability which is being exploited by criminals to launder money. There are several options that could be progressed to address this vulnerability, such as requiring agents to conduct CDD on both the vendor and purchaser in every instance, switching obligations from the vendor to the purchaser, or expanding the range of circumstances where a vendor's agent must conduct CDD on the purchaser to address specific money laundering typologies.

479. Many submitters were opposed to expanding AML/CFT obligations to both parties and increasing requirements relating to purchasers. Some noted this could cause disproportionate compliance costs and can result in a waste of resources and effort, delay transactions, and have an adverse impact on the ease of doing business. Others noted challenges in situations where there might be multiple offers, auctions, or tenders and because the real estate agent does not usually act for the purchaser. Others considered a better opportunity to detect money laundering was after the real estate agent had completed their part of the sale and purchase process. Private sales were also identified to be of significant risk and outside the purview of real estate agents. These views were reiterated during private sector engagement we conducted in April 2022.

480. Given the systemic nature of this threat and the potential for significant compliance costs and practical challenges, we recommend conducting further analysis to identify the specific methods that criminals are using to get illicit capital into the real estate market. Following this, agencies should consider what changes need to be made to the AML/CFT regime to combat those methods or typologies effectively and efficiently. This could include imposing additional requirements for real estate agents

or on other businesses involved in relation to particular areas of concern, e.g., private sales, on-selling, and the use of nominees. However, we note that combatting these risks could also involve operational changes (such as changing the standard form for Agreements for Sale and Purchase) and/or improving the sharing of information between businesses involved to ensure a coordinated response.

Recommendations

R50. Agencies, particularly FIU and DIA, undertake further analysis to assess the money laundering and terrorism financing risks in the real estate sector to identify the particular methods or typologies that are being used to place, layer, or integrate the proceeds of crime through real estate and which sectors or businesses would have visibility of or exposure to those typologies.

R51. Following the risk assessment, consider whether any further AML/CFT controls to prevent/deter this from happening. This could include additional obligations for real estate agents and law firms (e.g., by imposing additional requirements for private sales, on selling, list and sell, measures where nominees are used for purchases, risks associated with non-finance or privately funded purchases and increasing cooperation between the parties involved).

4.1.2. Combatting trade-based money laundering

481. Trade-based money laundering (TBML) is the process of disguising the proceeds of crime and moving value using trade transactions. TBML exploits the international trade system for the purpose of transferring value and obscuring the true origins of illicit wealth. TBML schemes vary in complexity but typically involve misrepresentation of the price, quantity, or quality of imports or exports.

482. It is difficult to estimate the extent to which TBML occurs globally, let alone domestically, in part due to a lack of awareness about TBML and the lack of coherent and reliable statistics or intelligence being gathered about TBML. However, the Asia Pacific Group on Money Laundering noted in their 2012 TBML typology report that TBML is a problem for many of the countries in the Asia-Pacific region and has serious significance as an avenue to launder proceeds of crime. This is reinforced by the NRA, which identifies trade-based activities as a key facilitator for transnational money laundering and a high priority vulnerability that needs to be addressed. As such, we have considered whether any changes to obligations for businesses should be made or whether there are further steps that could be taken to enhance information sharing to improve the identification of TBML.

Obligations for businesses to combat TBML

483. Businesses involved in trade finance may be in a position to identify TBML and provide actionable intelligence to law enforcement agencies. Parties involved in trade finance include banks, trade finance companies, importers and exporters, insurers, export credit agencies, trade brokers, as well as accountants and other DNFBPs. However, only some of these businesses (such as banks or accountants) have AML/CFT obligations related to the trade system, such as providing letters of credit or preparing processing and paying invoices (*see* "Engaging in or giving instructions").

484. We considered the extent to which we should clarify that preparing or processing invoices is captured by the Act, as well as whether preparing annual accounts and tax statements should be a captured activity. Most submitters stated the Act is not sufficiently clear regarding the extent to which the preparation and processing invoices is covered by the Act. Submitters agreed the Act should be clarified and also that obligations should align with the risks involved.[35] Most submitters also did not consider that preparing annual accounts or tax statements should become a captured

[35] We separately recommend clarifying whether this activity is captured – see *"Engaging in or giving instructions"*

activity due to the potential for disproportionate compliance costs for potentially limited benefits.

485. Given the range of businesses who are potentially exposed to TBML and the inherent complexity, we recommend conducting a risk assessment and detailed analysis of the trade finance system. This analysis should examine the trade finance system to identify the extent of TBML that may be occurring as well as businesses which are vulnerable to being exploited before any new businesses are included in the regime. This assessment should also confirm whether any additional sectors or activities should be included within the AML/CFT regime. This could include only limited obligations, depending on the associated costs and benefits w. In particular, agencies should consider whether importers and exporters or trade brokers should have obligations, especially given their exposure to domestic and international sanctions (*see* Supporting the implementation of financial sanctions obligations).

Recommendation

R52. Agencies, particularly FIU and Customs, conduct a risk assessment and general analysis of the trade finance system to identify the extent of TBML that may be occurring in New Zealand as well the businesses that are involved in activities that are at risk of being misused for TBML. This analysis should then be used to inform future advice regarding the costs and benefits of including any new sectors or activities within the AML/CFT regime.

Enhancing intelligence collection and sharing for TBML, including data-matching

486. The FIU collects a large amount of information from businesses (*see* Financial intelligence), and this information could be used to combat other offending more effectively if matched with data that other government agencies hold. For example, PTRs could be matched with trade data held by Customs to identify suspicious cross-border trade transactions that may indicate TBML. However, PTRs are not required for every type of trade finance transaction (e.g., letters of credit between banks), and the information collected through PTRs may not easily match up with other data held by Customs.

487. Most submitters were supportive of data matching arrangements being developed, noting that data matching would improve efficiencies within and across the regime, improve the ability of agencies to detect offending, and enable a cross-agency and whole-of-government approach to combatting financial crime. Only a few submitters were opposed to or concerned about the data matching, largely due to the potential privacy impacts. In line with our recommendation to consider additional obligations for businesses regarding TBML, we recommend agencies also identify what intelligence could or should be collected so that TBML can be more easily identified. In particular, Customs and the FIU should identify whether data-matching would improve transparency of the trade and trade finance system and enhance detection of TBML.

Recommendation

R53. As part of the analysis of the trade finance system, agencies should also identify what intelligence should or could be collected to enhance detection of TBML, as well as whether any FIU data should be matched with trade data to enhance transparency of the trade and trade finance system.

4.1.3. Protecting against the use of virtual assets for illicit purposes

488. Recent years have seen an increase in new and innovative technologies that can be used to swiftly transfer value around the world. Blockchain and distributed ledger technologies have the potential to radically change the financial landscape. However, their perceived anonymity, speed, and global reach also attracts those who want to escape scrutiny for both legitimate and illegitimate reasons. Businesses which provide services in respect of virtual assets (e.g., Bitcoin, Ethereum) have been identified

internationally as being vulnerable to significant money laundering and terrorism financing risks.

489. To combat this growing concern, the FATF issued binding standards in 2019 to require countries to take action to understand, identify, and address the risks that virtual asset service providers pose in their country. This includes applying AML/CFT obligations to businesses which provide one of the five types of virtual asset activities identified by the FATF, as well as adjusting existing obligations regarding occasional transactions and wire transfers to reflect the risks associated with virtual assets.

Providing a clear definition of a Virtual Asset Service Provider (VASP)

490. Currently the Act's definition of financial institution is sufficiently broad to cover four of the five types of VASPs required by the FATF. However, the Act does not cover VASPs which only provide safekeeping and/or administration of virtual assets but do not facilitate exchanges or transfers. Further, businesses and the general public may not be aware that VASPs have AML/CFT obligations due to the lack of an explicit legislative or regulatory reference to the sector.

491. There are several options for creating a definition of VASPs to provide clarity to the public and improve compliance with the FATF Standards, including:

- **incorporating the FATF's definition into law with any necessary changes:** this would ensure compliance with the FATF's standards and could include the opportunity to tailor the definition for the New Zealand context.
- **adopt the definition used in Australia regarding digital currency exchanges:** this would ensure a consistent trans-Tasman approach, but the Australian definition does not appear to cover all types of VASP the FATF expects to be captured by AML/CFT regimes.

492. Submitters were generally supportive of creating a definition for VASPs in the regime through issuing regulations and/or amending the Act. Submitters noted an overall preference for a specific definition for VASPs due to the uniqueness of the sector and to give more established financial institutions, such as banks, greater confidence in the VASP sector. Submitters were broadly comfortable with adopting a FATF definition, however noted that they would like the New Zealand context to be considered to ensure that the implementation of this definition worked for New Zealand businesses. The VASP industry also made suggestions that the FATF definition could be tweaked where necessary to fit into the Act.

493. We recommend issuing regulations defining VASPs as a type of reporting entity, in line with the definition provided by the FATF. Given the risks associated with the sector, we consider that this change should be progressed as soon as possible through issuing regulations. This definition should then be included in the Act as part of future amendments.

494. A specific definition for VASPs will ensure these businesses are clearly captured by the regime and achieve compliance with the FATF's requirements. We also consider that using the FATF definition would create the most certainty for VASPs operating internationally, given that all countries are expected to comply with the FATF's definition. However, we note that further work would be required to determine what is considered a virtual asset and how obligations would apply, particularly given recent developments in the virtual asset ecosystem, such as non-fungible tokens, decentralised autonomous organisations, and decentralised finance. We also consider that some adjustments to the FATF's definition may be required to ensure it is appropriate for the New Zealand context.

Recommendation

R54. Include virtual asset service providers as a type of reporting entity, in line with the definition provided by the FATF. This should be achieved initially through issuing regulations, and then the definition should be included in the Act itself.

Ensuring occasional virtual asset transactions are captured appropriately

495. There are currently no specific provisions for occasional transactions involving virtual assets, although some relevant transactions are captured through existing provisions in the Act. The existing thresholds apply to cash to virtual asset transactions, and vice versa, of NZD 10,000. However, this is does not comply with the FATF Standards, which require all virtual asset occasional transaction thresholds to be set at USD/EUR 1,000 due to the inherent risks associated with virtual assets. This approach also does not include virtual asset to virtual asset transactions.

496. Regulations could be issued to prescribe a specific occasional transaction threshold for virtual asset transactions, which could either be set at NZD 1,000 or NZD 1,500. An NZD 1,000 threshold would reflect the risks associated with the sector and would be consistent with the current threshold regarding wire transfers and currency exchange, while an NZD 1,500 threshold would align with the USD 1,000 threshold set in the FATF Standards.

497. Submitters agreed that an occasional transaction threshold should be introduced for VASPs, with some noting that they were currently conducting customer due diligence regardless of threshold. Submitters were split between NZD 1,000 and NZD 1,500 with some preferring the threshold aligning with other thresholds in New Zealand, while others preferred having a threshold which was equivalent to international virtual asset thresholds.

498. We recommend setting the threshold at NZD 1,000 at the time of transaction. We consider that this will allow for the greatest level of financial intelligence in the virtual asset industry, reflect the risks associated with the sector, and align with other AML/CFT thresholds. Based on industry feedback, we do not anticipate that this would result in disproportionate compliance costs, as VASPs which engaged with the review indicating that they are already viewing all customers as having a business relationship and conducting CDD irrespective of the transaction amount.

Recommendation

R55. Issue regulations to declare all virtual asset transactions at or above NZD 1,000 at the time of the transaction as occasional transactions, including virtual asset to virtual asset transfers.

Implementing the FATF's travel rule to improve transparency and traceability

499. The existing wire transfer requirements for VASPs do not apply to transactions made solely in virtual assets, which is required by the FATF Standards. In addition, the FATF expects that all virtual asset transfers are treated as cross-border wire transfers and require the VASP conducting the transaction to ensure that information about the parties to the transaction 'travels' with the transaction to the recipient VASP. Known as the "travel rule", this requirement helps ensure that all VASPs have full visibility about the underlying parties to the transaction irrespective of the type of virtual asset being transacted.

500. There are two options for implementing the travel rule in New Zealand:

- **create bespoke VASP specific wire transfer obligations:** this would require amending the Act to include new provisions separate from the existing wire transfer obligations but would help ensure obligations are appropriately tailored. However, this approach would take time as it would require legislative change to be progressed, meaning that risks associated with VASPs would take longer to be

mitigated. There is also the risk that New Zealand VASPs would be cut off from the international market due to not implementing the travel rule.

- **extend existing wire transfer obligations to VASPs:** the Act already provides obligations to ensure traceability and transparency of international funds transfers (*see* Wire transfers). These could be extended to include virtual asset transactions through issuing regulations to declare these transfers as wire transfers. However, we recognise that there are many issues with the existing wire transfer provisions, which would be compounded for VASPs if obligations cannot appropriately be tailored.

501. International wire transfers were the most widely commented on topic relating to virtual assets during public consultation. Submitters were wary about being too prescriptive, noting that some VASPS can differentiate between domestic and international wire transfers using technology like blockchain analysis. However, the industry generally supported introducing something similar to the FATF travel rule. The industry noted that they are often already required to comply with corresponding obligations in offshore jurisdictions and would support the New Zealand government helping them adhere to travel rule obligations.

502. We recommend issuing regulations to include virtual asset transfers within the existing wire transfer obligations. Given the risks associated with virtual assets, we consider that amending the Act would leave the vulnerability unaddressed for too long. While we note that there are several issues with the existing wire transfer obligations, these broadly relate to the definition of a wire transfer and would not undermine the effectiveness of this option (*see* Wire transfers), as a bespoke virtual asset definition could be developed.

503. To ensure VASPs have appropriate and proportionate compliance costs, we further recommend that the regulations should specify that all virtual asset transfers should be considered international wire transfers unless VASPs are satisfied that they do not involve international parties. This would mean that domestic virtual asset transactions would not be required to comply with the travel rule. We also recommend specifying bespoke identity and verification requirements for VASPs to ensure obligations align with the underlying technology.

Recommendation

R56. Issue regulations that require all virtual asset transfers to be considered international wire transfers *unless the entity is satisfied otherwise*, with bespoke identity obligations which reflect the nature of the underlying technology. These changes should be supported with guidance from the AML/CFT supervisors.

4.1.4. Making high-value goods less attractive for money laundering

504. Businesses which trade in high-value goods for cash were brought into the Act in 2019 to make it harder for criminals to move or use cash anonymously through high-value goods. Buying and selling high-value articles in cash is attractive for criminals because these transactions can be less visible to the government and other financial institutions, can be easily hidden, and can be transferred to third parties with limited documentation. However, we have identified challenges with the current settings for these businesses, known as high-value dealers (HVDs) that make it difficult to supervise the sector and obtain necessary financial intelligence, and which undermine the effectiveness of efforts make high-value goods less attractive for money laundering.

Definition of "high-value dealer"

505. A business only becomes an HVD if, in the ordinary course of business, it buys or sells the specified high value articles by way of singular or multiple cash transactions which equal or exceed the prescribed transaction threshold (currently NZD 10,000). We

have identified several issues with this definition that has made it difficult for DIA to supervise the sector and created uncertainty for businesses.

List of high-value articles

506. The list of articles in the definition of a HVD reflects the types of goods identified as posing a risk, including those commonly seized by Police. However, we note that by prescribing the specific articles, the Act may fail to address new or evolving risks if, for example, a new type of article is used for money laundering. Further, during the targeted engagement workshops in April 2022, attendees noted that the list makes arbitrary distinctions between goods which can create confusion for businesses.

507. We have identified two options that we could progress to address these issues:

- **review and amend the list of high value articles:** this could include determining whether any articles should be added or expanding the definition to provide greater clarity and better reflect risk.
- **remove the list from the definition entirely:** the effect of this would be that the buying or selling any article would become captured if it was over the relevant cash transaction.

508. As this issue was only raised in the latter phase of consultation, we recommend conducting further analysis to determine whether the list of articles should be expanded or removed. That said, our initial view is that any article bought or sold over the relevant cash transaction is vulnerable to money laundering and consideration should be given to removing the list. This would align with the approach taken in jurisdictions such as the United Kingdom, that do not distinguish between types of high value article and apply obligations to any business engaging in cash transactions over a threshold. As part of the further analysis, we would need to carefully consider whether removing the list of articles would create unintended consequences, including if there are any businesses that would inadvertently now be captured by the Act that should not be.

Recommendation

R57. Review the list of articles in the definition of an HVD to consider whether it should be removed or amended in order to be further strengthened or clarified.

Use of "in the ordinary course of business" and appropriate capture point

509. Currently, a business that only engages in a relevant cash transaction occasionally does not meet the definition of HVD under the Act. This creates ambiguity for businesses dealing in the specified articles regarding whether they have obligations under the Act or not. Relevant cash transactions are likely to be unusual at most for many dealers in these articles, and this also means that some cash transactions over the NZD 10,000 threshold are not currently subject to AML/CFT obligations. This poses a money laundering risk to our AML/CFT framework.

510. We identified various options we could progress to address these issues:

- **remove the phrase "in the ordinary course of business"**: this would mean a business would be captured under the Act if it ever transacts in relevant cash transactions (rather than if it only does so in the ordinary course of business). This would provide clarity to businesses around the point of capture and ensure that all relevant cash transactions involving specified high value articles are subject to AML/CFT obligations.
- **provide further guidance regarding "in the ordinary course of business":** for example, we could specify how many relevant transactions a business needs to make before it is considered "in the ordinary course of business". We note this would need

to align with DNFBPs (*see* "In the ordinary course of business"). This would provide clarity regarding the point at which AML/CFT obligations were applicable, but not result in AML/CFT obligations being applied to every relevant cash transaction.

- **declare all businesses dealers in specified high-value articles as reporting entities:** This would potentially capture thousands of businesses dealing in the specified high value articles as reporting entities, although many of them may never engage in relevant cash transactions. If AML/CFT obligations only applied to relevant cash transactions the compliance burden of this option would be minimised.

511. Most submitters supported amending the definition of HVD to include all businesses dealing in high value articles. Submitters considered this would provide clarity and better address the money laundering risks. However, submitters also identified the additional compliance costs that would accompany this, as well as increased costs for the supervisor. Submitters also noted that businesses are able to avoid obligations by not engaging in relevant cash transactions. This feedback was reiterated during private sector engagement in April 2022.

512. Overall, we do not consider it necessary to declare all businesses that deal in the specified high value articles as HVDs under the Act. We consider that this would create significant compliance burden for thousands of businesses that may never engage in the relevant cash transactions, or in cash at all. Instead, we recommend amending the Act to remove the phrase "in the ordinary course of business" from the definition of HVD. This will reduce ambiguity, address the risks associated with gaps in AML/CFT coverage and enable more effective supervision of the HVD sectors.[36] This would also provide businesses with a choice, to accept relevant cash transactions and be a HVD under the Act, or not to and avoid being subject to the Act. To mitigate the risks associated with the current gap for the meantime, we also recommend that further guidance is issued to provide a more definitive interpretation of the phrase "in the ordinary course of business".

513. We note that a challenge to this approach is that it could result in a sudden and challenging compliance burden for businesses once the transaction occurs. However, we consider the recommendation for reporting entity registration would mitigate this issue (*see* Registration for all reporting entities). If the recommendation regarding registration was progressed, we would look to set the requirement for HVDs so that they would need to be registered before they could lawfully make a relevant cash transaction. This would provide their supervisor with the necessary oversight to ensure that businesses are prepared for their compliance obligations prior to being brought into the Act.

Recommendation

R58. Amend the Act to remove the phrase "in the ordinary course of business" from the definition of a high-value dealer. This will set the capture point as an HVD as any business that transacts in cash over the relevant threshold. In the interim, AML/CFT supervisors should produce guidance which provides a clearer interpretation of "in the ordinary course of business".

Capturing non-cash transactions

514. While the risks associated with the HVD sectors is understood to predominantly relate to cash transactions, there is a risk that increasing cash transaction controls will increase risks associated with non-cash transactions. As such, we considered whether the Act needs to be amended to future proof against this potential change in behaviour by criminals.

[36] Note that HVDs are a sector not currently subject to registration with their AML/CFT supervisor. We recommend creating a registration framework that applies to the HVD sector that will further enable more effective supervision of HVDs.

515. At this time, we do not have enough evidence to support any obligations being imposed for non-cash transactions. We also acknowledge that this type of change would need to be justified considering the accompanying compliance burden. However, we are aware of growing risks of money laundering through third parties that use their bank account to purchase goods and are then repaid in cash. We expect these kinds of risks will increase as it becomes harder to launder money through cash. As a result, we recommend agencies review the risks associated with non-cash transactions for the specified high value articles. If warranted, AML/CFT obligations should be applied to non-cash transactions for certain high-value articles, with an appropriate threshold for obligations set (which could be higher than the cash transaction threshold).

Recommendation

R59. Conduct a risk assessment to understand the potential money laundering risks of non-cash transactions for high-value articles and explore whether applying some form of obligations to such transactions is necessary and, if so, the amount at which the threshold should be set.

Exclusion for industrial dealers in precious metals and stones

516. The FATF Standards require countries to include industrial dealers in precious metals and stones within their AML/CFT frameworks. However, the Act currently excludes the mining of precious metals and precious stones, manufacturing of jewellery and crafting or polishing precious stones, or the buying or selling or precious metals and precious stones for industrial purposes. Removing this exclusion could enable better intelligence gathering and improve the detection of money laundering, as well as being more compliant with FATF Standards.

517. We recommend removing the exclusion for industrial dealers in precious metals and stones. We have not been able to determine why industrial dealers were excluded from the scope of HVD, and we consider that any transaction that would otherwise be captured under the Act carries risk of money laundering and terrorism financing and should have obligations attached to it. We anticipate that only a small number of industrial transactions would be made in cash over the relevant threshold. In addition, any business that would be impacted can choose to stop accepting cash and thereby avoid AML/CFT obligations entirely.

Recommendation

R60. Amend the Act to remove the exclusion for industrial dealers in precious metals and stones.

Exemption for pawnbrokers

518. Pawnbrokers are fully exempt from the Act, even though they may engage in relevant cash transactions for the same high-value goods that HVDs engage in. Pawnbrokers may therefore have exposure to money laundering and terrorism financing risks, as well as having a small commercial advantage over HVDs. Including pawnbrokers in the Act would ensure that all businesses that trade high-value articles for cash are appropriately mitigating their money laundering and terrorism financing risks.

519. We identified two options for bringing pawnbrokers into the Act:

- **remove the exemption entirely:** this would mean pawnbrokers are subject to obligations as a HVD for buying, selling or pawnbroking activity involving relevant cash transactions for the high value articles. However, there is the potential that revoking the exemption entirely would mean that some pawnbroking activity is captured as providing loans. In turn, pawnbrokers would be subject to full AML/CFT obligations as financial institutions under the Act.

- **only capture pawnbrokers that engage in HVD-like activity:** this would have the same effect as the first option but provide certainty that a pawnbroker is not captured under the Act for transactions that are not included in the definition of a HVD (i.e., pawnbroking activity involving cash transactions under the relevant threshold, or not involving cash).

520. Most submitters were supportive of removing the exclusion to ensure a consistent approach for relevant cash transactions involving high-value articles. Submitters were also supportive of aligning requirements between the Act and *Secondhand Dealers and Pawnbrokers Act 2004* where relevant. One submitter noted that adhering to a higher standard where requirements are duplicated (such as record keeping) is unlikely to materially increase compliance costs and will ensure there are no unintended coverage gaps in the overall regime. These views were reiterated when we conducted further engagement on this topic in April 2022, including with the relevant peak body for pawnbrokers.

521. We recommend amending the exemption so that pawnbroker activities are captured by the Act if they meet the definition of an HVD. This change would be in line with the money laundering vulnerabilities associated with the use of cash for buying, selling or pawnbroking activity involving high-value goods. It would also increase New Zealand's compliance with FATF Standards. However, we consider that regulations should make it clear that pawning activity is not captured as providing a loan. We consider this recommendation is in line with the risk-based approach and would uphold financial inclusion considering that pawning can provide an immediate source of income for people in vulnerable circumstances.

522. We do not consider that including pawnbrokers as HVDs under the Act would create a significant compliance burden. As noted, pawnbrokers are already subject to the *Secondhand Dealers and Pawnbrokers Act 2004 which* includes similar identification and record keeping obligations. Further, we were informed by the pawnbroker industry that transactions commonly occur well below currently prescribed threshold of NZD 10,000, and as such very few pawnbrokers are likely to meet the HVD definition. We have considered the changes to the pawnbroker exemption in light of the broader recommendations for HVDs, and feedback from the pawnbroking industry indicated these changes would be workable.

Recommendation

R61. Amend the exemption to no longer apply to pawnbroker activities that meet the definition of HVDs and clarify that pawning is not captured under the Act as providing a loan.

Appropriate cash transaction threshold

523. We considered whether the currently prescribed NZD 10,000 transaction threshold should be lowered to better mitigate money laundering risks associated with the sector. Further, if the prescribed transaction threshold was also lowered, this change would support greater intelligence and law enforcement outcomes, particularly where transactions are being structured below NZD 10,000 (*see* Applicable threshold for reporting prescribed transactions). Lowering the threshold would also mean that more transactions attract AML/CFT obligations. However, based on data from 2018, we anticipate that a lower threshold would result in the following transaction volumes:

Table 20 - approximate volume of high-value transactions captured (2018)

Threshold	NZD 1,000	NZD 3,000	NZD 5,000	NZD 10,000
Volume of transactions captured	90 percent	85 percent	79 percent	61 percent

524. Most submitters were not supportive of lowering the threshold, noting that this would increase compliance costs for HVDs and would be inconsistent with how other businesses are treated. Submitters also noted that banks may have some visibility of repeat transactions, and that no threshold amount will achieve perfect visibility of the transactions. Submitters also considered that removing the word "ordinary" will better address the gap better compared to a lower threshold (*see* Recommendation R58).

525. As part of further engagement in April 2022 attendees reiterated concerns about this change, and also noted that lowering the threshold would create a large compliance burden on top of the other proposed changes to the HVD settings. However, some submitters supported lowering the threshold to improve visibility and mitigation of risks and suggested that it be set between NZD 1,000 to NZD 5,000.

526. We initially supported the option of lowering the threshold to NZD 5,000 due to 2018 data from FIU showing that approximately 39 percent of high-value articles seized as proceeds of crime have a value less than NZD 10,000. However, after further engagement with the private sector we agreed that this change may not be necessary on top of other proposed changes to the HVD settings which are also intended to increase the scope of transactions captured and enable better detection and deterrence of money laundering. As such, we recommend retaining the current threshold and re-evaluating whether it should be lowered once we have had time to assess the effectiveness of the other changes to the HVD settings. As part of this later review, we would consult fresh data on criminal asset recovery to help determine the appropriate threshold.

Recommendation

R62. Retain the current NZD 10,000 threshold for high-value dealers but revaluate whether the threshold should be lowered once other recommended changes to high-value dealer obligations have been implemented.

High value dealer obligations

527. HVDs are currently subject to fewer obligations than other types of business. For example, they are not required undertake risk assessments or implement an AML/CFT programme, nor are they under a mandatory obligation to submit SARs. This was largely because many HVDs are small businesses that at the time had little experience with regulatory regimes and had a low capacity to implement full AML/CFT obligations. However, the problem with this approach is that without these obligations, HVDs may not fully understand their money laundering and terrorism financing risks and may not be reporting suspicious activities, which ultimately undermines detection and deterrence of money laundering.

528. We identified the following options for increasing obligations for HVDs:

- **full obligations:** HVDs would be required to comply with the Act with the same obligations that all other businesses have, e.g., risk assessment, compliance programme, enhanced customer due diligence, and mandatory SARs. This would mitigate risks to the greatest extent but would also have the most significant increase in costs. However, we also note that the reported costs that HVDs incurred for the financial year ending 31 March 2022 exceeded those for DNFBPs (*see* Private sector costs of the regime).

- **full obligations for types of HVDs that are identified as higher risk:** this would be a similar approach to the full obligation but would be limited to the subset of HVDs which are identified as being high risk. This may lower compliance cost for the sector overall but would also risk displacing risk within the sector.

- **increased (but not full) obligations:** some obligations could be tailored for the HVD sector as they may be difficult for HVDs to comply with or are only partially relevant to their risks e.g., modified risk assessment, enhanced customer due-diligence and ongoing transactions monitoring. This would potentially reduce additional compliance costs while also increase risk mitigation across the sector.

- **add mandatory SARs to existing obligations:** this would potentially increase the detection of money laundering, but the effectiveness of this change may be undermined or limited by the lack of a requirement for the business to assess and understand their risks.

529. Most submitters thought HVDs should have increased or full obligations to improve intelligence collection and better address the risks in the sector. Some submitters specifically noted that HVDs should have a mandatory SAR obligation. However, a minority were opposed to increasing obligations for HVDs due to the increase in costs and complexity for the businesses.

530. We consider that HVDs should have increased obligations as the current settings are not sufficiently effective. At minimum, we consider that HVDs should have a mandatory obligation to submit SARs. The number of SARs received from the HVD sector is not consistent with their money laundering risks and may be a result of HVDs only having an optional, rather than a mandatory, obligation to submit a SAR. We also think that further obligations would be beneficial but also consider that obligations should be modified or simplified to reflect the relatively homogenous nature of the HVD sector. For example, the requirement to create a risk assessment could be simplified to reflect the homogenous cash transaction risks and ongoing transaction monitoring could be modified to focus only on detecting structuring.

Recommendation

R63. Amend the Act to increase obligations for HVDs. At minimum, HVDs should have a mandatory SARs obligation, and other obligations should be imposed if they are necessary to combat risks. However, any additional obligations should be tailored, if possible, to reflect the nature of the sector.

4.2. Challenges with existing terminology

4.2.1. "In the ordinary course of business"

531. A business must provide captured activities "in the ordinary course of business" for the business to be captured as a reporting entity under the Act. This phrase brings challenges, particularly for the DNFBP sectors where some activities may, by definition, only be provided on occasion (and alongside a much wider array of non-captured services). As such, some businesses are technically not required to conduct CDD in some high-risk scenarios because the activity is not considered 'ordinary'.

532. We considered whether we should prescribe when something is in the "ordinary course of business", or whether there were other options to provide clarity to DNFBPs. Relatedly, we noted that the FATF Standards require DNFBPs to comply with AML/CFT obligations whenever they undertake a captured activity. We therefore also considered the option of removing the word "ordinary" entirely, which would fully comply with the FATF Standards.

533. Many submitters advised there should be flexibility in the Act to allow infrequent activities without disproportionate compliance costs. Consequently, most submitters

were against removing the word 'ordinary', instead favouring prescribing a meaning to the phrase, although others considered this to be contrary to a risk-based approach. Conversely some submitters considered the word 'ordinary' should be removed from the phrase. This would provide clarity to DNFBPs and better address the risk associated with one-off activities.

534. We agree that capturing a business as a reporting entity if they only undertake an activity infrequently imposes considerable compliance burden. This is particularly so for those businesses that undertake no other captured activities and are not otherwise subject to the Act. That said, we note this leaves a gap in our AML/CFT regime that could be exploited by criminals. We therefore recommend that agencies conduct further analysis to understand the risks and determine the appropriate point at which requirements under the Act should apply.

Recommendation

R64. Review the intended meaning of "in the ordinary course of business" in section 5 with a view to amending or defining the phrase. Analysis should be undertaken to understand the risks associated with obligations that only apply if an activity is conducted in the ordinary course of business. Depending on this analysis, amendments to the Act should be made to provide clarity to DNFBPs around their obligations if they only undertake certain activities infrequently.

4.2.2. Businesses providing multiple types of activities

535. Section 6(4) states that the Act applies to a financial institution only to the extent it carries out financial institution activities, and to a DNFBP only to the extent it carries out DNFBP activities. This means that if a financial institution (e.g., a bank) carries out a DNFBP activity (e.g., sets up a company), it is not required to comply with the Act in respect of the latter activity. As such, some activities are not subject to AML/CFT requirements when provided by some businesses, which provides a competitive advantage as well as creates a vulnerability if those businesses are not applying AML/CFT controls, such as CDD.

536. We considered whether this gap should be closed so that a business is required to comply with AML/CFT requirements in respect of captured activities, irrespective on what type of reporting entity it is. Most submitters supported this change, noting it would remove competitive advantage and ensure risks are consistently addressed. Accordingly, we recommend amending the Act to ensure that captured activities are subject to AML/CFT requirements, regardless of the type of reporting entity that provides the service. This will ensure that all services have AML/CFT controls applied to them irrespective of the type of business involved. Given the competitive advantage and vulnerability that this gap provides, we further recommend issuing regulations to resolve this issue in the short term.

Recommendation

R65. Amend the Act to remove the term "only to the extent that" from section 6(4). In the meantime, issue regulations to clarify that a reporting entity that undertakes captured activities other than relating to its category of reporting entity must comply with the Act.

4.2.3. "Managing client funds"

Overlap between "managing client funds" and financial institution activities

537. The DNFBP activity of "managing client funds, accounts, securities, or other assets" overlaps with various financial institution activities. Some businesses are therefore

technically captured as both a financial institution and DNFBP under the Act.[37] This primarily results from the definition of trust and company service provider (TCSP), which includes "managing client funds", and means that any business is captured for that activity even if they are already a financial institution under the Act. This can result in confusion for businesses and duplication (e.g., a requirement to submit two annual reports, one as a financial institution and one as a DNFBP).

538. We considered whether this overlap should be removed so that a business can only be captured as one type of reporting entity. Most submitters agreed that the overlap should be removed, while some submitters raised broader issues around the appropriateness of the definition. We recommend issuing regulations to exclude a business from capture as a TCSP under the Act for managing client funds if they are already captured as a financial institution. In the long term, we recommend amending the Act to provide certainty, potentially by removing "managing client funds" from the scope of the definition of a TCSP.

Recommendation

R66. Issue regulations to exclude from the definition of TCSP, any person, whose only activity is a DNFBP activity (iv) if that person is already captured by the Act as a financial institution. This should then be changed in the Act itself.

"Sums paid as fees for professional services"

539. The definition of "managing client funds" currently excludes "sums paid as fees for professional services". It is not clear whether this only excludes the DNFBP's own professional fees, or whether it could be interpreted to mean any professional fees (e.g., fees held for any other party). We considered whether the meaning of professional fees should be clarified and what the appropriate definition would be. We note the DIA (as the AML/CFT supervisor of DNFBPs) holds the view that it only excludes the DNFBP's own professional fees.

540. Most submitters supported clarification of what is meant by "professional fees" and the inclusion of third-party fees within the scope of professional fees. Other submitters disagreed, and, noting risks with third party payments, considered that the DIA's interpretation is appropriate and should be clarified.

541. Overall, we are concerned that extending the scope of the exclusion to include the professional fees of any third party would pose considerable risks. We also note that we introduced regulations in 2021 that exempt funds that are professional fees for a third party in various low-risk circumstances.[38] As such, we recommend issuing regulations to clarify "sums paid as fees for professional services" means the DNFBP's own professional fees. This approach will clarify the scope of the term and ensure that risks associated with payments of sums to third parties are appropriately mitigated.

Recommendation

R67. Issue regulations to explicitly limit the exclusion "of sums paid as fees for professional services" in the definition of managing client funds as being the DNFBP's own professional fees. This should then be changed in the Act itself.

[37] This is because the definition of TCSP captures any person "managing client funds…" that is not a law firm, conveyancer, accounting practice, or real estate agent.

[38] This includes barrister fees and other professional fees paid to a third party in New Zealand relating to business carried out in New Zealand, in circumstances where those funds do not relate to a service captured by the Act (*Regulation 24AB AML/CFT (Exemptions) Regulations 2011*).

4.2.4. "Engaging in or giving instructions"

542. Businesses become captured as DNFBPs where they are "engaging in or giving instructions on behalf of a customer to another person." This applies to various activities, including conveyancing or real estate transactions, transfers of beneficial interest in property or transactions relating to creating, managing, or operating legal persons or arrangements. However, the current drafting is unclear, and leads to uncertainty and inconsistent approaches being taken by businesses.

543. This activity is intended to require AML/CFT obligations to be applied in certain situations when a DNFBP assists its client (in the absence of direct involvement in managing the client's funds or assets, acting as a nominee or trustee, or undertaking real estate agency work). The FATF Standards require a DNFBP to comply with AML/CFT obligations when they 'prepare for' various activities and transactions for their clients. However, the current drafting is not totally aligned with the FATF Standards, and we therefore considered whether it should be changed.

544. Most submitters agreed that the phrase is unclear, with "engaging in" particularly challenging for determining when to apply the Act's requirements. Other submitters considered the scope of activities and transactions potentially too wide. That said, some submitters thought the existing wording and scope appropriate.

545. We recommend amending the Act to clarify the activity of "engaging in or giving instructions". Noting this DNFBP activity is intended to capture situations other than when there is direct involvement in managing client affairs, we also consider there may be an opportunity to narrow its scope. This will provide clarity to the DNFBP sectors, ensure that the DNFBP activity is only applied where there are risks and reduce compliance costs overall. In the interim, agencies should explore whether regulations should be issued to clarify that certain activities are captured within the scope of this activity, such as preparing and processing invoices or the scope of conveyancing (*see* Obligations for businesses to combat TBML).

Recommendations

R68. Amend the definition of DNFBP activity (a)(vi), including the phrase 'engaging in or giving instructions', to clarify those activities that are required to be subject to this DNFBP activity. Note that this DNFBP activity is intended to apply to circumstances where a DNFBP has no direct involvement in managing a customer's funds, acting as a nominee or trustee, or undertaking real estate agency work.

R69. In the interim, issue regulations to provide clarity around the scope of this activity, such as its application to processing and preparing invoices (other than when also managing client funds) or involvement in real estate transactions (other than when undertaking real estate agency work).

4.2.5. Definition of financial institution activities

546. The definition of financial institution activities in the Act is close to the definition of financial services in the *Financial Service Providers (Registration and Dispute Resolution) Act 2008* (FSP Act), but the two are not completely aligned. We considered whether there should be alignment and how this should be progressed. The latter Act deals with several aspects of financial institution regulation, including registration, but the difference in terminology can result in inconsistent outcomes between the two Acts.

547. Most submitters were in favour of greater alignment, with only a small number opposed. Submitters considered alignment would reduce ambiguity or confusion and ensure that the FSP register provides complete visibility of all financial institutions that are reporting entities. Some submitters noted that the definition in the FATF Standards should be used in both Acts. We agree that alignment between the two definitions would mitigate current gaps in the visibility of financial institutions that are reporting entities. We also note that this crosses over with options for registration of

reporting entities (*see* Supervision, regulation, and enforcement). We therefore recommend further work be conducted with MBIE to explore options for alignment between the two definitions, if possible, noting that alignment may be difficult to achieve given the FSP Act's links with other financial markets legislation.

Recommendation

R70. Coordinate with MBIE and determine whether the *Financial Service Providers (Registration and Dispute Resolution) Act 2008* and/or the Act can be amended to ensure the terminology used to define financial activities are completely aligned with the FATF Standards.

4.2.6. Stored value instruments

548. Stored value instruments are devices which carry a redeemable balance (e.g., gift cards, apps, electronic cards). The risk of stored value instruments, and new electronic variants, lies primarily in their ability to be reloaded with cash and repeatedly used. In some cases, these instruments can be pre-loaded with foreign currencies with minimal CDD conducted on the purchaser of the instrument. These instruments are often widely accepted forms of payment, such as online gift cards, and in some cases allow the owner to withdraw funds from the card directly.

549. The current definition of a 'stored value instrument' is intended to cover instruments such as vouchers and gift cards, as well as similar value instruments like travel cards. However, the definition requires that the instrument be portable (implying tangibility), which excludes other purely digital or electronic types of stored value instruments that have since been developed. As such, we have considered whether the definition should be amended to capture all forms of stored value instruments, irrespective of whether they are tangible or purely digital.

550. Two options were considered to provide a solution to the broadening of stored value instruments:

- **issue guidance**, which could provide clarity and risk indicators to the industry regarding stored value instruments and encourage appropriate steps to be taken. However, issuing guidance may not be appropriate noting the level of risk associated with new forms of stored value instruments present, would need to align with the definition used in law, and could add confusion.

- **change the definition of stored value instruments** in Regulation 15 of the *AML/CFT (Definitions)* and *(Exemptions) Regulations 2011* to make the definitions technology neutral. This would reflect the risk of newer forms of stored value instruments, especially those used for scams and laundering purposes.

551. Submitters supported updating the definition of stored value instruments to reflect changes in technology and future proof against new and emerging technologies noting that it be technology neutral and should be discussed with industry to avoid any potential unintended consequences, especially on the Fintech sector. As such, we recommend amending the definition of stored value instruments to be technology neutral, and as such cover all potential instruments which are capable of storing monetary value in a form that is not physical currency.

Recommendation

R71. Amend the definition of stored value instruments in the *AML/CFT (Definitions) Regulations 2011* to be technology neutral to capture electronic or digital forms of stored value.

4.2.7. Minor changes to existing terminology in the Act

552. We recommend making the following minor changes to existing terminology:

Issue	Recommendation
Life insurer is not currently defined in the Act; however, the definition of life insurance policies is by cross reference to the *Insurance (Prudential Supervision) Act 2010*.	Define life insurer in the Act by reference to the *Insurance (Prudential Supervision) Act 2010*
The meaning of the exclusion of "cheque deposits" in the definition of occasional transaction in section 5 of the Act is unclear. It is intended to apply to a deposit by cheque made at a bank or non-bank deposit taker, such that it does not trigger an occasional transaction by the person making the deposit with the bank. However, this is not specified.	Limit the exclusion of cheque deposits only to deposits made at a bank, non-bank deposit taker, or similar institution in line with the original policy intent.
Legal arrangements are defined in section 5 as including a trust, a partnership a charitable entity, and any other prescribed arrangement (being an arrangement that involves a risk of money laundering or terrorism financing). No other legal arrangements have been prescribed, but some arrangements may pose risks, such as unincorporated societies or fiducie, truehand, fideicomiso or other foreign legal arrangements.	Issue regulations that prescribe the definition of legal arrangement to include unincorporated societies and any other types of legal arrangements.
Regulation 15 of the *AMLCFT (Definitions)* and *(Exemptions) Regulations 2011* apply to "single operations or operations that appear to be linked". However, the application of this phrase to the bulk-selling of stored value instruments to corporate/institutional customer is unclear where the instruments are intended for different recipient and are below the relevant thresholds.	Clarify the availability of Regulation 15 of the *AML/CFT* (*Definitions*) and (*Exemptions*) *Regulations 2011* to the bulk-selling of store to a corporate customer, in circumstances in which each SVI complies with the relevant threshold and is intended for a different recipient.

4.3. Potential new activities

4.3.1. Other businesses that could provide financial intelligence

553. There are an increasing number of third-party open banking platforms and providers offering services in New Zealand. Through application programming interfaces (APIs), the third-party provider can access a customer's bank account data and convey instructions to the bank to transact funds. In most circumstances these providers are not captured by the Act as financial institutions. This is because they only convey instructions to a bank to make a transfer, rather than having direct involvement in holding, transacting, or receiving funds for a customer. In addition, some commerce platforms or marketplace providers may, by virtue of the services they provide, be able to detect suspicious and fraudulent activity and potentially be exposed to domestic trade-based money laundering.

554. We consider that both open banking and commerce platforms are in a position to provide valuable financial intelligence which would assist in combatting illicit financial activity. Noting the rapid evolution of these platforms, we recommend conducting further analysis to determine whether there is benefit in including them as businesses with requirements under the Act, and if so, to what extent AML/CFT obligations should apply.

Recommendation

R72. Review whether there is benefit in including fintech providers offering open banking solutions and commerce or marketplace operators as reporting entities. This analysis should also include a comparison with other financial services related legislation to ensure consistency. Subject to the analysis, include them as a type of financial institution in the Act and implement appropriate AML/CFT obligations to align with their role in the financial system. This could be implemented by issuing regulations or by amending the Act.

4.3.2. Acting as a secretary of a company or partner in a partnership

555. People who act in a position of authority for a legal person can be exposed to money laundering or terrorism financing risks and used to obscure beneficial ownership. Currently, the Act captures natural or legal persons who act, or arrange for persons to act, as nominee directors or nominee shareholders or trustees in relation to legal persons or legal arrangements. This does not include persons acting as company secretaries, partners in partnerships, or similar positions in other legal persons. While this approach is not in line with the FATF Standards, we also recognise that company secretaries are not a position recognised in New Zealand company law.

556. We considered issuing regulations to include businesses and people who act as secretaries for companies, partners in partnerships, or equivalent positions for other legal persons and arrangements in the Act. This would bring the Act in line with the FATF Standards and address any accompanying money laundering risks. We do not consider there would be significant compliance costs imposed, as we anticipate that few, if any, businesses offered this service.

557. Most submitters were opposed to including acting as secretary within the regime, noting that capturing activities based on the title or description of a role is inconsistent with the activities-based nature of the regime. Others noted that a 'company secretary' is not a position which commonly exists in New Zealand and that the compliance costs may be unreasonably high if this change were implemented. While some supported including company secretaries, they nonetheless thought the activity should only attract obligations in high-risk circumstances. In line with industry feedback, we recommend maintaining the status quo for company secretaries. Although this would not address a small gap in terms of New Zealand's compliance with the FATF Standards, we consider this change would be more consistent with a risk-based approach .

Recommendation

R73. Maintain the status quo and do not include acting as company secretary within the scope of the Act.

4.3.3. Criminal defence lawyers

558. Lawyers who only provide criminal defence services have no obligations under the Act but may identify suspicious activities. For example, they may have a client who insists on paying legal fees in cash, which may indicate that criminal proceeds are being used to pay for their legal defence. However, criminal defence lawyers provide a vital service required for the justice system to function properly and a service to which everyone – including money launderers or terrorist financiers – is entitled.

559. We explored whether criminal defence lawyers should be included within the regime and have some AML/CFT obligations (e.g., to file SARs and report large cash transactions). Almost all submitters were opposed to this proposal, noting that it would undermine the lawyer's obligations to their client, impact legal professional privilege, create a barrier to justice, and limit a person's right to a fair trial. We therefore recommend maintaining the status quo and not imposing any AML/CFT obligations on criminal defence lawyers.

Recommendation

R74. Maintain the status quo and do not include criminal defence lawyers within the scope of the Act.

4.3.4. Non-life insurance businesses

560. Life insurance is currently the only type of insurance service that attracts obligations under the Act, which is consistent with the FATF Standards. However, insurance companies offering other types of insurance policies may be able to identify suspicious activity or behaviour, such as potential or actual frauds. Insurance policies can also be vulnerable to money laundering, for example where a customer makes an overpayment or requests a refund shortly after purchasing a policy.

561. Including non-life insurers in the Act could provide an additional source of financial intelligence and address money laundering vulnerabilities. Obligations of non-life insurers could also be tailored to ensure they are in line with the risks and vulnerabilities identified e.g., they might only be required to monitor accounts and report suspicious activity. Despite a potentially lower set of AML/CFT obligations, any change would still impose compliance costs and ultimately impact the availability of insurance.

562. Most submitters did not support non-life insurers having AML/CFT obligations. They considered the risks associated are minimal due to the low monetary amounts involved and existing controls in place to detect and prevent fraud, including already referring fraudulent activity to the Police. Submitters considered this to be an onerous inclusion with little benefit to the regime. If general insurers were included, almost all submitters supported tailored obligations for these businesses that are commensurate with the risks posed.

563. We recommend maintaining the status quo and not including non-life insurers within the regime. We do not consider the risk of money laundering and terrorist financing through these entities is significant enough to warrant their inclusion. We also note it may divert resource away from areas that pose significant harm, such as insurance fraud. Additionally, insurers require a crime to be reported to Police before paying out a claim, meaning that the Police are already able to receive intelligence about any criminality detected by insurers.

Recommendation

R75. Maintain the status quo and do not include non-life insurers within the scope of the Act.

4.3.5. Non-profit organisations vulnerable to terrorism financing

564. Charities and other non-profit organisations have been identified internationally by the FATF as being vulnerable to exploitation for terrorism financing. In New Zealand, registered charities that operate overseas and in high-risk jurisdictions, tax-exempt non-profits that are not registered charities, and non-resident tax charities are the types of non-profit organisations that have some vulnerabilities. However, non-profit organisations that are not registered charities and non-resident tax charities are not subject to monitoring or supervision.

565. We explored whether the Act could be used to mitigate the vulnerabilities of non-profit organisations which are not registered charities and non-resident tax charities by including them as reporting entities with appropriately tailored obligations. However, including these non-profits in the AML/CFT regime would have potentially significant compliance costs and risks undermining their ability to provide charitable services. Other options, such as ensuring that Charities Services or Inland Revenue have oversight, are outside of the scope of this review.

566. Submitters were split on the option of including these non-profit organisations within the AML/CFT regime, with a large portion of submitters unsure about the proposal. Those opposed were concerned about the compliance costs and the risk that the proposal would cause non-profits to stop operating. Submitters also noted that banks are typically involved in transactions, and the proposal could lead to non-profit organisations being de-risked.

567. We do not consider it is appropriate to include tax exempt non-profits and non-resident tax charities within the AML/CFT regime. While we recognise there are risks associated with these types of organisations, we consider such a measure could have significant implications and disproportionate compliance costs. We also consider that the AML/CFT regime is ill-equipped to best mitigate the risks associated with these organisations. Risks of abuse of non-profits are typically combatted by imposing public transparency and accountability measures, such as requirements to issue annual financial statements. Nevertheless, we will continue to work with other agencies, in particular Inland Revenue and Charities Services to increase monitoring or supervision of these charities.

Recommendation

R76. Maintain the status quo and do not include non-profit organisations which are not registered charities and non-resident tax charities within the scope of the Act. Agencies will continue to explore alternative options for increasing the monitoring or supervision of the charities.

4.4. Currently exempt sectors or activities

568. Regulatory or class exemptions are used to exclude types of activities or transactions from the Act, to mitigate unintended capture, or to relieve businesses of various obligations and ensure that their regulatory burden is proportionate to risks to which they are exposed. The FATF determined that New Zealand had granted a large number of exemptions, and not all were granted in cases of proven low money laundering or terrorism financing risks (*see* Applying for exemptions from the Act under section 157). We identified several regulatory exemptions that could be amended to bring them more in line with our money laundering and terrorism financing risks. We also asked submitters whether they have encountered issues with the operation of any regulatory exemptions or class exemptions.

4.4.1. Internet auctioneers and online marketplaces

569. Regulation 21A of the *AML/CFT (Definitions) Regulations 2011* excludes all internet auction providers from the Act. The definition of 'internet auction provider' is broad and incorporates online marketplaces even though they do not provide an auction service. The scope of the exclusion also applies to all activities an internet auction provider engages in, regardless of the risks associated with that activity in an internet auction setting. We have identified risks regarding internet auction providers and online marketplaces. For example, we identified that online marketplaces could be used to facilitate a domestic form of trade-based money laundering. Accordingly, we considered the scope of the exemption and the extent it should apply to internet auctioneers and online marketplaces.

570. Most submitters did not think that Regulation 21A should still apply, with submitters generally noting the risks associated with online marketplaces, particularly where high value, stolen, or non-existent goods are being bought or sold. Submitters considered that removing the exclusion would ensure a consistent approach between in person and online transactions. However, a minority of submitters thought the exemption should continue to apply to avoid unnecessary compliance costs and not stifle online commerce. Notwithstanding the above, submitters generally identified the need for further clarity about how the Act applies to online commerce, particularly with respect to international commerce platforms such as Amazon (*see* Territorial scope).

571. We recommend revoking Regulation 21A given the breadth of entities and activities captured by the exemption and the associated money laundering risks. This means internet auction providers and online marketplaces would have to fully comply with the Act where they issue or manage the means of payment. We consider that this activity in the context of internet auctions and online marketplaces can be used to facilitate money laundering and should therefore be subject to the Act.

572. However, we also recognise that some online marketplaces have internal controls which mean the risk is low and that an exemption for some or all aspects of the business may be justified. Accordingly, we recommend conducting further analysis to assess whether it is appropriate to issue a new exemption for online marketplaces. This decision should be based off a risk assessment and consider whether we could exempt some obligations (e.g., some CDD requirements, prescribed transaction reporting, independent audit) or certain activities that are demonstrably low risk. This analysis and any new requirements should consider issues relating to territorial scope of the Act and who the customer is (i.e., merchant or consumer). We do not consider that internet auction platforms have the same mitigating controls and therefore, it would be appropriate for these businesses to be fully captured when issuing or managing the means of payment.

Recommendations

R77. Revoke Regulation 21A of the *AML/CFT (Definitions) Regulations* 2011 which excludes internet auction providers from the Act, including online marketplaces.

R78. Explore whether to issue an appropriate exemption for some AML/CFT obligations based off a risk assessment for online marketplaces if there are aspects which are demonstrably low risk.

4.4.2. Special remittance card facilities

573. Regulation 10 of the *AML/CFT (Exemptions) Regulations 2011* provides a limited exemption from CDD obligations for businesses which offer certain types of remittance card facilities. This exemption is aimed at facilitating cross-border remittances to the Pacific and financial inclusion. However, it is not clear that the exemption is still necessary given the existence of other facilities that offer a similar service. We also identified that the exemption may not reflect our money laundering and terrorist financing risks, which was criticised in the Mutual Evaluation.

574. We received no submissions from the public indicating that special remittance cards are still being used or that the exemption is still being relied on by businesses. Submitters were also sceptical as to whether the exemption properly mitigates the relevant risks or that it facilitates remittances to the Pacific. We therefore recommend that we revoke Regulation 10 subject to final confirmation that it is no longer in use.

Recommendation

R79. Revoke Regulation 10 of the *AML/CFT (Exemptions) Regulations 2011* which provides a limited exemption for special remittance cards, subject to final confirmation that it is no longer in use.

4.4.3. Non-finance businesses which transfer money or value

575. Regulation 18A of the *AML/CFT (Definitions) Regulations 2011* has become problematic since the Act was amended in 2017 to include DNFBPs. This is because DNFBPs are, by definition, "non-finance businesses", and some DNFBPs regularly transfer money to facilitate the purchase of goods or services that are not relevant services. This can become managing client funds and thus is intended to attract AML/CFT obligations. However, this is currently unclear and could be clarified.

576. We recommend exploring amendments to provide further clarification around the scope of Regulation 18A, particularly in relation to DNFBPs. This could include limiting the exclusion from being a financial institution under the Act. This change would clarify that the DNFBP activity of managing client funds is not within scope of the exemption which would reflect the original policy intent. It would also provide an opportunity to identify any changes required to clarify what businesses should be within scope of the exemption. Most submitters were supportive of this approach.

Recommendation

R80. Explore amendments to Regulation 18A *AML/CFT (Definitions) Regulations 2011* to clarify its scope, including the option of limiting the exclusion from being a financial institution under the Act.

4.4.4. Workplace savings retirement schemes

577. Many workplace savings retirement schemes rely on the exemption contained in Regulation 20A of the *AML/CFT* (*Exemptions*) *Regulation 2011* for relevant services provided in respect of certain employer superannuation schemes. Regulation 20A currently permits additional contributions through payroll, provided they are determined as a percentage of salary/wages on the trust deed. The maximum percentage is outlined in the trust deed is the maximum voluntary contribution that members can make and is typically capped at 20 percent of salary or wage contributions.

578. We did not specifically consult on this exemption, however several submitters (including the workplace superannuation schemes themselves) submitted on this topic and suggested that Regulation 20A should be clarified to allow unlimited voluntary member contributions from their salary/payroll to support the members' ability to save for retirement.

579. We have not had the opportunity to fully assess the risks and impacts associated with progressing any amendments to Regulation 20A to increase the amount of voluntary contributions that could be made. Our preliminary analysis highlights that voluntary member contribution carry some money laundering risk given that some voluntary contributions are not locked in and members can request payments from their voluntary account at any time.

580. Therefore, we recommend conducting further analysis of risks to ensure the settings of Regulation 20A are aligned with the risks of these retirement schemes. We note that this analysis could result in further tightening Regulation 20A if the risks associated with these schemes are found to be higher than when the exemption was first issued. In addition, any changes to increase the amount of voluntary contributions could only be progressed if the analysis demonstrates the change would carry low risks of money laundering and terrorism financing.

Recommendation

R81. Explore whether any amendments should be made to Regulation 20A of the *AML/CFT (Exemptions) Regulation 2011* regarding workplace savings retirement schemes. This should involve assessing the risks associated with workplace savings retirement schemes and whether the existing settings are in line with those risks, as well as the impact to the broader sector that could result from any changes.

4.4.5. Non-court appointed liquidations

581. Regulations were issued in 2021 for court appointed liquidations to clarify who should be considered the customer and ensure AML/CFT requirements were appropriately tailored. However, feedback from submitters indicated that clarifications should also

be provided for non-court appointed liquidations, in respect of which the application of the Act can be challenging. We agree that the application of the Act to non-court appointed liquidations needs to be reviewed so that it is fit-for-purpose and aligns with the risks faced in the sector. We therefore recommend a review to determine whether similar regulations should be issued for non-court appointed liquidators as for those issued for court appointed liquidations.

Recommendation

R82. Review the application of the Act to non-court appointed types of liquidation with a view to exempting some AML/CFT obligations that are incompatible with the nature of the liquidator's work, while also ensuring other AML/CFT requirements are appropriate to the money laundering and terrorism financing risks faced in the sector.

4.4.6. Minor changes to existing exemptions

582. We recommend making the following minor changes to existing exemptions:

Issue	Recommendation
Regulation 24AC of the *AML/CFT (Exemptions) Regulations 2011* exempts reporting entities from certain sections obligations when subject to a Production Order or order issued under section 143(1)(a). However, reporting entities also receive orders under the *Customs and Excise Act 2018* which may inadvertently lead to tipping off. In addition, in the process of complying with the relevant order, the reporting entity may form suspicion about associated persons. The exemption does not explicitly cover associates and therefore there is a risk that suspicious associates are tipped off.	Expand the exemption to include reporting entities subject to an order issued under section 252 of the *Customs and Excise Act 2018* as well as in respect of any suspicious associates who are identified in the process of complying with the relevant order.
Regulation 17 *AML/CFT (Exemptions) Regulations 2011* exempts reporting entities that are not an insurance company who are providing a service under a premium funding agreement from section 14-26 of the Act but does not exempt them from the requirement to identify a customer under section 11. This means exempt reporting entities must conduct ongoing CDD and account monitoring under section 31, but as they have not conducted CDD they have nothing to review.	Link the exemption more directly to the level of money laundering and terrorism financing risk associated with premium funding and clarify intention (or not) to capture premium funding as an activity for the purposes of AML/CFT
Regulation 22 of the *AML/CFT (Exemptions) Regulation 2011* exempts debt collection services from the Act other than relating to suspicious activity reporting. Debt collection services are defined as "the collection of debt by a person other than the creditor to whom it is owed or, where it has been assigned, to whom it was originally owed". The scope of this definition is unclear.	Clarify that the definition of debt collection services only relates to the collection of unpaid debt rather than the collection of any funds owed by one person to another.
Regulation 9 of the *AML/CFT (Exemptions) Regulations 2011* currently exempts currency exchange transactions performed in hotels that do not exceed NZD 1000 from most obligations in the Act, except obligations to file suspicious activity reports and keep records of any reports filed. However, the way this exemption operates may cause confusion for hotel operators which could be exploited by people seeking to launder money or finance terrorism. In particular, hotel operators may not be aware that they have full obligations for any currency exchange transaction that exceeds NZD 1000, irrespective of how regularly they engage in any large value currency exchange transaction.	Clarify that the exemption applies to hotel providers which only undertake currency exchange transactions below NZD 1000.

4.5. New regulatory exemptions

4.5.1. Acting as a trustee or nominee

583. Many DNFBPs provide 'acting as a trustee or nominee' services by establishing one or more separate companies. Typically, these are wholly owned and controlled subsidiaries of a DNFBP that have obligations under the Act, including in circumstances when the parent DNFBP also has the same obligations. We asked businesses about how they provide trustee or nominee services, including whether we should issue an exemption for these types of companies in certain situations, and if so, what that exemption could look like.

584. Several submitters indicated that they use companies to act as a trustee or nominee, predominantly when acting for a trust or company that is a client of the DNFBP. Some set up a single company to service several clients, while others set up one such company per client. The directors of these subsidiary companies are generally, but not always, the directors or partners of the DNFBP. The subsidiary companies are used to ease the administration of the trust, manage risk, and to allow for independent and professional governance. Most submitters were also supportive of exempting trustee or nominee companies that are controlled by a parent DNFBP to reduce the duplication of compliance obligations, with some suggesting that the trustee companies be included in the DNFBP's annual report.

585. We recommend issuing a narrow regulatory exemption to cover companies established to act as trustees or nominees where they are controlled by a parent DNFBP (or financial institution, *see* Businesses providing multiple types of activities). While the potential for misuse of trusts and nominee arrangements is significant, we recognise that many trustee or nominee companies are genuinely set up for administrative purposes only and do not pose any additional risks that cannot be effectively mitigated under the parent reporting entity's AML/CFT programme. However, this does not preclude trustee or nominee companies from being used to obscure beneficial ownership and facilitate illicit activity. As such, we recommend carefully considering the following aspects of any exemption to ensure that it applies only in appropriate circumstances:

- **the extent of control exercised by the parent business:** defining control appropriately will be key to ensuring that the exemption only applies to companies in situations where a parent DNFBP has full AML/CFT oversight. Control could be defined by reference to concepts of "related" within the meaning of section 2(3) of the *Companies Act 1993* (e.g., where the company is a subsidiary of the parent DNFBP) or within the definition in Regulation 16 of the *AML/CFT (Exemptions) Regulations 2011*.

- **the extent of oversight or mitigation by the parent business:** even though we are proposing to exempt these companies from being reporting entities, we would still want to ensure that the parent business maintains full AML/CFT responsibility for the activities of the nominee or trustee company. This could include requiring the parent business to account for its nominee or trustee companies in its risk assessment and compliance programme, maintain a list of the companies, or include the companies' operations in their annual reports.

- **the nature of the underlying trust:** while we recognise that not all trusts are high risk (*see* Mandatory enhanced CDD for all trusts), there are well-documented instances where New Zealand trusts have been misused for illicit activity. Submitters identified that trusts could be higher risk where they involve offshore parties, offshore assets or accounts, complex deeds, or are settled by recent residents. An exemption will need to consider how to ensure these risks are mitigated.

586. We recommend conducting further engagement to determine these remaining settings. As a starting point, we consider that an exemption should apply to trustee or nominee companies that are wholly owned subsidiaries of a parent DNFBP that is a reporting entity in New Zealand. The parent DNFBP should be required to account for

the companies in its compliance programme, maintain a list of the companies, and report on them as part of the annual report.

Recommendation

R83. Issue a regulatory exemption for companies that act as a trustee or nominee and are controlled by a parent reporting entity in New Zealand (that has full AML/CFT responsibilities for activities of the nominee or trustee company), subject to further engagement with the sector to determine how control should be defined and the appropriate amount of oversight that the parent reporting entity should maintain over the companies.

4.5.2. Crown entities, Crown agents etc

587. More than 2,700 entities in New Zealand are structured as Crown entities, agents, or companies and many may provide services or activities which attract AML/CFT obligations. Seventeen Crown entities, agents, or companies currently have at least a partial exemption from the Act, generally in relation to specific products or ventures. We considered whether a regulatory exemption should be issued to exempt Crown entities, agents, and companies in general and, if so, what an exemption could look like. However, we would need to ensure that the exemption is risk based and does not introduce vulnerabilities into the AML/CFT regulatory regime.

588. There are several options for how an exemption of this nature could be drafted. A narrow option would be to exempt these entities only where their activities involve public funds and where the Crown is the sole customer, while a broad option would be to exempt any Crown organisation listed in the *Public Finance Act 1989* or *Crown Entities Act 2002*. However, we note that most of the existing Ministerial exemptions for Crown entities have been in respect of the entity issuing loans to the public using Crown funds. As such, a compromise position would be to exempt this activity through regulations, but with appropriate conditions to ensure the loans cannot be abused for illicit purposes.

589. Many submitters supported a regulatory exemption for Crown organisations, on the basis of their financial transparency requirements and assumed lower money laundering and terrorism financing risks. However, several disagreed on the basis that the Crown organisations involved may still be exposed to some risks. Some submitters also noted that any exemption might give Crown organisations a competitive advantage over other businesses operating in the same sector.

590. To help reduce compliance costs while avoiding the introduction of AML/CFT risks and vulnerabilities, we recommend issuing a regulatory exemption for Crown entities, agents, and companies from AML/CFT obligations in two circumstances: firstly, where the Crown is the sole customer and secondly where the entity is using public funds to provide loans to the public. The latter should be subject to appropriate conditions to ensure it does not create additional vulnerabilities, such as prohibiting the loans to be paid off early or using cash and ensuring that the entity is subject to sufficient public accountability mechanisms.

Recommendation

R84. Issue a regulatory exemption for Crown entities, agents etc that applies where the Crown is the sole customer of the activity and where they are using public funds to provide loans to the public. The exemption should include appropriate conditions in respect of the latter activity, such as prohibiting loans being paid off early or through cash and requiring the entity to be subject to sufficient public accountability mechanisms.

4.5.3. Low-value loan providers

591. Low-value loans can play an important role in providing support to communities in need, and the funds are typically provided by charities and used to support

community projects and social outcomes. However, providing loans attracts AML/CFT obligations, which can make it harder for organisations to provide this support, and these organisations often seek to be granted an exemption. Seven registered charities providing loans to low-income people have been granted a Ministerial exemption from the Act, many with a loan cap of NZD 6,000 per customer. An eighth is being considered for approval.

592. We explored whether this activity should be exempted entirely given that applying for an exemption can be a complex and time-consuming process. This exemption could be structured to apply only to certain types of loan providers (e.g., registered charities), to specific types of loans (e.g., loans for welfare purposes, which may not be provided by a registered charity), and/or to loans below a specific threshold.

593. Overall, submitters supported the proposal to exempt low-value loan activity being carried out by registered charities, noting that the risks associated with such loans are minimal and compliance costs can erode the benefit of providing the loans. Money laundering and terrorism financing risks are reduced for registered charities compared with other non-profits, due to the accompanying regulatory oversight, accountability requirements and financial scrutiny. However, some submitters disagreed with the proposed exemption, noting that it could still provide a loophole and create a vulnerability for money laundering to occur.

594. We recommend issuing a Ministerial class exemption for low value loan providers where they are registered charities, and where the maximum amount loaned to a customer does not exceed NZD 6,000 per annum. This exemption would cover all existing individual Ministerial exemptions that have been granted and remove the need for those entities to reapply when their exemption eventually expires. We further recommend that the exemption should include requirements that a customer be limited to taking out one such loan at any time which cannot be repaid more quickly than the agreed timeframe or repaid in cash.

Recommendation

R85. Issue a Ministerial class exemption for registered charities providing loans to customers below where the maximum amount that can be loaned to a customer is no more than NZD 6,000. This exemption should include conditions which limit the loans to one per customer and restrict the ability to repay loans quickly and in cash.

4.5.4. Application of Act to real estate agents for commercial leasing

595. Listing and arranging a commercial lease by real estate agents is a captured activity under the definition of a real estate transaction. Once leased, any property management activities are excluded from the Act. These settings mean AML/CFT obligations must be applied to the real estate agent's client (usually the lessor) and only up to the point a lease is entered into. The FATF Standards do not require real estate agents to apply AML/CFT obligations to commercial leasing (noting that ownership of the property does not transfer). However, the FIU has received SARs from real estate agents in respect of commercial leases which may indicate that there are risks associated with this type of real estate transaction.

596. Regulations were issued in 2021 to relax the timing of CDD requirements when arranging a commercial lease for a client. The amended requirements now better align with the way the commercial leasing sector operates in practice. Based on feedback provided during private sector engagement in April 2022, we consider there may be further concessions or an exemption that can be made to the application of the Act to commercial leasing. Alternatively, there may be circumstances in which some AML/CFT obligations should be applied to lessees rather than the lessor. We therefore recommend that agencies undertake further analysis to assess the level of risk associated with commercial leasing. This should determine the extent to which AML/CFT obligations should apply to commercial leasing, to which party to the lease, and/or the extent to which AML/CFT obligations could be exempted.

Recommendation

R86. Review the level of risk associated with commercial leasing and consider regulations to reduce or amend AML/CFT obligations for real estate agents to align with the risks, or exempt commercial leasing from the Act. This risk assessment should consider whether some AML/CFT obligations should apply to commercial lessees.

4.5.5. Other exemptions

597. We asked if any other new regulatory exemptions should be considered for types of reporting entities or activities captured by the Act but have low money laundering or terrorism financing risks. Submitters made a large number of suggestions. Of these, two cannot be progressed at this stage because they either already have a class exemption (retirement village statutory supervisors) or are currently being considered for a class exemption (accounting practices undertaking tax transfers between parties with overlapping interests).

598. Of the remaining suggestions for exemption, most appear to have some associated risks of money laundering or terrorism financing. In these cases, more information is required to consider whether specific activities might be considered for exemption. As part of our process to explore whether any other regulations are required to support a more risk-based approach (*see* Balancing prescription with risk-based obligations), we intend to work through the details of each proposal to assess the level of risk associated with a full or partial exemption for each.

Recommendation

R87. In line with other recommendations regarding the risk-based approach and financial inclusion, agencies should continue to work through the suggestions for exemptions and assess the money laundering and terrorism financing risks associated with the proposals.

4.6. Territorial scope

599. The Act does not set out where business activities need to be conducted in order to attract AML/CFT obligations in New Zealand. For example, there is no test to determine whether an activity provided solely online to New Zealanders by an offshore company attracts obligations, nor whether a New Zealand business which forms or incorporates companies, acts as a trustee, or provides financial services exclusive for foreign customers should be exempt from obligations under New Zealand law. The absence of any territorial scope provisions in the Act are increasingly raising complex questions of how to determine whether a business or business activity should be subject to AML/CFT obligations in New Zealand.

600. We considered whether the Act should define its territorial scope, with almost all submitters agreeing that it should. Submitters thought the Act could adopt approaches taken in other legislation, such as the *Companies Act 1993* or the *Financial Service Providers (Dispute and Resolution) Act 2008* or take a bespoke approach for the AML/CFT regime. For example, the Act could capture any business which carries out AML/CFT services in or to New Zealand or have customers or derive revenue from activity in or associated with New Zealand, or simply capture all New Zealand citizens and residents and legal persons incorporated in New Zealand that provide AML/CFT activities.

601. We agree that the Act should define its territorial scope as this ensures an even playing field between New Zealand businesses and offshore businesses offering services in New Zealand. In particular, it ensures that New Zealand businesses are not disadvantaged by being in New Zealand by the mere fact of having AML/CFT obligations. It also reduces the potential for offshore businesses to present a

vulnerability that could be exploited by money launderers or terrorist financiers by ensuring they also have AML/CFT obligations.

602. We do not have a recommendation for how the Act should define its territorial scope as we have not been able to compare the relative benefits or costs of the various approaches that could be taken (*see* Limitations of the approach). Our initial preference is to define the Act's scope by reference to providing services to or from New Zealand but note that this would need to be carefully designed to ensure it does not have unintended consequences. For example, the scope would likely need to have some form of threshold to ensure that one-off services are not captured but could also incorporate some form of exemption regime. This could allow overseas businesses to be excluded from the Act's capture if the business is based in a jurisdiction with comparable AML/CFT controls, which could also include consideration of the level of international cooperation between New Zealand and authorities in that country.

603. However, recognising that defining the Act's territorial scope would require legislative amendments to be progressed, in the interim we recommend reviewing and updating the existing territorial scope guidance. In particular, supervisors should consider whether guidance provides sufficient clarity to businesses, takes the appropriate approach in line with the purpose of the Act, and is consistent with guidance produced by other agencies in relation to other regimes. Supervisors should also consider whether providing examples of particular scenarios and whether they fall within the territorial scope of the Act would be beneficial, given the variety in how businesses can operate and connect with New Zealand.

Recommendations

R88. Conduct further analysis of potential approaches for defining the Act's territorial scope, including the initially preferred approach of defining the scope to include overseas businesses which provide activities to New Zealand above a prescribed threshold. Agencies should also consider the appropriateness of any exemption regime which could apply where the business is based in a jurisdiction with equivalent AML/CFT controls and sufficient levels of international cooperation with New Zealand.

R89. In the interim, supervisors should review and update the existing territorial scope guidance to ensure it is sufficiently clear, appropriate, and consistent with similar guidance produced by other agencies in relation to other regulatory regimes.

CHAPTER 5

Supervision, regulation, and enforcement

Summary

604. This chapter makes a number of recommendations to improve the supervision, regulation, and enforcement of the regime. A core component of the AML/CFT regime is that it needs to enable effective supervision and regulation of businesses. The supervision and monitoring of businesses should address and mitigate money laundering and terrorism financing risks in the economy, in part by promptly identifying, remedying, and sanctioning (where appropriate) businesses which do not adequately comply with their obligations. We have also considered whether there should be any regulation of businesses which provide services to reporting entities, specifically auditors, agents, and consultants.

605. We note that there are no specific AML/CFT specific registration or licensing framework, but that the regime relies on other sector-specific frameworks, such as the Financial Services Provider Register. However, this approach was criticised by the FATF and results in some sectors not having any registration requirements, other sectors not being subject to sufficient fit and proper or market entry checks, and some high-risk sectors not being licensed when they arguably should be. We recommend agencies further develop specific options for a comprehensive registration framework, which includes amending the Act to create a specific registration requirement for those sectors that have no existing requirements. We also recommend amending the Act to create a specific AML/CFT licensing framework for high-risk sectors that are not already required to be licensed (for example remitters and trust and company service providers).

606. We recognise the valuable contribution that many auditors, agents, and consultants provide to the AML/CFT regime. However, we also recognise that there are instances of unsatisfactory audits occurring in some sectors, and that the Act is not sufficiently mitigating the risks posed by agents. As such, we recommend further regulation of audits and auditors, such as creating a code of practice which details the requirements of an audit as well as amending the Act to introduce an accreditation regime for auditors. We consider that these steps will likely improve the quality and value of audits, but we also note that further work may be required if these changes do not sufficiently improve audit outcomes. With respect to agents, we recommend issuing regulations to ensure that businesses which use agents are appropriately vetting and training their agents as well as ensuring their agents comply with the requirements of the Act. We do not recommend any additional regulation for consultants at this stage.

607. Finally, we make a number of recommendations to ensure that effective, proportionate, and dissuasive penalties can be applied against businesses which fail to comply with the Act. In particular, we recommend allowing for infringements or fines to be imposed against businesses as well as for supervisors to be able to restrict, suspend, or cancel a business' AML/CFT or prudential licence or registration for non-compliance with the Act. We also recommend increasing the available penalties in the Act to ensure they are able to be proportionate to serious misconduct irrespective of the size or nature of the business involved, as well as for civil penalties to be imposed against employees, directors, and senior managers in appropriate circumstances. However, we also recognise that penalties should be risk based and proportionate in their application and recommend amending the Act to prescribe a non-exhaustive list of AML/CFT-specific aggravating and mitigating factors that must be considered when penalties are applied.

5.1. Licensing and registration

608. Most, but not all, businesses that have AML/CFT obligations have some other form of requirement to be registered and/or licensed that is not imposed by the AML/CFT Act. However, there are number of large gaps in terms of which businesses are required to register, meaning that supervisors, particularly the DIA, are unable to easily identify which businesses they supervise. In addition, some high-risk businesses are only subject to limited fit and proper checks before being able to offer the services. This means that there is a greater risk of these businesses being owned or controlled by criminals or their associates.

609. We considered what, if any, changes should be made to the Act to support licensing and registration, given that any licensing or registration requirement would need to be compatible with existing requirements such as the Financial Service Providers (FSP) Register. For context, licensing a business usually means that the business needs to satisfy objective criteria to demonstrate that they are suitable to provide the business activity and requires agencies to actively approve the business to carry out the relevant services. It can also allow the licensing agency to impose limits or conditions on how the business operates. Registering a business, by contrast, usually does not require the business to satisfy the various criteria, except that they intend to provide the relevant activity and potentially satisfy a fit-and-proper test.

5.1.1. Registration for all reporting entities

610. There are two broad issues with the current registration requirements, as identified by the FATF:

- **no registration requirement for some sectors** – there are currently six financial institution sectors (debt collectors, factoring, tax pooling, payroll remittance, cash transport and safety deposit boxes) and three other non-financial sectors (trust and company service providers, high-value dealers and accountants that are not chartered accountants) that do not have to be registered or licensed. This limits the AML/CFT supervisor's visibility of these sectors. In addition, this means that businesses in these sectors are not required to undergo any fit and proper checks, meaning that criminals or their associates could own or control businesses within these sectors.

- **inadequate "fit and proper" or criminal record check requirements** – for those financial sectors that are only required to register on the FSP Register, fit and proper or criminal record checks only apply to controlling ownership equal to or more than 50 percent. The FATF determined this is high and inconsistent with the relevant ownership thresholds adopted in other legislation. In turn, the FATF determined this does not fully prevent criminals or their associates from owning or controlling businesses in these sectors.

611. There are various options we could progress to increase visibility of the reporting entity population and enable more effective fit and proper or criminal record checks. This includes coordinating with MBIE to expand its FSP registration requirements to include the six financial institution sectors that do not currently have to be registered (*see* Definition of financial institution activities). Concurrently, the controlling ownership threshold for fit and proper or criminal record checks could be lowered as part of any changes to the FSP Register. Furthermore, the Act could be amended to establish an AML/CFT specific registration requirement which applies only to non-financial sectors (i.e., those without an existing registration requirement) or to all sectors, even those with existing registration requirements.

612. Most submitters did not support an AML/CFT specific registration process. Submitters considered this would be a duplication and both a financial and administrative burden. Instead, most submitters supported integration of AML/CFT registration into existing requirements, particularly for financial institutions under the FSP Register. That said there was support for a registration requirement for those sectors without any existing

requirements when we conducted targeted engagement in April 2022. There was also support for a central publicly available register that would list all reporting entities in the one place across all sectors.

613. We agree with the concerns raised by the private sector about duplication of registration requirements and cost. However, we also consider the current gaps in visibility and fit and proper or criminal record checks pose risks that should be addressed. Ensuring all sectors are required to register and, be subject to appropriate fit and proper checks, would also improve New Zealand's compliance with the FATF Standards.

614. Accordingly, we recommend agencies further develop specific options for a comprehensive registration regime in coordination with MBIE. In particular, we recommend developing options for amending the Act to create a specific registration requirement for those sectors not currently required to be registered, which will need to include more detail about the process for registration and the associated costs. For those sectors currently only required to register on the FSP Register, we recommend coordination with MBIE to consider lowering the controlling ownership threshold for fit and proper or criminal record checks. Finally, for those sectors registered or licensed under other legislations (other than by RBNZ or FMA), we recommend progressing a requirement to notify the relevant AML/CFT supervisor of reporting entity status.[39]

Recommendations

R90. Further develop and progress options for AML/CFT reporting entity registration so that supervisors have visibility of their supervised populations and consistent fit and proper or criminal record checks adequately prevent businesses being owned or controlled by criminals or their associates This should include further engagement with relevant agencies and the private sector.

R91. For sectors registered or licensed by peak bodies or government agencies (other than RBNZ and FMA), develop options to ensure the AML/CFT supervisor and the FIU are notified that a business is a reporting entity.

5.1.2. AML/CFT licensing for some reporting entities

615. As noted above, there is no specific AML/CFT registration or licensing framework for reporting entities, including no licensing for high-risk sectors, such as remitters, virtual asset service providers (VASPs), and trust and company service providers (TCSPs). In the remittance and VASP sectors, businesses are only required to register on the FSP Register, whereas there is no specific registration requirement for TCSPs anywhere. Relatedly, and for the remittance sector, the FATF identified deficiencies in our ability to combat underground providers operating in breach of requirements to register on the FSP Register. The FATF noted a lack of coordination between MBIE (the FSP Registrar), the FMA (responsible for enforcement of the FSP Register) and the DIA (as the AML/CFT supervisor of remitters) due to their separate regulatory functions.

616. We considered whether some reporting entities, particularly those in high-risk sectors, should be subject to a licensing framework or enhanced market entry controls (over and above those included in the FSP Register). This could incorporate fit and proper checks and other measures necessary for the AML/CFT supervisor or another appropriate body to make a qualitative determination whether a business has the required level of capability and competency to operate, and to mitigate its money laundering and terrorism financing risks. Additionally, such a framework could increase options for dealing with non-compliance. For example, the AML/CFT supervisor or licensing body could be empowered to impose conditions to manage or restrict activities in certain circumstances or against a business that was operating while not licensed or approved to do so (*see* Allowing for intermediary enforcement options).

[39] Incorporated into these processes could be a requirement to register with the FIU for the goAML system to be able to report SARs and PTRs, and in turn also receive disseminations regarding updates to UN Sanctions lists.

617. There are two options that could be progressed for licensing or enhanced market entry controls for high-risk sectors:

- **introduce an AML/CFT licensing framework for high-risk sectors:** obtaining a licence from the relevant supervisor or an appropriate licensing body would be a prerequisite for FSP registration to be able to provide the relevant service. The requirement to obtain a licence could include a review of the business' risk assessment and AML/CFT programme, declarations and checks to assess criminal associations, eligibility, AML/CFT capability and/or competency.

- **coordinate with MBIE to implement enhanced controls as part of FSP registration:** the AML/CFT supervisor could seek further information and undertake checks similar to those outlined above for licensing. Subject to the outcome of this process, the AML/CFT supervisor would be able to direct the registrar to approve or decline registration based on assessment of the level of risk.

618. Most submitters opposed a broad or general licensing framework but supported licensing or enhanced market entry controls for high-risk sectors that are not otherwise licensed. Submitters noted this may provide assurance to banks around AML/CFT capability and therefore assist in reducing de-risking (*see* De-risking). There was further support for a licensing framework for high-risk sectors during targeted private sector engagement in April 2022, including from the remittance sector. More broadly, licensing was preferred over enhanced market entry controls because it provided the most assurance of AML/CFT capability. Additionally, attendees noted that this approach would not allow businesses to present a FSP registration to mean they are a government authorised or endorsed provider (noting there have been issues of businesses misusing the FSP Register in this way).

619. We agree that only high-risk sectors should be licensed or subject to enhanced market entry controls. We also agree that a licensing framework is the preferred option over enhanced market entry controls as part of FSP registration requirements. Licensing high-risk sectors will allow supervisors to better manage the risks within the sector, including providing additional options and authority to address non-compliance or underground providers (*see* Allowing for intermediary enforcement options).

620. As such, we recommend amending the Act to introduce a licensing requirement in respect of high-risk sectors. The licensing framework should, at minimum, cover TCSPs, MVTS providers and potentially currency exchanges (noting this is often provided alongside a MVTS service). The framework should also provide the ability for other sectors to be included, such as VASPs, should this be justified by the risks of the sector. We note that further detail will need to be developed as part of implementing this recommendation, specifically in respect of who is responsible for assessing the license application and costs associated with the process. While the applicant will likely need to pay for some or all of the costs of being licensed, we anticipate that a licensing framework will lead more efficient and effective risk management overall.

Recommendation

R92. Subject to further engagement (particularly regarding costs), amend the Act to include an AML/CFT licensing framework for high-risk sectors (that are not licensed under other legislations). Licensing should be undertaken by the AML/CFT supervisor or another appropriate body and be a pre-requisite for registration on the FSPR to provide the relevant service.

5.2. Regulating auditors, consultants, and agents

5.2.1. Regulating independent auditors

621. The FATF Standards require businesses to be regularly audited to test the effectiveness of their AML/CFT programme. However, despite the AML/CFT supervisors revised 2019 Audit Guidelines, some businesses and auditors still appear unsure what is required by an audit.

Relatedly, there are no specific standards or qualifications required to undertake an independent audit other than be "independent" and "appropriately qualified". Other than market forces, there are also no controls on how much an auditor may fairly and reasonably charge. Ensuring auditors are suitably qualified, standards are adhered to, and costs are fair and reasonable, may assist in the delivery of a more robust independent audit framework.

622. We identified several options that could be progressed that are not mutually exclusive, such as:

- **revise and expand on existing guidance** to ensure expectations for audits are sufficiently clear, as well as setting out expectations and qualifications required to be an independent auditor. However, a large amount of guidance has been issued and the quality of audits has not improved. In addition, guidance is not enforceable.
- **introduce a new code of practice** introduce more explicit requirements and standards for an independent audit to comply with the requirements of the Act, including appropriate levels of assurance considering the level of risk and size of the business. As codes of practice are enforceable, businesses would need to comply with the requirements of the code or ensure their alternative approach is equally effective (*see* Making or amending codes of practice under section 64).
- **amend the Act** include additional prescriptive requirements for audits and auditors. This could include explicitly stating an audit must test the effectiveness of an AML/CFT programme and/or allowing creation of auditor standards and qualifications.
- **introduce an external validation process** to provide assurance that auditors are appropriately qualified to undertake audits and that standards are adhered to. This could be through registration, accreditation, or licensing and include a mechanism to ensure costs are fair and reasonable.

623. Most submitters raised issues with the requirements, the quality, and cost of audits. They supported introducing standards and qualification requirements to ensure quality and consistency, noting the current variability. Many submitters also supported an accreditation or licensing process for auditors. However, some submitters suggested introducing more prescriptive requirements may restrict the scope and flexibility and in turn, the quality of an audit. Other submitters noted potential increase in costs due to limited supply of auditors. These views were also reiterated during the targeted engagement workshops in April 2022.

624. To address the issues with the independent audit framework, we initially recommend requesting the supervisors prepare a code of practice to set out more explicit requirements for an independent audit to comply with the Act. We consider this may improve the quality of audits and consistency of standards, but without a need for further changes that would increase the cost of audits even more. For the longer term, we recommend reviewing the impact of this code of practice to determine if further measures are required. Options then include amendments to the Act, creating auditor standards, registration, accreditation or licensing frameworks and a mechanism to ensure the costs of audits are fair and reasonable.

Recommendations

R93. Request that the AML/CFT supervisors develop code of practice that sets out more explicit provisions for an independent audit to comply with the requirements of the Act, including appropriate levels of assurance considering the level of risk and size of the reporting entity.

R94. For the longer term, and subject to review of the impact of Recommendation R93 above, consider whether additional measures are required to regulate auditors and independent audits. This could include amending the Act to state an audit must test the effectiveness of an AML/CFT programme, allow creation of auditor standards, a registration, accreditation or licensing framework and a mechanism to ensure the costs of audits are fair and reasonable.

5.2.2. Regulating consultants

625. Since the Act took effect, there has been an increase in the use of consultants by businesses to undertake their risk assessments and develop AML/CFT programmes. There is a varying level of consultant capability in the market and no standards, registration, or licensing requirements for AML/CFT consultancy services. Ensuring consultants adhere to standards and are appropriately qualified may improve the quality and consistency of their services.

626. We identified several options for improving consultant standards:

- **specify the requirements for consultants in the Act**, including requirements and standards for operating as an AML/CFT consultant.
- **introduce a licensing, registration, or accreditation process** to ensure consultants are appropriately qualified and adhering to relevant standards.
- **amend the Act to enable regulations for consultants to be implemented** such as prescribing the requirements that consultants must adhere to when providing services.

627. Most submitters did not support legislative or regulatory requirements for consultants. Submitters noted this would be contrary to the intent of the Act, add further complexity and cost, as well as undermine the value that consultants can provide. However, some submitters supported requirements for consultants, including registration or licensing, noting they should be required to provide sound advice to clients. Other submitters thought guidance could be provided to consultants to set expectations. These views were reiterated during the private sector in April 2022. Overall, we agree with industry views and recommend retaining the status quo. We do not consider any regulatory requirements should be introduced for consultants.

Recommendation

R95. Remain with the status quo and do not regulate consultants in the Act.

5.2.3. Regulating agents

628. Some businesses appoint and rely on agents to carry out AML/CFT obligations. For example, a business may rely on an agent to conduct CDD, keep records, provide training, or undertake account monitoring to identify suspicious activity. However, it is not clear in the Act what AML/CFT requirements an agent may be relied upon, other than CDD pursuant to section 34. Relatedly, it is not clear the extent to which a business is responsible and liable for the AML/CFT functions carried out by an agent on its behalf. In addition, there is no explicit requirement in the Act for a business to maintain a list of its agents, nor to ensure its agents are suitable and trained to undertake AML/CFT duties. For the MVTS sector specifically, the FATF identified these gaps as deficiencies in our AML/CFT framework.

629. We considered whether specifying how businesses may use agents, and their obligations and liability under the Act when doing so, would make relying on agents more workable and address areas of risks. We identified several options which could be progressed to ensure our AML/CFT settings for agents, which are not necessarily mutually exclusive:

- **specify the AML/CFT obligations for which an agent is responsible**, versus the obligations which the reporting entity has responsibility and any obligations where there is joint responsibility.
- **prescribe that an agent is itself a reporting entity under the Act.** In turn, the agent would be required to have its own AML/CFT programme and be responsible for meeting all its own AML/CFT obligations, including submitting SARs.

- **prescribe that an agent may undertake any function for a reporting entity** (including reporting PTRs or SARs), but that this occurs as part of the reporting entity's AML/CFT programme.
- **require reporting entities to ensure the agent complies with the Act** through having appropriate policies, procedures, and controls (PPCs), including a requirement that agents are subject to vetting and training. We could also require a reporting entity to maintain a list of agents as part of its programme which must be provided to the AML/CFT supervisor upon request.
- **issue guidance** to clarify the different circumstances, types of agents and AML/CFT functions that an agent can undertake under the Act.

630. Most submitters identified a need for clarity around the functions that an agent may undertake for a reporting entity, including when obligations can be outsourced to a third-party provider. Many submitters also considered that there should be standards to which agents are held. However, submitters were split on whether there should be regulatory requirements for agents such as minimum standards or whether the reporting entity should be responsible for ensuring compliance of their agents. These views were reiterated during private sector engagement in April 2022. Some of the attendees at the workshops considered there should be no prescribed requirements for agents at all, noting that the general law agency applies and enables an agent to undertake any function. Attendees also noted the need to distinguish between outsourcing providers (which may act as an agent) and broader agency relationships.

631. Overall, we agree the functions and circumstances in which agents may be used should be clarified. However, in the short term we do not consider it necessary to prescribe these requirements in regulations or the Act. Instead, we recommend issuing guidance to assist businesses in understanding the different types of agents and the ways they can be used to undertake AML/CFT functions. We also consider there should be clarity for businesses regarding their responsibilities when they rely on an agent. We therefore recommend issuing regulations to require a business to have PPCs for the AML/CFT functions that an agent undertakes on its behalf. There should also be PPCs for the vetting and training of agents and a requirement to maintain a list of agents that the AML/CFT supervisor can access upon request.

632. For the longer term, we recommend conducting further analysis to consider whether this guidance and prescribed programme requirements are effective to mitigate the risks associated with use of agents. If not, we recommend considering further regulations or legislative amendments in the future. We make additional recommendations specific to the use of agents in the MVTS sector (*see* Money or value transfer service providers).

Recommendations

R96. Request the AML/CFT supervisors develop guidance to clarify the different circumstances and types of agents that can be used by reporting entities under the Act.

R97. Require a reporting entity to do the following by issuing regulations:

- include PPCs in its AML/CFT programmes for training and vetting of agents.
- include PPCs in its AML/CFT programmes for all AML/CFT functions undertaken by an agent on its behalf (including identifying grounds under section 31(2)(b) for reporting a SAR).
- maintain a list of its agents (as part of its AML/CFT programme). The list of agents must be provided to the AML/CFT supervisor on request.

R98. For the longer term, if these recommendations do not provide sufficient clarity or effective controls regarding the use of agents, consider if further regulations or amendments to the Act are required. For example, this could define and explicitly prescribe the different AML/CFT functions that an agent is able to undertake for a reporting entity and liability for compliance.

5.3. Offences and penalties

633. A comprehensive and effective offence and penalty regime is necessary for ensuring good regulatory outcomes and that businesses comply with their obligations. Supervisors need to be able to respond to non-compliance when it is detected and impose penalties that are proportionate and dissuasive to influence decision making within businesses. In particular, enforcement action should encourage compliance and not be factored into the cost of doing business.

5.3.1. Comprehensiveness of penalty regime

634. The Act allows for a range of penalties to be imposed for non-compliance. Supervisors can impose civil sanctions, including issuing formal warnings, accepting enforceable undertakings, seeking injunctions from the High Court, and applying for pecuniary penalties. In addition, businesses which knowingly or recklessly engage in non-compliance can be prosecuted and held criminally liable.

635. Overall, the AML/CFT supervisors make use of the full range of sanctions and penalties available in the Act, but primarily make use of public or private formal warnings in most cases of non-compliance, with enforceable undertakings and High Court injunctions seldom used. In addition, pecuniary penalties can only be imposed following a resource-intensive court process and the ultimate penalties imposed may not be in proportion to the seriousness of the breaches. Further, the FATF considered that the penalty framework in the Act is not sufficiently comprehensive in that it does not enable proportionate, effective, and dissuasive penalties in every instance. In addition, we have identified areas where there is no corresponding offence for conduct which we consider should be criminalised.

Range of offences in the Act

636. We identified several areas where the Act is not able to effectively respond to specific conduct of concern. In particular:

- **failing to assist or obstructing the FIU:** there is an offence for failing to assist or obstruct a supervisor (sections 102 – 103), but these do not apply where the FIU makes a request under section 143 for a reporting entity to provide all records, documents, or information relevant to a SAR or PTR the FIU has received. As such, a reporting entity would face no consequences under the Act if they failed to comply or provided false information to the FIU.

- **structuring legal persons and arrangements or obligations:** the Act currently makes it an offence to structure a transaction to avoid the application of AML/CFT requirements. However, this does not cover people structuring legal persons or arrangements to avoid beneficial ownership requirements, nor does it cover people structuring non-transaction-based obligations (e.g., providing false identity documents to defeat CDD requirements).

637. We recommend amending the Act to include offences that respond to this conduct. Specifically, we recommend introducing an offence for a reporting entity to wilfully obstruct the FIU in the exercise of its powers or under the Act or knowingly provide false or misleading information following a request under section 143. These offences should have penalties in line with the penalties which exist for sections 102 and 103, as set out in section 105.

638. We note that the existing structuring offence is a strict liability offence, meaning that the prosecution does not have to prove that the person intentionally, knowingly, or recklessly structured the transaction to avoid AML/CFT obligations. As such, we consider that the existing structuring offence should be expanded to hold people strictly liable where they structure their compliance with any non-transaction-based obligation to avoid application of the Act. However, we consider that a separate offence should be created to cover where someone knowingly or recklessly structures a legal person or arrangement to avoid

beneficial ownership requirements. These offences should apply to any person, not just reporting entities.

Recommendations

R99. Create new offences for reporting entities obstructing the FIU (consistent with section 102) or knowingly or recklessly providing the FIU with false information (consistent with section 103) following a request under section 143.

R100. Amend the structuring offence in section 101 to include structuring any non-transaction-based AML/CFT obligations (e.g., using a false identity or other document to avoid AML/CFT obligations).

R101. Create a new offence for knowingly or recklessly structuring a legal person or legal arrangement to avoid or obstruct inquiries into the beneficial ownership of the legal person or arrangement.

Allowing for intermediary enforcement options

639. The Act does not currently provide the ability for AML/CFT supervisors to respond to moderately serious non-compliance efficiently and appropriately, i.e., conduct that is more serious than should be responded to with a formal warning, but not sufficiently serious to warrant an injunction or pecuniary penalties. There are two broad options for how the Act could be amended to increase the range of intermediary enforcement options, which are not mutually exclusive:

- **create an infringement offence regime:** AML/CFT supervisors could have the ability to issue infringement notices for non-compliance that is straightforward to identify and where a "one size fits all" approach can be taken. For example, notices could be issued for administrative matters (e.g., where businesses do not submit annual reports on time) or straightforward but nonetheless moderately serious non-compliance (e.g., failure to have an AML/CFT programme).

- **allow for the restriction, suspension, or cancellation of a licence or registration:** supervisors could be empowered to restrict a reporting entity's licence or registration as a response to non-compliance. This could be the AML/CFT registration or licence for those businesses required to be registered or licensed under the Act (*see* Licensing and registration) while for other businesses it would be their existing prudential licence or registration, e.g., a licence issued by FMA under the *Financial Markets Conduct Act 2013*.

640. Submitters were split on whether there should include additional intermediary enforcement options, with slightly more opposed to the proposal than in support. Some submitters were in favour of reporting noncompliance to professional bodies and forcing businesses to cease business activity. Submitters also noted that there would need to be monitoring for situations where there is an aggregation of fines as this could indicate more serious compliance deficiencies.

641. We conducted further targeted engagement on this issue in April 2022, where attendees at engagement workshops indicated they were broadly comfortable with an infringement scheme being developed but urged caution about impacting a business' licence or registration for non-compliance with the Act. Attendees noted that the seriousness of restricting, suspending, or cancelling a registration or licence would depend on the sector and that the option must only be used appropriately.

642. We recommend amending the Act to allow for infringement notices to be issued as well as for a registration or licence in appropriate instances of non-compliance with AML/CFT requirements. International experience has demonstrated that these enforcement tools can be effective at driving compliance across sectors and appropriately and proportionately to non-compliance. This change would also address one of the FATF's primary concerns about New Zealand's AML/CFT framework and help increase the overall effectiveness of

supervision. However, further engagement with other regulators[40] is required to ensure that the additional tools are appropriate, and that the overall regime is coherent.

Recommendations

R102. Amend the Act to enable infringement notices to be issued in appropriate circumstances (e.g., failure to provide annual report on time, failure to have an AML/CFT programme).

R103. Enable AML/CFT supervisors to restrict, suspend, or cancel a business' AML/CFT or prudential licence or registration (and/or request the relevant registration or licensing authority to do so) following AML/CFT non-compliance.

R104. As part of implementing Recommendation R103, agencies should conduct further engagement with the relevant agencies and bodies which are responsible for maintaining and administering the regimes under which reporting entities are licensed or registered to ensure that the overall regulatory regime is cohesive and coherent.

Allowing for higher penalties at the top end of seriousness

643. The Act provides for civil pecuniary penalties and criminal penalties for serious non-compliance. Businesses which breach their obligations in a continuous or serious manner can face penalties of up to NZD 2 million for civil penalties and up to NZD 5 million for criminal penalties. However, while these penalties are large in the New Zealand context, they may not be sufficiently proportionate or dissuasive for large businesses, including branches of multinational companies. Further, as was shown by the cost survey, the maximum penalties available may be less than what some businesses are spending on complying with the Act (*see* Cost of the regime).

644. We identified several options to ensure that proportionate penalties can be applied in all instances. One option would be to increase the maximum penalties available in the Act, which could be an absolute increase, or different maximum penalties prescribed depending on the size of the business or the relevant sector. Another option would be for the Act to specify that penalties may be individually applied to each instance of noncompliance, rather than on a representative or aggregate basis. Finally, the Act could allow for penalties to be a multiple of the profits the business made during the period of noncompliance, which would align with the approach taken with the offence of bribing a foreign public official (section 105C of the *Crimes Act 1961*).

645. Most submitters did not support increasing the penalties in the Act to account for serious breaches by larger and more complex businesses, noting that increasing the penalties has the potential to further marginalise certain sectors (e.g., remitters). However, some submitters considered there should be higher penalties and that size or annual turnover should be important considerations when determining penalty. Submitters also noted the current penalties do not align with international practice and are unlikely to exceed the cost of compliance for some businesses.

646. We conducted further targeted engagement on this topic April 2022. Attendees at the engagement workshops agreed that penalties are not proportionate for some businesses but are for the vast majority of businesses with AML/CFT obligations (which are typically small to medium enterprises). Attendees noted the need to ensure proportionately, and that small businesses do not face significantly increased penalties as a result of any changes. Of the various options, attendees generally preferred increasing the penalties overall, rather than applying penalties per instance of non-compliance or on the basis of profit during the period of non-compliance.

647. We recommend amending the Act to increase the maximum penalties to ensure they are proportionate and effective considering the size or nature of the business involved. Primary consideration should be given to prescribing different maximum penalties depending on the

[40] These other regimes are those established by the *Reserve Bank Act 1989, Insurance (Prudential Supervision) Act 2010, Financial Markets Conduct Act 2013, Gambling Act 2003, Lawyers and Conveyancers Act 2006, New Zealand Institute of Chartered Accountants Act 1996, Real Estate Agents Act 2008,* and *Secondhand Dealers and Pawnbrokers Act 2004*,

size or type of business involved. Subject to further analysis, we consider this approach would provide the greatest discretion to the judiciary and regulators and incentivise compliance with the Act.

Recommendation

R105. Amend the Act to increase available penalties ensuring they are able to be proportionate to the level of non-compliance and appropriate to the size or nature of the business. This could be achieved by increasing the maximum penalties available or prescribing different maximum penalties depending on the size or the type of business.

Ensuring penalties are risk-based and proportionate

648. There are no requirements in the Act to ensure that the enforcement action or penalty imposed by the AML/CFT supervisor or court or is proportionate (other than requirements in the *Sentencing Act 2002)*. This means that enforcement decisions or penalties may not appropriately consider the gravity and the duration of a breach of the Act, including whether there are mitigating factors such as reliance in good faith on advice of a consultant. Several attendees at targeted engagement workshops we ran in April 2022 agreed the application of enforcement measures and penalties should be more risk-based and applied more proportionately.

649. To ensure that that penalties are risk-based and proportionate, we recommend amending the Act to prescribe a non-exhaustive list of aggravating and mitigating factors that the supervisor or judiciary must consider when making enforcement decisions or imposing a penalty. In particular, the supervisor or Court should be required to consider the gravity and duration of the breach, the extent of any reliance on advice provided to the business in good faith, whether there have been previous breaches, and the impact of the breach on the broader AML/CFT system.

Recommendation

R106. Amend the Act to prescribe a non-exhaustive list of AML/CFT-specific aggravating and mitigating factors that need to be considered when applying penalties, such as the gravity and duration of the breach, compliance history, the extent of any reliance on advice in good faith, and a consideration of the consequences of the breach on the broader AML/CFT system.

5.3.2. Sanctions for employees, directors, and senior management

650. The FATF noted that criminal sanctions can apply to directors and senior managers of reporting entities in New Zealand, but not civil sanctions (unless the reporting entity is a partnership). [41] Enabling civil sanctions to be applied to directors, senior managers, and other relevant people could ensure that the individuals responsible for compliance decisions or governance are held accountable for non-compliance that occurs. This would also avoid penalties being factored into the cost of doing business or being paid indirectly by a business' shareholders or customers. Furthermore, the Act does not currently allow for penalties to be applied to agents of a business where they have not complied with the Act, as the principal is typically liable for the conduct of its agent.

651. Most submitters were opposed to extending sanctions to include directors and senior managers and urged caution noting that this change would risk increasing the difficulty in finding people who are willing to be directors or senior managers and negatively impact insurance availability and affordability. Some submitters also indicated there are already sufficient incentives to comply such as avoiding reputational damage or existing director liability frameworks. That said, some submitters thought sanctions should be extended to

[41] *R v QF, FC and JFL* [2019] NZHC 3058

directors and senior managers and noted that liability should only apply to people who were ultimately responsible for making the decision and that penalties should only apply in instances of gross negligence rather than technical non-compliance. In addition, submitters noted that insurance should be available or any restrictions on insurance or indemnification appropriately prescribed.

652. Several attendees at targeted engagement workshops in April 2022 noted the need for caution as to extending sanctions to directors or senior managers noting that it should be applied in limited circumstances where there has been serious wrongdoing. Others noted that extending liability to directors and senior managers can also help change the compliance culture within organisations, especially when they are relatively new to the regime. Some noted challenges to changing the culture within DNFBPs and getting senior managers and directors to take their new obligations under the Act seriously and implementing appropriate compliance programmes.

653. We recommend amending the Act to extend civil sanctions to directors, senior managers, employees, and agents in appropriate circumstances, such as where they were responsible for making the decision(s) that resulted in non-compliance with AML/CFT obligations. However, we consider that compliance officers should have a statutory defence where they have acted in good faith, but the reporting entity has not complied with relevant AML/CFT obligations. As part of making this change, agencies should consider international and legislative design best practices, as well as ensuring consistency with other relevant regimes (such as the *Credit Contracts and Consumer Finance Act 2003).*

654. In line with the concerns raised by submitters, we consider that sanctions for directors, senior managers, and employees should be reserved only for serious (rather than administrative) instances of noncompliance. For example, it would be more appropriate to impose civil liability where a business has failed to sufficiently establish or implement its compliance programme, but less appropriate where a business fails to submit an annual return on time. Extending civil liability in this way is consistent with other regulatory regimes, is international best practice, and will help ensure that businesses take their obligations seriously.

Recommendations

R107. Extend civil sanctions to directors, senior managers, employees, and agents in appropriate circumstances, such as where they were responsible for making the decision that resulted in the business not complying with their AML/CFT obligations.

R108. Provide a statutory defence for compliance officers where they have acted in good faith, but the reporting entity has not complied with their AML/CFT obligations.

5.3.3. Time limit for prosecuting AML/CFT offences

655. Sections 99 and 104 of the Act state the limitation period for prosecuting an offence under the Act is three years after the date on which the offence was committed. While this is in line with the potential penalty of two years imprisonment, it does risk some conduct going unpunished because too much time has elapsed; this also limits the range of enforcement actions that supervisors can take to address AML/CFT non-compliance. There can be significant delay between the offence occurring and this being detected by the supervisor.

656. Most submitters supported changing the timeframe, noting it should align with other obligations such as record keeping obligations or tax legislation. Other submitters suggested the timeframe should be between six months or a year up to seven years. Accordingly, we recommend extending the time limit for prosecuting AML/CFT offences from three years to seven years. This change will ensure AML/CFT supervisors have sufficient time to escalate their response to a breach of the Act, including prosecuting a business where appropriate. In addition, we note that businesses have an obligation to keep records for five years (which we recommend increasing to seven years – *see* Recommendation R147); as such, the AML/CFT supervisors may identify noncompliance through examining historical records but after three years have already elapsed.

Recommendation

R109. Extend the time limit for prosecuting AML/CFT offences from three years to seven years.

5.3.4. Liquidation following non-payment of AML/CFT Penalties

657. Unlike RBNZ and FMA,[42] the DIA does not have the power to apply to a court to liquidate a business to recover penalties and costs obtained in proceedings undertaken under the Act. We considered whether DIA should have this power. Most submitters supported the proposal, with only a small number opposed. As such, we recommend amending the Act to clarify all supervisors' standing to recover pecuniary penalties and costs awarded in AML/CFT proceedings. This will ensure that the DIA has the same powers as RBNZ and the FMA to apply to liquidate a company that has not paid a pecuniary penalty. To align with other enactments permitting recovery of pecuniary penalties, we also recommend requiring that the AML/CFT supervisor's actual costs in bringing the proceedings be paid first.

Recommendations

R110. Amend section 132(2) to clarify supervisors' standing to recover penalties and costs awarded in proceedings undertaken under the Act.

R111. As part of the above amendments, make a consequential change to section 241(2)(c) of the *Companies Act 1993* to include "if the company is a reporting entity under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, the AML/CFT supervisor for the company."

R112. Include a new section 90A of the Act to align with the approach to recovery of penalties to that of other enactments permitting the recovery of pecuniary penalties and state "if the court orders that a person pay a pecuniary penalty, the court must also order that the penalty must be applied first to pay the AML/CFT supervisor's actual costs in bringing the proceedings."

5.3.5. Minor changes to offences and penalties

658. We recommend making the following minor changes to the offence and penalty framework:

Issue	Recommendation
AML/CFT supervisors can issue a formal warning for failure to comply with AML/CFT requirements. However, naming this a "formal warning" does not necessarily carry the intended weight with the sector.	Include "formal warnings" in addition to "censure" as an option for responding to non-compliance.
There are two civil liability acts not explicitly included in section 78 of the Act. These are 1) failing to submit a suspicious activity report; 2) failures in respect of a risk assessment.[43] It is also currently unclear whether 3) failing to submit an annual report to an AML/CFT supervisor is a civil liability act.	Amend section 78 to include all specific compliance breaches as civil liability acts

[42] Section 241(2)(c) states a liquidator may be appointed by the court, on the application of the FMA if the company is a financial markets participant and on the application of RBNZ if the company is a licensed insurer.

[43] *Department of Internal Affairs v Ping An Finance Group New Zealand Company Limited* [2017] NZHC 2363, at [5]; *Department of Internal Affairs v Qian Duoduo Limited* [2018] NZHC 1887, at [3].

CHAPTER 6

Preventive measures

Summary

659. This chapter considers and makes a large number of recommendations regarding the obligations that businesses have in the Act in order to prevent or mitigate the risk of being misused for money laundering or terrorism financing. Effective preventive measures should be informed by and reflect an understanding of money laundering and terrorism financing risks and ultimately protect businesses from harm. However, AML/CFT obligations also impose significant and sometimes disproportionate compliance costs on businesses, particularly where they are not imposed in an efficient way or do not allow for innovative approaches to be taken.

660. We make a number of recommendations regarding customer due diligence (CDD) obligations which we anticipate will ease compliance costs and frustrations for businesses as well as support a more risk-based approach being taken. For example, we recommend reviewing and updating the Identity Verification Code of Practice to reflect the Digital Identity Trust Services Framework (once enacted), issuing regulations to exempt all businesses from the requirement to verify address information except where enhanced CDD is required, and also issuing regulations to relaxing the requirement to conduct enhanced CDD for customers which are trusts. We also recommend issuing regulations to clarify the definition of a beneficial owner, expanding what information needs to be collected about legal persons and legal arrangements, and expanding the range of measures that businesses can take to mitigate a customer which is higher risk. Finally, we recommend issuing regulations to provide further clarity for CDD obligations in respect of various non-financial activities.

661. We note that the Act's requirements with respect to Politically Exposed Persons (PEPs) were criticised by the FATF and do not reflect the risk in New Zealand. As such, for foreign PEPs, we recommend amending the definition of PEP in the Act, requiring businesses to have appropriate risk management systems in place to determine whether a customer is a foreign PEP and specifying that PEP checks should conducted at the appropriate time depending on the level of risk involved with the relationship. We also recommend that the definition of PEP should be amended to include domestic PEPs, given there have been several instances of public sector corruption and fraud observed while the Act has been in operation. However, we recognise that domestic PEPs are typically less risky than foreign PEPs and recommend lesser requirements for identifying and mitigating the risk of a domestic PEP compared with foreign PEPs.

662. The FATF also made a number of criticisms about the requirements regarding sending and receiving funds via a wire transfer. Given that wire transfer obligations are intended to prevent terrorists and other criminals from having unregulated access to international payment systems and to enable misuse to be easily detected, we make a number of recommendations for change that should be progressed through issuing regulations. In particular, we recommend introducing limited requirements to collect identity about the parties to an international wire transfers below NZD 1,000 as well as further obligations on intermediary and beneficiary institutions to detect and respond to incomplete wire transfers. However, we also recognise that terminology in the Act relating to wire transfers is outdated and needs considerable reform, and we recommend repealing and replacing the terminology in the Act in consultation with the private sector. We note that this would also provide an opportunity to resolve issues with prescribed transaction reporting (*see* Prescribed transaction reports).

663. We also make a series of recommendations regarding the provisions in the Act relating to reliance. Relying on a third party to conduct CDD is one of the main ways that businesses

can reduce their compliance obligations, particularly where a customer is in another country or where there are multiple businesses involved in a transaction or activity. We note that the Digital Identity Services Trust Framework and register of beneficial ownership for companies and trusts will likely reduce the extent to which CDD is duplicated across the regime and address issues raised by submitters. Nevertheless, we recommend continuing to explore the reliance provisions in the Act, including whether the "approved entity" scheme can ever be used and the provisions relating to reliance within a designated group of businesses.

664. New Zealand is exposed to global or international risks of money laundering or terrorism financing from other countries or transnational organised crime groups: some of these countries have been publicly identified by the FATF as being high risk, but other customers from countries should also be considered in appropriate circumstances. We recommend updating existing guidance to provide further detail about dealing with other countries to ensure a more nuanced and risk-based approach can be taken by businesses, and also recommend issuing regulations to clarify how to deal with countries which are on the FATF's greylist or blacklist. However, some countries are so risky that further countermeasures are justified, and as such, we recommend issuing regulations to mitigate the risk posed by Iran and the Democratic People's Republic of Korea. We also recommend amending the Act to ensure a sufficiently broad range of countermeasures can be imposed if required, which should include exploring the feasibility of issuing countermeasures against specific transnational crime groups to combat the threat those groups pose to New Zealand.

665. Finally, we also make a number of more minor recommendations relating to record keeping, correspondent banking, money or value transfer services, the use of new technologies, and internal controls. These recommendations include further clarifying and reconciling record keeping obligations to align with the *Privacy Act 2020*, updating requirements for correspondent banking relationships, requiring businesses to conduct a risk assessment before using a new technology or product, and providing businesses with the option of having a compliance officer as a senior manager in the business. We also recommend amending the Act to ensure that groups of businesses develop programmes to mitigate their group-level risks, and agencies further explore what obligations should be developed to support the implementation of targeted financial sanctions obligations.

6.1. Customer due diligence

666. Customer due diligence (CDD) is a cornerstone of the AML/CFT regime. Knowing who a customer is, verifying any information provided and understanding their risk profile protects businesses from misuse. Developing a clear understanding of why a customer is forming a particular relationship also enables businesses to properly detect unusual or potentially suspicious behaviour.

6.1.1. Verifying customer due diligence information

Identity Verification Code of Practice (IVCOP)

667. Verifying the name and date of birth of customers, beneficial owners of customers and persons acting on behalf of customers is a core CDD requirement. It protects against business relationships being established anonymously or under a false identity and helps to assess the level of risk associated with a person. The current Amended Identity Verification Code of Practice (IVCOP) for this requirement was issued by the AML/CFT supervisors in 2013. If adhered to, it provides a 'safe harbour' to businesses for the verification of their low and medium risk customers.

668. We considered whether the IVCOP was still fit-for-purpose or whether it should be replaced or changed. We noted that the establishment of the Digital Identity Services Trust Framework could assist businesses meet AML/CFT obligations and be used with any new code of practice. The Trust Framework is scheduled for enactment in 2024.

669. Most submitters considered that the IVCOP should be reviewed and updated, with some suggesting it be discarded entirely. Submitters identified Issues with all parts of the IVCOP, including face-to-face verification and the use of copies of documents certified by the trusted referees. There were particular concerns in relation to the IVCOP's electronic identity verification (EIV) provisions which submitters considered unclear. Some submitters also suggested there be a different level of verification requirement for low, medium, and high-risk persons respectively (noting the latter category are not currently subject to the IVCOP)These views were reiterated in the private sector consultation in April 2022.

670. We agree that the IVCOP requires review and should be replaced. There are two options for this:

- request the AML/CFT supervisors review and update the IVCOP as an immediate priority. If this option is progressed, we note a further review and update may then be required once the Trust Framework is enacted.
- request the AML/CFT supervisors commence work on reviewing the IVCOP and in relation to EIV, this should occur in conjunction with the development of the Trust Framework.

671. Overall, our preference is the second option. We recommend a full review of the IVCOP across all the identified issues, including the different verification options, risk-based requirements and to align with the Trust Framework. This option will be more efficient for businesses ultimately as their name and date of birth verification procedures may only need to change once.

Recommendation

R113. Request the AML/CFT supervisors review and replace the IVCOP with a new code of practice setting out best practice verification requirements in relation to name and date of birth. This should review provisions for face-to-face verification, use of certified copies and electronic identity verification. The review and implementation of the new code of practice should be completed by and aligned with the implementation of the Digital Identity Services Trust Framework.

Verifying address information

672. One of the Act's current requirements is to verify the address of a customer, a beneficial owner of a customer or a person acting on behalf of a customer. Address verification was included as a measure to ensure accuracy of a person's identity information as well as further enabling transactions to be traced around the economy and thereby support law enforcement investigations. We noted that most countries do not have this requirement and identified a range of challenges with the verification requirement. This includes negative impact on financial inclusion and disproportionate compliance costs.

673. We considered the compliance burden that this requirement places on businesses and examined opportunities to reduce it. We identified several options for changing the current address verification requirements:

- **the requirement to verify address could be removed or reduced:** the requirements could be removed for all or some types of persons (i.e., natural persons, legal persons or legal arrangements), or required only in high-risk situations
- **an alternative approach to verifying address could be prescribed:** businesses could instead be required to take reasonable steps, according to the level of risk involved, to verify that the address provided is a genuine address. For example, by using the NZ Post address finder system.

674. Almost all submitters supported removing or reducing address verification requirements. Many questioned its usefulness for combatting money laundering or terrorism financing and others highlighted the disproportionate compliance cost. There was less support for the alternative option of verifying that an address was genuine. This was viewed as

unnecessary and potentially problematic for persons outside of New Zealand. This view was also expressed during private sector engagement in April 2022.

675. Overall, we agree with industry feedback and recommend significantly reducing address verification requirements through issuing regulations in the short term. Doing so will enable businesses to better deploy their finite compliance resource to other AML/CFT obligations and take a more risk-based approach. However, we also consider that a requirement to verify a person's address is useful in some higher risk circumstances to deter criminals from providing a false address and support law enforcement investigations. Accordingly, we recommend continuing to require address information to be verified in high-risk circumstances (i.e., when enhanced CDD is triggered). For other standard CDD circumstances, we recommend further analysis to determine if there is benefit in requiring businesses to verify that an address is genuine in some circumstances. If so, this requirement should be introduced.

676. We also note that for customers that are legal persons or legal arrangements with complex ownership structures, establishing where the registered office or the location or place of business may be useful as part of the wider CDD process. In addition, we note the FATF Standards require address information to be verified for legal persons or legal arrangements as one of the CDD requirements. Given that address information must still be obtained, and the verification requirement remains in enhanced CDD situations, we consider any adverse impact on compliance with the FATF Standards to be negligible.

Recommendation

R114. Issue regulations to exempt the address verification requirement for all customers, beneficial owners and persons acting on behalf of a customer other than when enhanced CDD is required. As part of this process, and for customers requiring standard CDD, consider whether regulations should be introduced requiring businesses to verify an address as genuine according to the level of risk. These changes should then be amended in the Act itself.

Unavailability of independent verification sources

677. A fundamental requirement of the Act is that verification is undertaken using data, documents, or information from a reliable and independent source. This ensures it is accurate. However, there are some limited circumstances where documents from independent sources simply do not exist. Primarily this arises with documents that are privately held, such as relating to legal arrangements, company constitutions or nominee arrangements. In some circumstances, it may also arise in relation to a person's address.

678. We considered the extent to which this posed compliance challenges for businesses and whether some concessions could be made. Submitters acknowledged these issues and were supportive of amendments. Overall, we consider that the use of reliable and independent sources should remain the status quo. However, we recommend issuing regulations to provide an alternative option in situations where data, documents or information from an independent source is not available. In those instances, businesses should be required to use data, documents or information that is reliable (but without a requirement that it be independent). This could be accompanied by guidance from supervisors regarding use of these provisions.

Recommendation

R115. Issue regulations stating that in circumstances when it is not possible to verify required information regarding legal persons or legal arrangements from a reliable or independent source, it is possible to use reliable (but not independent) verification data, documents, or information. This does not apply to biographical information or information regarding source of wealth or source of funds.

6.1.2. Identifying the beneficial owner

679. Understanding underlying ownership or control of legal persons or legal arrangements is another core requirement of the Act. This helps ensure that criminals and terrorists do not use legal persons or arrangements to obscure their involvement in transactions, activities, or ownership of assets.

Definition of beneficial owner

680. The current definition of beneficial owner poses challenges for businesses and the regime overall. It does not include a person with "ultimate ownership or control". This may lead to certain persons not being identified as beneficial owners that should be, which means that businesses may not fully appreciate the risks associated with the customer. Conversely, both limbs of the definition include a person on whose behalf a transaction is conducted (POWBATIC). This may result in other persons being caught by the definition unnecessarily such as customers of customers and significantly increases compliance costs for businesses.[44]

681. We considered whether the current definition of beneficial owner should be amended, and if so how. Submitters mostly agreed that improvements are required to clarify who meets the criteria for beneficial owner. Some submitters noted this would avoid the need for over-compliance and in turn, lead to cost savings and a more risk-based approach. However, there were a wide range of views on what could be done. Some submitters suggested having more prescription, such as prescribing all persons that should be identified as beneficial owners of a legal arrangement (and all persons, such as settlors or protectors of trusts). Other submitters suggested less prescription and focussing on a risk-based approach regarding the level of verification required. These views were reiterated during private sector engagement in April 2022.

682. Despite the range of views outlined above, there was broad support for the following options which could be implemented through issuing regulations:

- **clarifying the definition of a beneficial owner**, in particular that it includes a person with "ultimate ownership or control". This will ensure there is an explicit requirement to identify and verify all persons that meet the criteria for beneficial owner. This could also include clarifying that POWBATIC meets the criteria for beneficial owner only in circumstances where they exercise indirect ownership or control of a customer. If we did this, a business would only have direct obligations in relation to a customer of a customer in those situations where enhanced CDD was required.

- **amending the ownership threshold** in Regulation 5 of the *AML/CFT (Definitions) Regulations 2011* from "more than 25%" to "25% or more" to ensure that a quarter ownership meets the criteria. This also aligns with the FATF Standards.

683. We could also revoke existing class and regulatory exemptions (specifically Parts 4 and 5 of the *AML/CFT (Class Exemptions) Notice 2018* and Regulation 24 of the *AML/CFT (Exemptions) Regulations 2011*) if these changes were made as they would be redundant once the role of the POWBATIC is clarified.

Beneficial ownership register(s)

684. Many submitters considered the steps currently being taken by MBIE to develop and implement a beneficial ownership register (for legal persons) had important implications for AML/CFT obligations. Submitters strongly supported ensuring businesses had access to the register and that opportunities to use it for AML/CFT purposes were maximised.

[44] This is the interpretation taking in the beneficial ownership guideline issued by supervisors in 2012. This interpretation also led to the introduction of the Managing Intermediaries Exemptions (*see AML/CFT (Class Exemptions) Notice 2018*) and *Regulation 24 AML/CFT (Exemptions) Regulations 2011* relating to trust accounts.

685. Several submitters also suggested that a similar register be developed for trusts and other legal arrangements. Submitters considered that a register with some information accessible by businesses would similarly provide significant cost savings and efficiencies, as well as generally improve the ability for agencies to understand the risks posed by trusts and other legal arrangements in New Zealand.

Consideration of beneficial ownership register for trusts

A register of beneficial ownership for trusts was considered and ultimately rejected by the Law Commission in 2013 during their review of the Law of Trusts (Law Commission Review of the Law of Trusts (NZLC R130, 2013) at chapter 18). The Law Commission's primary concern was that a register of trusts would significantly alter the nature of trusts by giving them a publicly registered status. This would be a departure from the current treatment of trusts as essentially private arrangements between citizens. The Law Commission also queried whether the "problems" with trusts were truly problems or whether the privacy and confidentiality of a trust are fundamental for how a trust operates. The Law Commission also noted that the costs of registration would be significant and would ultimately not be the best approach to improving accountability of trustees to beneficiaries.

While the Law Commission's reasoning and concerns are understandable, the landscape has significantly shifted since 2013 which justifies this topic being examined again. In particular:

- the Panama, Paradise, and Pandora Papers have been published by the International Consortium of Investigative Journalists in 2016, 2017, and 2021 and identified trusts registered in or associated with New Zealand as being involved in illicit financial activity.
- following the Shewan Report in 2016, Inland Revenue developed and implemented a register of foreign trusts which resulted in the number of foreign trusts associated with New Zealand decreasing by 75 percent (from 12,000 to 3,000 in 2020).
- Inland Revenue has also increased its collection of tax information from trusts which generate a taxable income, and now requires trustees to disclose significantly more detail about the parties to the trust on an annual basis.
- the FATF found that New Zealand was only moderately effective at ensuring the transparency of legal persons and legal arrangements and recommended New Zealand take proactive steps to improve the transparency of express trusts, including considering a register of trusts.

However, despite the above, we note that implementing a register for trusts would likely involve amendments being made to the *Trusts Act 2019* rather than amendments to the Act.

Use of beneficial ownership registers for AML/CFT requirements

686. Overall, we consider that beneficial ownership registers offer significant potential benefit to businesses to assist in meeting AML/CFT obligations. These could significantly increase the efficiency of CDD processes, providing reliable and independent information that can be leveraged by reporting entities and reduce duplication.

687. For trusts and legal arrangements, a register would also improve the ability for agencies to understand and assess the risks of trusts, compliment recent policy changes made by Inland Revenue and align with MBIE's ongoing work regarding companies and limited partnerships. We consider that a register is not incompatible with the private and confidential nature of trusts. A register would not need to make public all the information about the trust or may not need to be publicly accessible at all, to achieve the identified benefits.[45]

688. Consequently, we make several recommendations relating to beneficial ownership. In relation to the development of a beneficial ownership register for legal persons, there should be coordination with MBIE to ensure that the definition of beneficial owner aligns

[45] For example, a register may only make public the existence of the trust and the identity of one of the trustees. More information about the trust (e.g., the identity of the settlor, beneficiaries, or protector) could be made available to reporting entities upon request and potentially following payment of a fee, with only law enforcement agencies able to access all the information on the register for law enforcement purposes.

with the Act. Further work should be undertaken to consider potential use (and reliance) on the register by businesses to meet AML/CFT obligations. In relation to trusts and other legal arrangements, we recommend agencies undertake further work to explore the feasibility of a register, and in turn, how this could also be leveraged to assist businesses to meet AML/CFT obligations.

689. While the above recommendations are in progress, we also recommend that some clarifications should be made in the interim through issuing regulations (as per paragraph 682). This will ensure that those persons intended to meet the criteria for beneficial owner are identified and verified, while at the concurrently reducing a need for over-compliance for persons that should not be considered beneficial owners.

Recommendations

R116. Review and amend the definition of beneficial owner in the Act. This should include coordination with MBIE and alignment with the definition to be used for the beneficial ownership register for legal persons. As part of this process:

- Ensure the definition applies to persons with ultimate ownership or control, and only applies to POWBATICs if they exercise indirect ownership or control over the customer.
- Consider whether there is a need to also prescribe certain types of persons who must be identified/verified for legal arrangements (e.g., settlors or protectors of trusts, nominees in relation to legal persons).
- Review the potential use of the beneficial ownership register by reporting entities to meet AML/CFT requirements. This includes identifying those low-risk situations where reporting entities may be able to rely wholly on the register compared to situations where additional beneficial ownership verification may be required.

R117. Concurrent to the above, agencies should undertake further work to explore the feasibility of a register of beneficial ownership of trusts and legal arrangements. This should include consideration of use of the register for reporting entities to assist meeting AML/CFT obligations in relation to trusts and legal arrangements.

In the interim:

R118. Issue regulations to clarify that the definition of beneficial owner includes a person with ultimate ownership or control, and only applies to a POWBATIC that meets this threshold, whether directly or indirectly.

R119. Revoke Regulation 24 (Exemptions) in relation to trust accounts.

R120. Review whether the Managing Intermediaries Exemptions remain necessary and amend or revoke if they are not.

6.1.3. Specific information for legal persons and legal arrangements

690. Due to the potential use of legal persons and arrangements to mask criminal activity, we could explore options to ensure that businesses understand the legal structures of their customers. This is consistent with the FATF Standards that require businesses to understand the nature of the customer's ownership and control structure, and to obtain and verify its legal form and proof of existence and powers that bind and regulate (e.g., understanding voting rights or founding documents setting out how the legal person or arrangement can operate).

691. We considered whether these requirements should be included in the Act. Submitters were split on the proposal, with roughly half supportive and half opposed or concerned about the proposal. Those in favour advised they were already obtaining this information, and that mandating its collection would ensure a consistent approach across industry and bring New Zealand in line with the FATF Standards. Those against were concerned about potential compliance costs and the level of prescription this would bring. Others supported a requirement to obtain this information but not to verify it.

692. Overall, we recommend issuing regulations to require businesses to obtain this information, with the level of verification only required according to the level of risk. This will ensure compliance costs are proportionate and that businesses could choose not to verify the information for simple legal structures or in low-risk situations.

Recommendation

R121. Issue regulations requiring reporting entities to obtain information about legal form and proof of existence, ownership and control structure, and powers that bind and regulate, and verify this information according to the level of risk. These changes should then be amended in the Act itself.

6.1.4. Obligations in situations of higher risk

Source of wealth or source of funds, additional enhanced CDD measures

693. Enhanced CDD is a key component of determining whether a high-risk customer, transaction or situation is suspicious, or whether activities appear high risk but can ultimately be established as legitimate. Under the Act's current settings, the enhanced CDD measures are limited to obtaining and verifying information regarding source of wealth or funds. There is no differentiation between the two. This means enhanced CDD efforts may not necessarily be directed at which of the two, or both, is most relevant to mitigate the risks.

694. Relatedly, the Act does not include options for implementing other enhanced CDD measures to mitigate risks. For example, in some situations, the examination of the purpose of a transaction may be particularly important. Other potential additional measures include obtaining further information from the customer, enhanced monitoring of a business relationship, or obtaining senior management approval for transactions or to continue a business relationship. These are all options identified in the FATF Standards.

695. We considered whether there should be a requirement to differentiate the circumstances in which the source of wealth versus funds was examined. We also considered whether businesses should be required to implement additional enhanced CDD measures, and in what circumstances.

696. In relation to source of wealth or funds, we identified several options:

- require an AML/CFT programme to differentiate between when a business must obtain and verify information regarding wealth versus funds, or both, dependent on what is required to mitigate the risks.
- prescribe the circumstances in which information regarding source of wealth or source of funds must respectively be obtained and verified. For example, wealth at commencement of a business relationship versus funds for a transaction within a business relationship, or for an occasional activity or transaction.
- issue a code of practice to differentiate between source of wealth and source of funds requirements, as well as undertaking enhanced CDD more broadly according to the level of risk.

697. In relation to other enhanced CDD measures, we also identified several options:

- require that in addition to source of funds or wealth requirements, additional measures must be implemented as are required to mitigate the risk.
- require that additional measures must be implemented, potentially including, but not limited to source of funds or wealth requirements, as are required to mitigate the risk.
- introduce more prescriptive requirements, such as requiring additional enhanced CDD measures at the start and throughout a business relationship as are required to mitigate

the risk. Alternatively, introduce requirements that information regarding the purpose of a transaction be obtained where the risk relates to the reason for a transaction.

698. Submitters identified a range of issues regarding verification of source or wealth of funds. These included challenges determining which to examine, how to examine them and the application of a risk-based approach. Most submitters supported clarity to addressing some of these challenges. Some submitters were cautious, advising that too much prescription poses challenges in itself.

699. Submitters broadly supported additional enhanced CDD measures, with some businesses advising that they had already adopted them. However, there were a range of views on how this should occur, with submitters generally split on whether this should be mandated or incorporated into guidance. Some submitters favoured less prescription, while others suggested a code of practice. Some submitters cautioned that too much prescription may lead to an overly burdensome compliance cost at odds with a risk-based approach. These views were reiterated in the private sector engagement in April 2022.

700. Overall, we acknowledge that too much prescription has the potential to cause challenges for businesses. However, we also consider it important that businesses apply the appropriate range of enhanced CDD measures as is necessary to mitigate their risks. Consequently, we recommend changes in two phases. For the longer term, we recommend introducing a range of enhanced CDD options to align with the purpose of the Act and best address the risks. This should include consideration of the role of source of wealth or funds verification as a part of enhanced CDD, and whether it should be mandatory or whether other available measures could be used as an alternative in some circumstances. In the interim, we recommend issuing regulations to improve the effectiveness of the enhanced CDD settings, without significant impact or cost to businesses.

Recommendations

R122. Review whether the current sections 23 and 24 enhanced CDD requirements are appropriate or require amendment. This should include consideration of whether businesses should be required to take further additional measures in addition to, or instead of, the current source of wealth or funds requirements in order to manage and mitigate the risk their customers present. As part of this, consider whether the Act should also be amended to differentiate between the requirement to obtain and verify source of wealth or source of funds as is required to mitigate identified money laundering and terrorism financing risks.

In the meantime:

R123. Issue regulations to require a business to differentiate when information must be obtained and verified regarding source of wealth or source of funds, or both, as is required to mitigate the risks.

R124. Issue regulations to require a business to implement any additional enhanced CDD measures at the start and for the duration of a business relationship as are required to mitigate the risks.

Mandatory enhanced CDD for all trusts

701. Currently, enhanced CDD is mandatory for all customers that are trusts or other vehicles for holding personal assets. Not all trusts or other vehicles for holding personal assets are inherently high risk, and as such, our current requirements are inconsistent with a risk-based approach and not required by the FATF Standards. The FATF recommended that we review our mandatory enhanced CDD requirements for trusts.

702. We considered whether allowing more risk-based flexibility regarding enhanced CDD requirements for trusts or other vehicles for holding personal assets may significantly reduce compliance burden without jeopardising the ability to mitigate risks. We identified several options:

- **repeal the relevant sections of the Act entirely** so that enhanced CDD is no longer mandatory for these types of customers. However, enhanced CDD would still be required if the business considered it was justified on the basis of risk.

- **retain the requirement to obtain information** on source of wealth or funds but remove the requirement to verify this information for certain types of lower risk trusts.
- **introduce more prescriptive requirements**, such as through regulations or a code of practice, setting out the process for conducting enhanced CDD and factors to consider when assessing the level of risk. If certain low-risk criteria are met, an exemption from verification requirements should apply or be minimal.

703. Most submitters supported removing the mandatory requirement for enhanced CDD and agreed that the majority of trusts with which they interact were not high risk. However, some submitters supported the status quo due to a perceived inherently higher risk compared to other categories of customer. Others noted that vehicles for holding personal assets no longer needed to be included given the changes in 2021 to requirements for nominee directors and shareholders. These views were reiterated in the private sector consultation in April 2022.

704. Overall, we consider that agencies should take steps to reduce and ultimately remove the mandatory enhanced CDD requirements for trusts and other vehicles for holding personal assets. Similar to the other enhanced CDD issues discussed above, we recommend a phased approach. For the longer term, we recommend reviewing whether the mandatory requirements can be removed entirely. In the interim, we recommend issuing regulations to exempt the requirement to verify source of wealth or funds information for low-risk types. We consider an exemption of this nature will reduce compliance without jeopardising the ability to mitigate risk.

Recommendations

R125. Review whether mandatory CDD remains necessary for all customers that are trusts or other vehicles for holding personal assets. If not, repeal sections 22(1)(a)(i) and 22(1)(b)(i) of the Act.

R126. In the interim, implement Regulations to prescribe a process for conducting enhanced CDD on trusts, including identifying types of trusts that are suitably low risk and other factors to consider when assessing the level of risk. If certain low-risk criteria are met, an exemption from verification requirements should apply. This should be accompanied by guidance from supervisors regarding a risk-based approach.

Conducting customer due diligence in all suspicious circumstances

705. There is currently a gap in the Act relating to transactions occurring outside of a business relationship, but under any applicable threshold to be captured as an occasional transaction. While these transactions are typically considered low risk, this is not always so. Notably, there are some types of high-risk or suspicious transactions that may only be relatively low value (e.g., where there is risk of terrorism financing or online child exploitation).

706. We considered whether we should close this loophole and asked what level of CDD should be required and in what circumstances. We noted that the FATF Standards require CDD to be conducted in all instances of suspicion. In general, submitters agreed a requirement for CDD in all suspicious circumstances is consistent with the overall aim of the Act and therefore worthwhile. However, there were mixed views on the level of CDD that should be required and how this could work in practice, particularly if the CDD requirement was to be triggered after the transaction.

707. We recommend introducing a CDD requirement to close this gap. The CDD requirement should be introduced only in those circumstances where there may be grounds to report a suspicious activity. We consider that the number of high-risk or suspicious transactions that occur outside a business relationship and below the threshold for CDD (as an occasional transaction) is likely to be very small. If it arises, this is most likely to be in the MVTS or VASP sectors. Accordingly, we do not consider there will be a significant impact on most sectors. Introducing the requirement when a person seeks to conduct a transaction (rather than after the transaction) will also minimise the practical challenges raised by submitters.

This also means carrying out the transaction would be prohibited, and a potentially serious crime prevented, if a business is not able to complete CDD.

Recommendation

R127. Issue regulations (pursuant to section 14(1)(d)) so that CDD must be conducted if a person seeks to conduct an activity or transaction through a reporting entity that is outside a business relationship and not an occasional transaction or activity. This obligation arises in any circumstances where there may be grounds to report a suspicious activity as per section 39A of the Act. These changes should then be amended in the Act itself, along with a prohibition on carrying out the transaction under section 37 if CDD cannot be completed.

Avoiding tipping off

708. Undertaking CDD (particularly enhanced CDD) is a key part of determining whether there are grounds to submit a SAR. This also ensures that any resulting report can be of the highest quality and use to law enforcement agencies. However, there is a risk that conducting CDD, particularly if it relates to a specific transaction or activity, could inadvertently 'tip off' the customer of a pending law enforcement interest in them (i.e., that a SAR is going to be submitted).

709. The FATF Standards acknowledge this risk. The standards anticipate that once suspicion has been formed and if there is a reasonable belief that conducting CDD would tip off the customer, a business should be able to undertake a lower level of CDD and instead submit a SAR. While our Act has strict prohibitions around disclosing the existence of a SAR, it does not contain the tipping off provisions anticipated by the FATF. The only exception to this is the narrow set of circumstances when a person is subject to an order issued under section 143(1)(a) or Production Order issued under the *Search and Surveillance Act 2012*.

710. We considered whether the Act should include provisions to align with the FATF Standards, sought views on tipping off risks more broadly and options to address it. We received a wide range of submissions, with some submitters agreeing that the conduct of enhanced CDD could tip off the customer. There was specific concern about section 22A of the Act, which triggers an enhanced CDD obligation after suspicion has been formed (for existing customers and customers conducting an occasional transaction/activity). Other submitters raised issues around staff safety if they had to conduct enhanced CDD in certain circumstances. Submitters also expressed a need for additional guidance about what might alert the customer to a potential law enforcement interest in them and how to avoid it.

711. We agree with submitters that section 22A of the Act poses challenges. We also note that section 22(1)(c) and (d) of the Act already apply to existing customers and persons conducting an occasional transaction or activity and in turn already provide triggers for enhanced CDD to be conducted in higher risk situations. We also agree that the relationship between enhanced CDD requirements and the risk of tipping off, as well as the prohibitions under section 37 of the Act, is one of nuance that needs to be carefully managed. We therefore recommend repealing 22A of the Act. We also recommend agencies undertake further analysis to determine whether a lower level of CDD should be permitted in some circumstances when suspicion has been formed. In the meantime, we recommend issuing guidance regarding enhanced CDD and its relationship with forming suspicion to ensure the current requirements of the Act are understood.

Recommendations

R128. Issue guidance around the use of enhanced CDD (s22(1)(c) and (d)) to assist in determining grounds for suspicion, the prohibitions under section 37 and the Act's tipping off provisions relating to the existence of a SAR, to ensure these requirements are understood by reporting entities.

R129. Repeal section 22A of the Act.

R130. Review the current circumstances in which a lower level of CDD is permitted to avoid alerting the customer to potential law enforcement interest. Consider if there are grounds to expand this, for example in relation to bank accounts in some circumstances.

6.1.5. Obligations in situations of lower risk

Eligibility for simplified CDD

712. Currently the Act identifies certain categories of customer as eligible for a simplified form of CDD. This is based on an assessment of a lower level of inherent risk associated with these customer types. The Act also contains provisions for certain types of transaction, or certain products and service, to be prescribed to require a lower level of simplified CDD. However, these provisions of the Act are not currently used as much as they could be (*see* Balancing prescription with risk-based obligations).

713. We considered whether the range of circumstances in which simplified CDD could be conducted should be expanded. Submitters broadly supported this proposal, with a few specific situations suggested. We recommend agencies undertake further analysis to determine further circumstances in which only simplified CDD is required. This could include additional categories of customer, or certain products and services more broadly, where the risk is sufficiently low to reduce and/or target AML/CFT requirements. This has the potential to reduce compliance cost for some businesses, without jeopardising the ability to mitigate the risks.

Recommendation

R131. Undertake a review to identify further categories of customer and any products or services where the money laundering and terrorism financing risk is sufficiently low to enable simplified CDD. Issue regulations to allow simplified CDD measures for these situations. These changes should then be amended in the Act itself.

Conducting simplified CDD on persons acting on behalf of large organisations

714. One particularly problematic aspect of the current simplified CDD provisions occurs when a customer may have various employees acting for it. One example of this is a large organisation with multiple employees authorised to undertake specified functions at any one time, such as within a contact centre. Currently, section 18(3) and sections 19-20 of the Act require the full name and date of birth of each individual employee to be identified and verified, along with their authority to act. This imposes significant compliance costs on both the organisation and any reporting entity conducting CDD, which is not justified by the risks associated with the relationship.

715. We considered streamlining this process and through allowing a senior manager to authorise employees to undertake certain functions, without necessitating the identity of each of those employees (including their date of birth) to be individually verified. Conditions could be attached to this such as only using approved contact details for the employee and restricting the scope of the authority to act. Submitters supported this proposal, and also considered that this should not be limited to large organisations. Other submitters raised challenges applying obligations to persons acting on behalf of customers more broadly. There was also a note of caution about ensuring the person was genuinely

acting on behalf of the customer, had authority to do so and could only act within the scope of this authority (to mitigate fraud or theft risk).

716. Overall, we recommend streamlining the CDD process for situations when there may be multiple persons acting on behalf of a customer by electronic means. To ensure risks are still mitigated, this should be conditional on a senior manager of the customer delegating authority to employees to undertake certain functions and providing their relevant contact details.

Recommendation

R132. Issue regulations enabling a senior manager of a customer (that has been identified and verified in accordance with sections 19-20) to delegate authority to employees to act on behalf of the customer by electronic means. The senior manager must provide the delegated employees' authorised contact details (e.g., email address) to the reporting entity, with the reporting entity then exempt identifying and verifying the full name and date of birth for those delegated employees. These changes should then be amended in the Act itself.

6.1.6. Ongoing customer due diligence and account monitoring

Risk-rating of customers

717. Many of the requirements of the Act are risk-based, in that they are required to be implemented according to the level of risk posed by the customer, transaction, or activity. A risk-based approach applies to the level of required verification of CDD information and the frequency and intensity of ongoing CDD and account monitoring.

718. In line with our general consideration of whether the Act strikes the right balance between being risk-based and prescriptive, we also considered how this applies to ongoing CDD. Specifically, the Act could require a business to risk-rate a new customer and consider or update this rating during ongoing CDD and account monitoring. This obligation could be accompanied by a requirement when on-boarding a new customer to consider any applicable guidance issued by the supervisor, e.g., a list of red flags or high-risk situations. During the private sector engagement in April 2022, various attendees advised they already risk-rate customers and consider this implicit to the Act's requirements.

719. Accordingly, we recommend issuing regulations to explicitly require businesses to risk-rate customers as part of CDD, including ongoing CDD. We consider that these requirements will assist and support businesses in navigating the Act's risk-based requirements. For those smaller businesses with less sophisticated compliance models, we anticipate this will better signpost the Act and enable them to understand and direct their resource at the areas of higher risk.

Recommendation

R133. Issue regulations to include an explicit requirement that reporting entities risk-rate new customers (including consideration of guidance issued by supervisors). This risk rating must then be considered and updated as part of ongoing CDD and account monitoring of a business relationship. These changes should then be amended in the Act itself.

Updating CDD information and account monitoring, including for existing customers

720. While businesses must review CDD information when undertaking ongoing CDD and account monitoring, there is no explicit requirement to update a customer's records during this process (outside of situations when enhanced CDD is triggered). Similarly, there is no explicit requirement to consider when CDD was last conducted. Without updating relevant customer records, businesses may not have a full understanding of their customer's identity and risk profile. This does not comply with the FATF Standards.

721. This issue arises for both existing (pre-Act) customers and for customers with whom business relationships were established after the Act took effect. Indeed, for existing customers for whom historical information may be extremely limited, the only explicit trigger occurs if there has been a material change in the business relationship and insufficient information is held (as per section 14(1)(c) of the Act). This is a high threshold to trigger CDD and was also identified by the FATF as a deficiency.

722. We considered whether these were vulnerabilities that should be addressed and looked at ongoing CDD and account monitoring requirements more broadly. For existing customers, we identified several options:

- **introduce a timeframe or 'sinking lid'**, which would prescribe a timeframe by which customers need to have their CDD completed.
- **amend the trigger in section 14(1)(c)** to a material change in the business relationship OR insufficient held about the customer.
- **change what is meant by material change**, such as by removing 'material' from the definition or expanding the scope of what constitutes a change.

723. Most submitters agreed that a lack of CDD information or records on existing customers is a vulnerability for businesses and for the system overall, and that this should be addressed. However, there were mixed views on what to do, with a slight preference for the timeframe or sinking lid approach. Other submitters opposed further prescription and advocated for a risk-based approach or maintaining the status quo but with additional guidance.

724. For ongoing CDD in general, some submitters considered that the current requirements are clear and appropriate, whereas a large number thought they should be clarified. Several submitters considered that CDD should be updated, with other submitters stating that they do this already. Similarly, some submitters supported an explicit requirement to consider when CDD was last conducted, with others again noting that they did this already. There was wide agreement that any additional ongoing CDD should take a risk-based approach to avoid a potentially significant compliance cost. These views were reiterated at the private sector consultation in April 2022.

725. Overall, we recommend introducing a requirement to update or obtain information as part of ongoing CDD. We also recommend this process includes consideration of when CDD was last conducted. This should align with the current requirements under section 31(4)(b) to review CDD information, or for an existing customer, to review any other information held. To ensure requirements are directed appropriately, we do not intend to prescribe specific obligations or timeframes and instead recommend a risk-based approach. Noting we consider that this issue impacts on existing customers to other customers, we do not recommend additional or amended requirements for existing customers in section 14 of the Act.[46]

Recommendations

R134. Issue regulations to clarify that the requirement of section 31(4)(a) and (b) to review a customer's account activity, transaction behaviour and CDD information (or for an existing customer, other information held) is according to the level of risk involved. This should then be amended in the Act itself.

R135. Introduce an additional ongoing CDD requirement to update (for a post-Act customer) or obtain (for an existing customer) CDD information if required. This should be a risk-based requirement, also considering the timing when CDD was last conducted. Appropriate wording should be developed in consultation with the private sector, covering requirements for post-Act and existing customers respectively. These requirements should be introduced through regulations initially and then be amended in the Act itself.

[46] There was broad support for this proposal at the targeted engagement workshops we ran in April 2022.

Monitoring non-financial activities

726. In addition to the ongoing CDD and account monitoring issues discussed above, there is a further issue most relevant to the DNFBP sectors. Section 31 of the Act only contains explicit requirements to monitor financial transactions. There is no accompanying requirement to monitor other activities, including DNFBP activities within a business relationship, such as actions as a nominee or trustee, real estate agency work or providing a business or correspondence address. We considered whether this was a vulnerability that should be addressed. And if so, the extent to which non-financial activities undertaken should be subject to monitoring obligations.

727. Submitters acknowledged the gap, with some advising that account monitoring is not relevant for DNFBPs or is largely unclear. More broadly however, there was resistance to requirements that were too prescriptive noting the need for a risk-based approach. Overall, we recommend extending ongoing monitoring obligations to activities undertaken by DNFBPs. However, as with monitoring of accounts and transactions, these requirements should only be according to the level of risk. Noting the scope of the Act, we do not consider it necessary to include other types of activities other than DNFBP activities.

Recommendation

R136. Issue regulations of the Act to state "regularly review any customer's activities described in the definition of designated non-financial business or profession in section 5(1) of the Act." These changes should then be enacted in section 31 of the Act.

6.1.7. Beneficiaries of life and other investment-related insurance

728. The FATF Standards include a requirement to obtain the name of any beneficiaries or classes of beneficiaries of life insurance policies and require businesses to consider the risk posed by the beneficiary when determining what level of CDD to conduct. We considered whether we should introduce such requirements, noting that no life insurers in New Zealand offer the types of life insurance products that are considered risky. Most submitters did not support the proposal, noting that it could result in unnecessary and disproportionate compliance costs. We do not recommend making changes to life insurance requirements and note that in the FATF gave minimal weight to this issue in New Zealand's Mutual Evaluation.

Recommendation

R137. Retain the status quo and do not impose any additional requirements for beneficiaries of life insurance policies.

6.1.8. Definition of customer

729. Identifying who the person is that meets the definition of a customer is not always clear, particularly where the transaction or relationship is complex, and many parties are involved, including intermediaries. This means that some businesses may be conducting CDD on multiple parties or conducting CDD on the wrong party if risks are to be addressed.

730. Regulations have previously been issued to prescribe who the customer is in some situations (e.g., real estate transactions), and we considered whether further prescription is required in specific circumstances. This includes when forming a legal person or arrangement, acting as a nominee or trustee, or when establishing an account or facility for a legal arrangement more broadly (noting a legal arrangement does not have legal personality by definition). We also considered whether the definition of customer was fit for purpose in general.

731. Some submitters considered the definition vague, unclear and could benefit from further refinement. It was identified as particularly challenging when dealing with trusts, estates,

complex structures, or complex transactions.[47] Most submitters supported regulations prescribing who the customer is in those situations where there are challenges.

732. We consider that the broad definition of customer is fit for purpose in most circumstances. However, we recommend issuing regulations to prescribe the customer in some situations. This will provide clarity to businesses, ensure consistency across the AML/CFT regime, and better mitigate the risks. The relevant situations primarily arise for the DNFBP sectors when forming, arranging, or acting for legal persons or arrangements. However, we also recommend when establishing an account or facility for a trust, it is clarified that the trust rather than its trustees is the customer.

Recommendations

R138. Issue regulations to prescribe that when establishing a facility for a trust, the relevant trust is the customer (and not the trustees who may be the facility holder).

R139. Issue regulations to prescribe appropriate CDD obligations for the formation of a legal person or legal arrangement. This should include a requirement to identify and verify the identities of the beneficial owners of the (to be formed) legal person or arrangement, as well as any person acting on their behalf.

R140. Issue regulations to prescribe the customer as the relevant legal person or arrangement when acting or arranging for someone to act as a nominee director, nominee shareholder or a trustee.

Managing funds in DNFBP trust accounts

733. There are potentially significant money laundering and terrorism financing risks associated with DNFBP trust accounts. When funds are held or moved through a DNFBP's trust account, it acts as a layer obscuring visibility of the origin of the money from the purpose for which it is being transacted. This is a vulnerability that can be exploited by criminals.

734. We considered whether the current AML/CFT settings for managing funds in DNFBP trust accounts were fit for purpose. Particularly we considered the extent to which obligations should apply to a non-client, which is not currently clear in the Act. For example, a DNFBP may hold funds that are ultimately intended for the DNFBP's client, but in the meantime are held in escrow for both parties until the transaction or activity concludes. We also considered whether the risk profile of trust accounts was the same across law firms, accounting practices, TCSPs and real estate agents.

735. We identified several options to progress, including in combination with each other:

- declaring any non-client paying funds into a trust account to be a customer under the Act, in turn requiring full AML/CFT obligations to be applied.
- prescribing that a non-client paying funds into a trust account is not a customer under the Act, unless conducting an occasional transaction.[48]
- introducing additional types of occasional transaction requirements which are specific to DNFBP trust accounts. For example, this could include funds received from a non-client that are not in line with instructions, more than expected, or constitute an elevated level of risk.
- introducing a broader requirement for DNFBPs to implement additional measures as are necessary to mitigate and manage the risks associated with their trust accounts (similar to requirements for new and developing technologies under section 30 of the Act).

[47] Other situations included non-court appointed liquidations (*see* Non-court appointed liquidations) and managing funds of non-clients (*see* Managing funds in DNFBP trust accounts).

[48] This includes the current occasional transactions prescribed under the Act, such as cash or cheque payments. This also includes circumstances when the non-client is an originator of a wire transfer, such as when funds in escrow need to be refunded or the non-client requests a payment to a third-party.

736. Submitters generally agreed there were risks associated with trust accounts noting a concern was refunds to third parties, with some suggesting that these refunds should be prohibited in their entirety. Others noted that transactions outside the nature or risk profile of the business relationship with the client could be triggers for CDD. Submitters considered that the risks associated with law firm or accounting practice trust accounts were lower than other sectors due to their professional obligations. More broadly, submitters agreed that clarity on obligations in relation to non-clients was required.

737. Overall, we consider that there are some vulnerabilities associated with the AML/CFT settings for DNFBP trust accounts that need to be addressed. However, we do not consider it necessary to introduce a requirement that all non-clients require full AML/CFT obligations to be applied when a DNFBP holds funds for the non-client in its trust account. Instead, we consider that changes should be implemented in two phases. For the longer term, we recommend reviewing the risks associated with trust accounts and implementing any additional measures as required to mitigate the risks. In the interim, we recommend issuing regulations to clarify the application of the Act to non-clients and target the higher risk circumstances when CDD requirements must be applied to them. Specifically, regulations should state that a non-client holding funds in a DNFBP's trust account is not that DNFBP's customer, unless the non-client undertakes an occasional transaction.

Recommendations

R141. Undertake a review of the money laundering and terrorism financing risks associated with DNFBP trust accounts and implement any additional AML/CFT requirements as required to mitigate the risks. This could include inclusion of an additional enhanced CDD requirement in the Act that a DNFBP must take any additional measures that may be needed to mitigate and manage the risks associated with managing funds in its trust account.

In the interim:

R142. Issue regulations that state a non-client holding funds in a DNFBP's trust account is exempt from being a customer under the Act, except if the non-client is undertaking an occasional transaction.

R143. Review whether any additional occasional transactions are required in relation to transactions through DNFBP trust accounts by non-clients (e.g., funds received exceed what is expected, elevated level of risk, payments to third-parties).

Timing of CDD obligations within a DNFBP business relationship

738. In some circumstances, the nature of a business relationship with a DNFBP may be more akin to a repeat client than a relationship of ongoing duration. As such, the Act's CDD requirements are sometimes difficult for DNFBPs to understand and apply, which results in additional compliance costs for those businesses.

739. Submitters from DNFBPs identified challenges determining when CDD is required on a repeat client (for whom there may be extended periods during which no activities or transactions were conducted). Submitters identified a further challenge in determining the point at which CDD is required when a non-captured activity (e.g., advice sought from a law firm) transitions to a captured activity (e.g., proceed with a house purchase). For law firms, this has previously been identified as particularly problematic in situations where advice is urgently sought, which then quickly transitions into an instruction for a captured activity. While we do not consider it necessary to amend the definition of business relationship, we agree it poses challenges for DNFBPs in some circumstances. We therefore recommend amending CDD requirements to clarify their application in the context of DNFBP business relationships.

Recommendation

R144. Review and amend the Act to clarify the application of AML/CFT obligations in circumstances when a DNFBP has a repeat client but does not have ongoing instructions, activities or transactions occurring with a business relationship. Concurrently, review and clarify the point at which CDD is required by a DNFBP if a non-captured activity transitions to captured activity.

6.1.9. Minor changes to customer due diligence requirements

740. We recommend making the following minor changes to CDD requirements:

Issue	Recommendation
In various sections of the Act, where a requirement for CDD is triggered outside a business relationship, there is reference to a customer seeking to conduct an occasional transaction or occasional activity. A person (outside a business relationship) becomes a customer if they conduct or seek to conduct an occasional transaction or occasional activity.	Amend the Act to replace the term 'customer' with 'person' in sections 14(1)(b), 18(1)(b), 22(1)(b), 22(1)(b)(ii), 22(2)(b), and 22(5)(b) to align with the definition of customer in section 5.
Regulation 10 of the *AML/CFT (Requirements and Compliance) Regulations 2011* require reporting entities to obtain information about the existence and name of any nominee directors and nominee shareholders. However, the definition of nominee director can include situations where directors of subsidiary companies or joint venture companies are required or accustomed to follow the directions from the holding company or appointing shareholder. This arrangement is not intended to be captured by the additional requirements.	Amend the definition of nominee director in Regulation 10 to exclude instances where the director is required or accustomed to follow the directions of a holding company or appointing shareholder.
Section 37 applies prohibitions if a reporting entity "is unable to" conduct CDD in accordance with the Act. One reading of this is that if a reporting entity can conduct CDD as required, but merely chooses not to, the prohibitions do not apply.	Replace "is unable to" with "does not" in section 37 to ensure the prohibitions apply in all appropriate instances where CDD is not conducted.
Simplified CDD is intended to apply only in situations where there are proven lower risks. There is no explicit requirement for businesses to not apply simplified CDD measures where there are higher risks, including where there is a suspicion of money laundering or terrorism financing	Issue a regulation which states that simplified CDD is not appropriate where there may be grounds to report a suspicious activity as per section 39A of the Act.
For real estate agents, CDD must currently be conducted before entering into an agency agreement with a client. This is often problematic in practice, particularly where a client is a legal person or arrangement requiring a more complex CDD process. Allowing slightly more flexibility for real estate agents will be more efficient for businesses without impacting on the level of risk.	For a customer that is a vendor, amend Regulation 24A of the *AML/CFT (Definitions) Regulations 2011* to require CDD to be conducted prior to listing the property, or prior to the sale/purchase agreement being signed (whichever is earlier).

Issue	Recommendation
A real estate agent that acts for a vendor client may have a relationship with another real estate agent to act as a conjunctional agent (and assist find a buyer, with commission shared). The conjunctional agent does not itself enter an agency with the vendor client. The application of CDD requirements requires clarification for these situations.	Issue regulations to clarify that a conjunction agent (acting for a real estate agent whose client is a vendor) does not have any direct obligations to conduct CDD on the vendor, but that SAR reporting obligations continue to apply.
Regulation 12 of the *AML/CFT (Requirements and Compliance) Regulations 2011* is intended to require mandatory CDD for a customer that is a limited partnership or overseas limited partnership with a nominee general partner. However, one reading of the regulation is that the nominee general partner is the customer.	Amend the regulation to state "a customer …that is b) a limited partnership or overseas limited partnership with a nominee general partner".

6.2. Record keeping

741. Effective record keeping is key for an AML/CFT regime to operate effectively. The purpose of keeping records is three-fold: it should enable law enforcement agencies to reconstruct individual transactions to investigate and if necessary, provide evidence for prosecution of criminal activity. It should also enable businesses to review and reconstruct a customer's transaction history when undertaking ongoing CDD and account monitoring, and to report suspicious activity. Finally, it should provide sufficient basis for supervisors to determine the extent to which a business is complying with obligations, particularly CDD and account monitoring obligations.

742. We asked generally whether businesses had challenges with complying with record keeping obligations. Submitters considered the requirements appropriate, although some identified the following areas that could be clarified or further refined:

- the extent to which legally privileged records can be requested, including by auditors
- requirements regarding destruction of records
- whether businesses are required to keep records of the document used to verify a person's identity, given the potential for identity theft and cyber-attacks
- which (if any) records should be retained in a form enabling their 'immediate' availability
- reconciling differences in legal requirements to keep the same record, such as under the *Financial Markets Conduct Act 2013* and the *Privacy Act 2020* and the general statute of limitations.

743. Regarding the first three issues, we recommend AML/CFT supervisors provide further guidance which covers these topics and aligns with the updated requirements of the *Privacy Act 2020*. This guidance should take care to not inadvertently increase compliance costs for businesses, noting that it can be expensive to keep and destroy records, especially physical records. We also recommend supervisors consult with the Privacy Commissioner in the development of this guidance.

744. Regarding the fourth issue, we note that the court in *Department of Internal Affairs v OTT Trading Group Ltd* [2020] NZHC 1663 held that records must be kept in a form that enables them to be immediately accessible. However, we recognise that this is unclear and recommend clarifying this requirement in the Act. In particular, we recommend amending the Act to specify the timeframe within which businesses are required to comply with requests to produce records. This timeframe should be consistent with *OTT Trading Group*

Ltd as well as the FATF's expectation that businesses are required to ensure CDD information and transaction records are provided 'swiftly'.

745. Regarding the final issue, we recommend reconciling the record keeping requirements with the Act with other relevant legislation (e.g., *Tax Administration Act 1994*) where businesses are under obligations to keep the same record for different periods of time. This could result in a longer timeframe to keep records under the Act but will simplify a business' overall obligations.

Recommendations

R145. In consultation with the Privacy Commissioner, develop and issue further guidance which covers a) the extent to which legally privileged records can be requested by supervisors and auditors b) expectations on businesses to keep records of the document used to verify a person's identity and c) the application of relevant *Privacy Act 2020* principles, including the extent to which businesses should be destroying records.

R146. Amend the Act to clarify the timeframe within which businesses are required to comply with requests to produce records. This timeframe should be consistent with existing jurisprudence on the issue as well as the FATF's requirement that records are provided swiftly.

R147. Reconcile record keeping requirements in the Act with other relevant legislation (e.g., *Tax Administration Act, Financial Markets Conduct Act)* to ensure businesses have consistent requirements to keep the same record under the various regimes.

6.2.1. Transactions outside a business relationship

746. Businesses are exempt from keeping records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold. The basis for this exemption is that the parties will not have been subject to CDD, so the business may not have the information about who the parties are in the first place.

747. We asked whether the exemption made it difficult for businesses to reconstruct transactions and whether the exemption should be removed. Most submitters supported keeping the exemption in place, although several submitters supported removing the exemption. On balance, we recommend removing the exemption as this will reduce the complexity of record keeping obligations. However, we anticipate that the AML/CFT supervisors will need to provide updated guidance about how businesses can comply with this obligation, noting that CDD would not have been conducted in the situation where the exemption applies.

Recommendation

R148. Revoke Regulation 8 of the *AML/CFT (Exemptions) Regulations 2011* applying to a transaction that occurs outside of a business relationship but is not an occasional transaction. The business would then have to keep records of the parties to a transaction where the transaction is outside a business relationship or below the occasional transaction threshold.

6.2.2. Minor changes to record keeping requirements

748. We also recommend making the following minor changes to record keeping requirements:

Issue	Recommendation
Businesses are not required to keep records of prescribed transaction reports.	Issue a regulation which requires businesses to keep records of prescribed transaction reports for five years.

Issue	Recommendation
The Act does not set out how long businesses should retain account files, business correspondence, and written findings.	Issue a regulation which requires businesses to retain account files, business correspondence, and written findings for five years.

6.3. Politically exposed persons

749. Due to their position and influence within governments or international organisations, politically exposed persons (PEPs) can pose significant money laundering and terrorism financing risks. PEPs may have control or influence over government expenditure and can therefore be involved in corrupt activity, either of their own volition or because they have been targeted by criminal networks. PEPs may also be vulnerable to foreign interference, which is a growing concern globally and one to which New Zealand is not immune.

750. The FATF Standards include requirements for how countries should mitigate the risks of PEPs, which distinguishes between foreign PEPs, domestic PEPs, and international organisation PEPs. The FATF's view – which reflects international consensus – is that foreign PEPs should always be considered to be high risk and dealt with accordingly, while domestic and international organisation PEPs may only be risky in limited circumstances. As such, we have split our recommendations and focus on foreign PEPs separately from domestic and international organisation PEPs.

6.3.1. Foreign politically exposed persons

751. The Act provides obligations and controls only in respect of foreign PEPs. A PEP is defined as a person who holds (or held in the past 12 months) a prominent public function in any overseas country, as well as their immediate family members and close associates. Businesses are required to take reasonable steps to determine whether the customer or beneficial owner of a customer is a PEP. If so, the business much have senior manager approval to continue the business relationship and obtain and verify information about the source of wealth or source of funds of the customer.

752. As New Zealand is generally considered to be a country with high levels of integrity, we may be attractive to corrupt foreign PEPs to use for laundering the proceeds of corruption. For example, the US government seized $260 million in assets held in New Zealand trusts as part 1MBD fund investigation, which was a corruption scandal in Malaysia.[49] In addition, the Panama, Paradise, and Pandora Papers all demonstrate how attractive New Zealand trusts and companies can be to those seeking to conduct illicit financial activity, including corruption. Accordingly, we have considered how to strengthen the current requirements regarding foreign PEPs as well as address the deficiencies identified by the FATF as part of New Zealand's Mutual Evaluation

Time limitation of the PEP definition

753. The current definition of PEP only includes a person that holds or has held a prominent public function in the past 12 months. This does not reflect the ability for a person to continue to hold influence for some time after formally ceasing to hold a position of public responsibility. The FATF identified this a significant deficiency as it could result in customers not being identified and treated as PEPs that should be.

754. We identified several options to resolve this deficiency:

- **increase the timeframe in the definition,** for example to 24 or 36 months.

[49] Reuters, *New Zealand court lets Low family replace trustees in 1MDB-linked case* (January 20, 2017). Available online at: https://www.reuters.com/article/us-malaysia-scandal-newzealand-idUSKBN1540FR

- **remove the timeframe in the definition** and replace it with a requirement to apply a risk-based approach to determining whether a former PEP should still be treated as high risk. This could be supported by guidance or a code of practice.

- **take a combined approach** by including a prescribed timeframe as well as requiring a risk-based approach for dealing with customers when the timeframe no longer applies.

755. Most submitters agreed the time limit should be removed to require businesses to determine the level of influence that the customer still retains, noting this would achieve greater consistency with the FATF Standards and international practice. Some submitters preferred a combined approach, with a small number opposing any changes to the time limit. We conducted further engagement on this topic in April 2022, and the consensus from attendees was to take a combined approach with a small adjustment to the prescribed timeframe.

756. In line with industry feedback, we recommend taking a combined approach to the definition of PEP, with the timeframe extended to 24 months. We consider this strikes the right balance between a clear and consistent expectation for persons who previously held prominent public functions, while also ensuring that risks can continue to be mitigated for a person who public influence endures. This approach also addresses the FATF's concerns.

Recommendation

R149. Extend the timeframe for which a person is considered a PEP from 12 to 24 months and require businesses to take a risk-based approach to determine whether a person should still be treated as a PEP after 24 months.

Identifying whether a customer is a foreign PEP

757. There are two separate but related issues with the current requirements to identify whether a customer is a foreign PEP: the first is the nature of steps to be taken, while the second is when the steps should be taken.

Steps to be taken

758. The FATF Standards requires businesses to have risk management systems in place to determine whether a customer or a beneficial owner is a foreign PEP. In practice, this requires proactive steps to assess risk profile, CDD information and for a business to undertake its own research to make this determination.

759. We identified various options to ensure businesses are taking appropriate steps to identify a foreign PEP:

- **require a business to have appropriate risk management systems in place** to identify whether a customer or beneficial owner is a PEP. In practice, businesses would be required to ensure they are taking proactive steps, but the nature of those steps would depend on the business.

- **require a business to take proactive steps** to identify whether a customer is a PEP. This would achieve the same outcome as requiring a business to have appropriate risk management systems in place but would be explicit in that the steps taken should be proactive.

- **the supervisors could issue a code of practice** or further guidance to set out what constitutes "reasonable steps". This could align with the FATF Standards but may be limited in terms of the ability to require proactive steps to be taken as the Act only specifies that businesses take reasonable steps.

760. Submitters broadly supported the status quo but noted that it would be helpful if 'reasonable steps' was further defined, including whether it was mandatory for businesses

to use a third-party provider for PEP screening. Submitters also supported of businesses being able to consider their level of exposure to foreign PEPs when determining the extent to which they need to take proactive steps, given that most businesses do not have any exposure. We conducted further engagement on this topic in April 2022, where attendees broadly agreed the Act should require proactive steps according to the level of risk involved.

761. We recommend amending the Act to require businesses to have appropriate risk management systems to determine whether a customer or beneficial owner is a foreign PEP. We consider this approach will provide clarity to businesses that the extent of the proactive steps required is dependent on the level of risk. We anticipate this change will be supported with guidance from supervisors.

Recommendation

R150. Amend the current 'reasonable steps' requirement in section 26 to instead require businesses to have appropriate risk management systems in place to determine whether a customer or beneficial owner is a foreign PEP.

When PEP checks should occur

762. The Act requires businesses to determine whether a customer or beneficial owner is a PEP as soon as practicable *after* the business relationship is established or an occasional activity or transaction is conducted. While the FATF Standards are not explicit when businesses should be conducting PEP checks, the clear implication is that this occurs as part of establishing a business relationship or before conducting the occasional transaction or activity. This ensures mitigation measures are applied at the appropriate point, noting for example, there is little value in obtaining senior manager approval after a transaction has occurred. However, we recognise that bringing PEP checking requirements forward may significantly increase compliance costs for businesses.

763. We identified two options for when PEP checks could be required as part of establishing a business relationship. The Act could require PEP checks to be:

- **completed *before* establishing the business relationship,** which would require every business, including those with limited exposure to foreign PEPs, to carry out the reasonable or proactive steps to determine whether a customer or beneficial owner is a foreign PEP.
- **carried out at the appropriate time according to the level of risk:** this could allow for PEP checks to occur at different times depending on the risk. For some low-risk transactions (e.g., deposits into 'locked in' investment schemes), PEP checks could occur as soon as practicable after the relationship is established, while for higher risk scenarios PPE checks may be required before the business relationship is established or services are provided. The high and low risk scenarios could be specified in law or left for the business to determine with guidance issued in support.

764. For occasional transactions or activities, the only option is for checks to occur before the occasional transaction or activity is conducted. However, to ensure this approach does not result in unnecessarily high compliance costs, we could specify that PEP checks are only required where information is received that clearly indicates a customer or a beneficial owner is a PEP.

765. Submitters were generally split on which approach should be taken. Approximately half the submitters preferred the status quo, which allows for businesses to perform "day two" checks. However, the other half of submitters considered checks should occur before establishing the relationship. Other submitters raised concerns about PEP checks more generally, noting that any changes would have significant operational impact These concerns were reiterated during the targeted engagement session that we conducted in April 2022, and attendees generally supported a risk-based approach for when PEP checks should occur.

766. In line with industry feedback, we recommend amending the Act so that PEP checks must be conducted at the appropriate time depending on the level of risk involved with the business relationship. This will allow businesses to appropriately tailor their approach based on various risk factors, such as the nature of their business and the products being offered. For example, a low-risk business (such as a KiwiSaver provider) may only need to conduct PEP checks at the point of first withdrawal, while a high-risk business should conduct its PEP checks before services are provided. This approach will also allow businesses to adjust timeframes if transactions are limited and risks mitigated, until such time as PEP checks are complete.

767. We further recommend agencies undertake analysis, introduce regulations, or amend the Act to identify and prescribe any types of business relationship or activities where PEP checks must be conducted before providing the service. For example, before a company or trust is formed. As part of this, introduce regulations and then amend the Act to specify that for an occasional transaction or activity, a PEP check is only required prior to the transaction or activity if information is received that clearly indicates the customer is a PEP.

Recommendations

R151. Amend the Act to require PEP checks to be conducted at an appropriate time depending on the level of risk involved in the business relationship. For high-risk circumstances, this should result in PEP checks occurring before services are provided to the customer.

R152. Undertake further analysis and then introduce regulations or amend the Act to prescribe types of business relationship or activities where PEP checks must be conducted before providing the service (e.g., before a company or trust is formed). As part of this, introduce regulations or amend the Act to specify that for an occasional transaction or activity, a PEP check is only required prior to the transaction or activity if information is received that clearly indicates the customer is a PEP.

Mitigating the risks of a foreign PEP

768. Once a customer or beneficial owner is identified as a foreign PEP, the Act requires senior management approval to continue the business relationship and that information is obtained and verified regarding the source of wealth or source of funds of the customer or beneficial owner. In addition, because of the level of risk, a business may be required to conduct increased monitoring of the business relationship (section 31(2)).

769. These requirements mostly comply with the FATF Standards, except for the requirement that senior management approval be obtained before the relationship is established, and that both the source of wealth and source of funds be obtained and verified. We identified options to address these deficiencies

- **requiring senior manager approval, where possible:** in line with our recommendation for the timing of PEP checks (*see* Recommendation R151), some PEP checks could be required before providing the service. In these circumstances, senior manager approval could also be required prior to establishing the business relationship. However, for PEP checks only required at an appropriate time depending on the level of risk, senior management approval could only be required to continue the relationship.

- **requiring compliance officer approval instead of the senior manager:** this may be more efficient and useful than the status quo which requires approval of a senior manager.

- **requiring source of wealth and source of funds to be verified:** this change would align with the FATF Standards.

770. Submitters identified a range of measures that are taken to mitigate the risks of a foreign PEP. This includes conducting PEP checks before establishing the relationship or conducting the transaction, and then obtaining approval from the compliance officer or a senior manager before doing so. However, some submitters stated no additional steps are taken beyond conducting CDD. When we discussed this during our April 2022 engagement

workshops, attendees were broadly supportive of further prescription including allowing businesses to seek the approval of the compliance officer instead of the senior manager.

771. Accordingly, we recommend amending the Act to require businesses to seek senior manager or compliance officer approval before establishing or continuing the relationship. We also recommend that the Act is amended to require businesses to take reasonable measures to establish the source of funds *and* the source of funds of customers and beneficial owners identified as a foreign PEP. We consider that this approach strikes the right balance between compliance costs and effectively mitigating the risk of a PEP, and broadly reflects existing industry practice.

Recommendation

R153. Amend the Act to require senior manager *or* compliance officer approval to establish or continue a business relationship with a foreign PEP, and to take reasonable steps to obtain information and verify the source of wealth *and* source of funds of the foreign PEP.

6.3.2. Domestic and international organisation politically exposed persons

772. The Act only imposes requirements on foreign PEPs. This means there are no explicit requirements to mitigate risks posed by persons holding prominent functions in New Zealand or on behalf of international organisations. As noted, domestic and international organisation PEPs may not have the same risk profile as foreign PEPs. However, there are still risks associated with these persons. This is true even in countries such as New Zealand where the perceived level of corruption is low and there have been instances of public sector fraud and corruption.[50] Accordingly, we considered whether the Act should be amended to improve detection and deterrence of domestic and international organisation corruption and fraud.

Definition of a domestic or international organisation PEP

773. We considered whether the definition of PEP should include domestic and international organisation PEPs. For domestic PEPs, we identified two options:

- **prescribe the exact roles and prominent public functions in the definition**, e.g., Ministers, local government Councillors, members of the judiciary. This is a prescriptive approach and would result in all persons holding the prescribed roles being included as a domestic PEP irrespective of the functions undertaken. While this could provide certainty and clarity to businesses, supervisors, and the public, it also risks persons being subject to additional AML/CFT obligations that should not be (e.g., they are not involved in decisions regarding procurement processes or budgetary spending).

- **take a more principled or functional approach to the definition** to include a person as a domestic PEP if they hold a "prominent function". We could define prominent function appropriately to mitigate the risks. (e.g., holding final approval over procurement processes, decision making powers over subsidies, responsibility for budgetary spending). Focussing on the function rather than the position is a more nuanced and risk-based approach.

774. For international organisation PEP, there are a broad range of roles, functions, and types of organisations. Consequently, prescribing the exact roles for a definition of international organisation PEP would be extremely challenging. However, we could again take a functional or principled approach and define international organisation PEPs as senior members of the organisation (e.g., directors, deputy directors, and members of the board or equivalent functions).

[50] See, for example, the public sector corruption and fraud cases identified by the Serious Fraud Office: https://sfo.govt.nz/fraud-and-corruption/what-we-do/public-sector-fraud-and-corruption/

775. Submitters were split on whether domestic and international organisation PEPs should be subject to specific AML/CFT requirements. Those opposed were concerned about resulting compliance costs, particularly if there is the same level of obligations currently required for foreign PEPs. Notwithstanding this, a significant number of submitters supported including domestic and international organisation PEPs, with about half stating they already treat domestic PEPs in the same way as foreign PEPs despite no explicit requirement to do so. During the private sector engagement in April 2022, attendees again expressed concerns about domestic PEPs being included in the Act, although the consensus was that the change should be made.

776. Given the instances of public sector corruption and fraud that have occurred in New Zealand, we consider that domestic and international organisation PEPs should have specific requirements under the Act. We therefore recommend amending the definition of PEP to include domestic and international organisation PEPs. We recommend taking a functional or principled approach, with the definition utilising the functions a person holds rather than the position. We note this change will also assist protect against foreign interference at all levels of government and aligns with industry practice for many businesses. We appreciate industry concerns about the potential costs associated with specific requirements for domestic and international organisation PEPs. However, we consider this concern can be mitigated by recommendations for less onerous requirements when compared to foreign PEPs (as discussed in the sections below)

Recommendations

R154. Amend the Act to include domestic PEPs in the definition of PEP. The definition should include a person holding a 'prominent function' within New Zealand, which should be prescribed appropriately (e.g., holding final approval over procurement processes above a certain level, decision making powers over subsidies or grants, or responsibility for budgetary spending). The definition should also prescribe a specific monetary threshold for the functions to ensure that only people with sufficient seniority meet the definition of a PEP.

R155. Amend the Act to include international organisation PEPs in the definition of PEP. The definition should include a person entrusted with a prominent function by an international organisation (e.g., director, deputy director, and a member of the board or equivalent position).

Identifying whether a customer is a domestic or international organisation PEP

777. Unlike foreign PEPs, the FATF does not consider domestic or international organisation PEPs to be inherently high risk. Accordingly, the FATF Standards require appropriate measures, based on an assessment of the level of risk, to determine whether a customer or beneficial owner is a domestic or international organisation PEP. If domestic and international organisation PEPs are explicitly included in the Act, we identified two options for requirements to identify if a customer or beneficial is a domestic or international organisation PEP:

- **require a business to have appropriate risk management systems** to determine whether a customer or beneficial owner is a domestic or international organisation PEP (which is consistent with the requirements for foreign PEPs) or
- **require a business to take reasonable measures**, according to the level of risk, to determine whether the customer or beneficial owner is a domestic or international organisation PEP (which is consistent with the FATF Standards).

778. Overall, submitters preferred a requirement to take 'reasonable steps' according to the level of risk involved, to identify domestic PEPs and international organisation PEPs. Only a few submitters did not agree and thought the requirements should be prescribed. Submitters also noted that the increased compliance cost would only apply to those businesses not already taking steps to identify domestic or international organisation PEPs.

779. We recommend amending the Act to require businesses to take reasonable and risk-based measures to identify domestic or international organisation PEPs. In practice, businesses

will need to take a risk-based approach to reviewing information obtained about a customer during CDD to determine if they are dealing with a PEP. In contrast to foreign PEPs, the checks can be conducted as part of normal CDD processes and will not require businesses to take proactive steps or implement expensive screening solutions.

Recommendation

R156. Amend the Act to require businesses to take reasonable steps, according to the level of risk involved, to identify whether a customer or beneficial owner is a domestic or international organisation PEP.

Mitigating the risks of a domestic or international organisation PEP

780. Given the potentially lower risks that domestic and international organisation PEPs pose, the FATF Standards allow flexibility for businesses to determine what, if any, additional mitigation measures are required. Options include those that are mandatory under the FATF Standards for foreign PEPs, i.e., obtaining senior manager approval to commence or continue the business relationship, taking reasonable steps to verify source of wealth and source of funds, and conducting enhanced monitoring of the business relationship.

781. If domestic and international organisation PEPs are explicitly included in the Act, we have identified two options for requirements to manage and mitigate the risks they pose. We could mandate that all additional measures are required in every instance for domestic and international organisation PEPs. Alternatively, we could allow businesses to determine, in accordance with a risk-based approach, what, if any, additional measures are required to manage the specific risks that the customer presents. Submitters provided limited feedback on this in response to the consultation document. However, during the private sector engagement workshops in April 2022, most attendees agreed businesses should be required to determine whether any additional steps are required to mitigate the risks. Only a few attendees preferred a more prescriptive approach.

782. In line with industry feedback, we recommend amending the Act to require businesses to determine what, if any, additional measures are required to manage the risks a domestic PEP or international organisation PEP presents. This determination should be based on an assessment of the risks associated with the function the PEP has been entrusted with, as well as other relevant risks the business is exposed to. If no additional risks are identified resulting from the customer or beneficial owner's status as a domestic or international organisation PEP, no additional steps are required. We consider this provides the most flexibility and is consistent the level of risk associated with domestic and international organisation PEPs in New Zealand.

Recommendation

R157. Amend the Act to require businesses to determine what, if any, additional measures are required to manage the risk of the domestic or international organisation PEP according to the level of risk involved with the relationship or transaction/activity.

6.4. Supporting the implementation of financial sanctions

783. As noted, all persons are required to implement financial sanctions as a result of obligations in the *Terrorism Suppression Act 2002*, *United Nations Act 1946*, and *Russia Sanctions Act 2022* (*see* Supporting the implementation of financial sanctions). However, there are no supporting or wrap around obligations on businesses to ensure that these financial sanctions are being appropriately implemented. This risks a business failing to recognise that a customer's assets must be frozen. The consequences of a financial sanctions breach are potentially severe for New Zealand and the business. The funds or assets could be used to support terrorism or proliferation of weapons of mass destruction, and the business could be committing an offence

784. We identified a range of obligations that could be developed to support the implementation of financial sanctions, such as:

- **requiring businesses to assess their risk or exposure** to designated individuals or entities and sanctions evasion**,** which would enable them to identify and understand their exposure and risk to a sanctions breach.
- **including financial sanctions implementation as part of an AML/CFT programme** – this could require businesses to identify and articulate their PPCs for ensuring financial sanctions obligations are implemented without delay. The nature of those PPCs could be guided by the risk assessment as well as guidance from agencies.
- **requiring businesses to get prompt notification of changes to designation lists** – this could require businesses to specify in their AML/CFT programmes how they ensure they are promptly notified about changes to designation lists (additions, changes, removals) and what action will be taken following a notification. If this option were progressed, we anticipate that the Government would need to provide a low- or no-cost option to assist businesses to comply.
- **screening for designated persons and entities** – this could require businesses to screen customer names prior to establishing a business relationship or conducting a transaction. Alternatively, a code of practice could be issued setting out steps to ensure appropriate screening of customers and transactions is in place.
- **providing notification of actions taken** – this involves creating a reporting obligation separate from SARs and suspicious property reports under the *Terrorism Suppression Act* to require businesses to report any assets frozen or actions taken in compliance with financial sanctions prohibition, including attempted transactions that were stopped.
- **providing assurance for ongoing action** – this involves creating a mandatory or optional requirement for the FIU or supervisor to review frozen assets and confirm the action by the business taken is appropriate. Alternatively, assurance could be provided through a process for dealing with false positives, for example an agency could confirm that a person is not a sanctioned individual and the business then release assets which have been inadvertently frozen.

785. Submitters broadly recognised more could be done to support implementation of financial sanctions obligations. However, there was no clear preference on what should be done, and several submitters urged caution due to the potential for significant compliance costs. Submitters also noted more support should be provided from Government across the board, such as issuing guidance and codes of practice or providing resources for businesses to use.

786. We recommend agencies continue to identify and develop appropriate obligations to support businesses implement financial sanctions obligations. Given the lack of consensus from submitters and the potential for significant compliance costs, further consultation and engagement is required to identify the appropriate obligations. We consider the starting point for future consultation and further cost/benefit analysis should be including sanctions requirements in risk assessments and AML/CFT programmes, steps required for screening and processes for dealing with possible matches and false positives.

Recommendation

R158. Agencies continue to explore through consultation what obligations are appropriate to support businesses in implementing their financial sanctions obligations, with the following obligations as a starting point:

- a requirement for businesses to assess their exposure to potential breach, non-implementation, or evasion of sanctions obligations.
- a requirement for businesses to include appropriate PPCs in their compliance programme which reflects their risk assessment and the nature of their business.

- a specific requirement for businesses to ensure they are promptly notified about changes to sanctions lists, with the government providing a free solution that covers sanctions for terrorism, proliferation of weapons of mass destruction, and any other relevant sanctions in force.
- an obligation for businesses to report what actions they have taken as a result of a sanctions notification (if any), including when attempted transactions are stopped.
- developing a process for dealing with possible matches, with agencies confirming when a person is not a sanctioned individual and that assets can be unfrozen.

6.5. Correspondent banking

787. Section 29 of the Act outlines requirements for banks when they establish correspondent banking relationships, when one bank (the correspondent bank) provides banking services to another bank (the respondent bank). These relationships are particularly vulnerable as the correspondent bank can be exposed to the risks from customers of the respondent bank, with whom the correspondent bank has no relationship and little visibility. In worst-case scenarios, the respondent bank could be being misused for large-scale money laundering.[51] Due to these risks, the Act (and the FATF Standards) require correspondent banks to take various steps before establishing correspondent banking relationships to fully understand the nature of the respondent bank's business.

788. One gap identified in the MER is that the "correspondent banking relationship" does not cover relationships outside the banking sector. Relationships similar to correspondent banking relationships may exist in other sectors. We considered the extent to which these relationships existed, and whether the requirements for managing risks of correspondent banking relationships need updating.

789. Several submitters considered the Act's correspondent banking requirements should be clarified or amended. Some suggested updates to reflect industry practice, as well as clarifying expectations for assessing whether the respondent's AML/CFT controls are adequate or effective. Submitters also noted correspondent banks should be subject to ongoing monitoring. In addition, submitters suggested clarifying that banks are not required to "know their customer's customer". There were no examples provided of correspondent relationships in other sectors.

790. In line with feedback and to address the deficiency identified by the FATF, we recommend amending section 29 of the Act to apply to reporting entities in general, rather than just banks. While we are unaware of similar correspondent relationships existing in other sectors, this will ensure sufficient controls if correspondent relationships do arise in non-banking sectors. We also recommend RBNZ issue further guidance to clarify what is expected to meet correspondent banking obligations.

Recommendations

R159. Amend section 29 to improve clarity, including by removing "effective" from section 29(2)(c). In addition, the requirements should apply to reporting entities in general, rather than just banks.

R160. RBNZ should issue further guidance to clarify what is expected to meet correspondent banking requirements.

[51] Per Dow Jones: "In 2017, for example, Denmark's Danske Bank was embroiled in a scandal when its Estonian branch handled about €200 billion in illicit money through correspondent banks around the world, including JPMorgan and Deutsche Bank, as well as Sweden's Swedbank. Danske Bank's chief executive was subsequently ousted, the lender is still subject to litigation that will run into the tens of millions of dollars; its share price halved when the details were aired." Available at: https://www.dowjones.com/professional/risk/glossary/correspondent-banking/understanding-risk/

6.6. Money or value transfer service providers

6.6.1. Licensing of MVTS providers

791. Remitters, or money or value transfer service (MVTS) providers, are identified both in New Zealand and internationally as a high-risk sector. We therefore considered if MVTS providers in New Zealand should be subject to a licensing framework or enhanced market entry controls and in what form this should take.

792. As identified (*see* AML/CFT licensing for some reporting entities), submitters supported licensing or enhanced market entry controls for high-risk sectors (that are not licensed elsewhere). Submitters noted this may provide assurance to banks around AML/CFT capability and therefore assist counter de-risking. During the private sector engagement workshop in April 2022, there was specific support for a licensing framework for MVTS providers, including from attendees within the MVTS sector. Attendees preferred licensing over other forms of enhanced market entry control because it provided the most assurance of AML/CFT capability.

793. In line with our general recommendation for licensing (*see* Recommendation R92), we recommend implementing a licensing framework for the MVTS sector. Licensing considerations should include fit and proper requirements and AML/CFT capability and competency, as well as options for sanctioning non-compliant licensees or unlicensed providers operating underground. We also recommend a licensing requirement for currency exchange services, noting that currency exchange is itself considered medium-high risk in New Zealand and often provided alongside MVTS.

Recommendation

R161. Develop a licensing framework for MVTS providers (to potentially include currency exchange noting this is often provided alongside MVTS) that:

- introduces fit and proper requirements (including to prevent MVTS providers being owned, controlled, or operated by criminals or their associates) and ensure only providers with sufficient AML/CFT capability are able to provide a MVTS service.
- has appropriate and proportionate mechanisms for sanctioning non-compliance. This includes restricting or cancelling an ability to provide the service, as well as taking action against providers operating without a licence. Obtaining a licence should also be a pre-requisite for FSP registration.

6.6.2. Agents of MVTS providers

794. The use of agents in the MVTS sector is common and some MVTS providers have networks of agents around the country. It is important that there are effective and workable AML/CFT settings to mitigate the risks associated with agency delivery models. This includes the extent to which an MVTS provider must have oversight, responsibility for and control over the AML/CFT compliance of its agents.

795. We have generally considered issues relating to agents across all types of reporting entity, including the lack of clarity regarding the functions an agent may undertake for a reporting entity (*see* Regulating agents). For the short term to address the issues identified, we recommend providing further guidance on the use of agents (*see* Recommendation R96). We also recommend issuing regulations requiring businesses to have PPCs for vetting and training agents, ensuring functions undertaken by agents comply with the Act and that a list of agents is maintained (*see* Recommendation R97).

796. We consider these recommendations appropriate for the use of agents across all sectors, including the MVTS sector. We determined that further options, such as differentiating respective AML/CFT functions, responsibilities and liability between a reporting entity and

its agent, should not be progressed at this time. However, this is an option for the longer term (*see* Recommendation R98).

797. That said (and noting that the MVTS sector is a high-risk sector) we consider that some additional measures specific to the MVTS sector are necessary and recommend that the development of a licensing framework for the MVTS sector includes consideration of the AML/CFT settings where agency models are used. For example, this some AML/CFT obligations could be imposed directly onto an agent, such as SAR reporting where the agent has identified grounds for suspicion, or liability for compliance in certain circumstances (*see* Recommendation R107).

Recommendation

R162. As part of the development of a licensing framework, examine the role of agents in a MVTS provider's AML/CFT programme. This should include considering whether some AML/CFT obligations should be imposed directly onto agents, for example SAR reporting in circumstances where they have identified grounds for suspicion and whether sanctions for non-compliance could be imposed on an agent rather than the provider (if the provider had taken all reasonable steps to comply).

6.6.3. Master agents and tipping off provisions

798. Large international MVTS providers sometimes engage master agents to assist with delivering their remittance service. A master agent typically assists with training, vetting, assurance and monitoring the compliance of various sub-agents on behalf of the MVTS provider. In addition to this, a master agent may itself operate as an agent of the MVTS provider, while also separately providing its own unrelated financial services (for which it is a reporting entity in its own right).

799. Along with the issues discussed in the section above relating to the use of agents in the MVTS sector, there are further issues specific to the use of master agents. The Act includes provisions for a master agent and its sub-agents to form a designated business group to share AML/CFT obligations. However, this is predicated on both master agent and sub-agents being reporting entities under the Act, which is not the case. In addition, this does not consider the role and responsibilities of the MVTS provider, noting that both master agent and sub-agent are acting on the MVTS provider's behalf and delivering its remittance service.

800. It is therefore not clear what responsibility or liability a master agent has for AML/CFT functions undertaken by a sub-agent (for the MVTS provider), including the circumstances in which a master agent is itself captured as a reporting entity. Relatedly, and outside of a DBG, the Act does not contain provisions that explicitly allow a MVTS provider, its master agent, or a sub-agent to share SAR information for AML/CFT compliance purposes. It is therefore unclear whether this is considered tipping off.

801. We considered whether the role of master agents should be clarified, and if so, how. We also considered whether a MVTS provider, its master agent and a sub-agent should be able to share SAR information for AML/CFT compliance purposes. Most submitters supported clarification of the role of master agents in a MVTS network. Attendees at the targeted engagement workshops in April 2022, including from the MVTS sector, supported aligning the application of the Act with the various activities that a master agent may engage in. Attendees also supported sharing of SAR information between an MVTS provider, a master agent and if necessary, a sub-agent for AML/CFT compliance purposes.

802. Overall, we agree the application of the Act should be clarified for the different activities a master agent may engage in. We also agree there should be the ability to share SAR information within a MVTS network where this is beneficial for compliance purposes. We therefore recommend exempting a master agent from being a reporting entity (in its own right) when undertaking activities for an MVTS provider in relation to a network of sub-agents. We also recommend exempting the tipping off restrictions within a MVTS network in appropriate circumstances. Noting the current lack of clarity in the Act on these issues,

we recommend issuing regulations in the short term (while the development of a licensing framework for the MVTS provider is progressed – *see* Recommendation R92). Alongside development of the licensing framework, we also recommend determining whether the DBG provisions for the MVTS sector should be amended or repealed on the basis they are redundant.

Recommendations

R163. Introduce the following measures by regulations:

- Exempt a master agent from being a reporting entity in relation to training, monitoring and other assurance activities undertaken for a network of sub-agents (on behalf of a MVTS provider). This is to clarify that in these circumstances, it acts on behalf of the principal MVTS provider (as part of the MVTS provider's AML/CFT programme). This is discrete from other circumstances when it may itself be an agent of a network provider or a reporting entity for separate financial services it provides.
- Exempt a MVTS provider, its master agent and if necessary, a sub-agent, from tipping off restrictions under section 46, allowing them to share SAR information between themselves when necessary for the purposes of AML/CFT compliance.

R164. In conjunction with Recommendations R161, R162, and R163 consider whether it is necessary to amend the DBG provisions for the MVTS sector or repeal them on the basis they are redundant.

6.6.4. Submitting Suspicious Activity Reports

803. As MVTS providers may be involved in both sides of a wire transfer, they might identify suspicious activity that might not otherwise be detected. The FATF Standards require MTVS providers that control both the ordering and beneficiary side of a wire transfer to consider information from both sides to determine whether a SAR is required. If so, the SAR should be submitted to the FIU in any affected country. This is not a requirement for MVTS providers in the Act.

804. We could issue regulations or amend the Act to state a MVTS provider that controls both the ordering and beneficiary end of a wire transfer must consider both sides of the transfer to determine whether a SAR has to be submitted. Alternatively, we could issue guidance encouraging MVTS providers to take this approach, although this would not comply with the FATF Standards or necessarily address the risks.

805. Most submitters supported aligning the Act with the FATF Standards. Those submitters who did not support this noted New Zealand's framework is not analogous to other jurisdictions and considered this requirement may cause complexity. We therefore recommend issuing regulations to require MVTS providers that control both the ordering and beneficiary side to consider both sides of the transaction to determine whether a SAR should be submitted. Not only will this comply with the FATF Standards, but it may also better address risks involving MVTS providers and wire transfers.

Recommendation

R165. Issue regulations that MTVS providers, who control both the ordering and beneficiary end of a wire transfer, should consider information from both sides of the transfer to determine whether a SAR is required. If so, the SAR should be submitted to the FIU in any countries affected by the suspicious transfer.

6.7. Mitigating the risks of new technologies

806. Developing new products, new delivery mechanisms, and using new or developing technologies can expose a business to emerging risks not previously considered. As a

result, the FATF Standards require businesses to identify, assess, and mitigate the risks associated with developing or using new products, practices, and technologies.

807. The Act requires businesses to assess their business, products, and delivery methods in their risk assessments. However, this does not comply with the FATF Standards for new technologies because there is no explicit requirement for risks to be assessed and appropriate mitigation measures put in place before a new product is launched. New technologies expose a business to new risks and methods of money laundering or terrorist financing. Undertaking a risk assessment prior to using a new product or technology enables a business to assess and mitigate new vulnerabilities at the outset. To address this gap, we considered whether to issue regulations to explicitly require businesses to understand the risk of new products or technologies prior to implementation. This could require risk assessments to be updated prior to launch, and measures put in place as part of AML/CFT programme to mitigate the identified risks.

808. Submitters were split on whether a requirement should be introduced to require new technologies to be assessed prior to launch. Those submitters that agreed considered it would lead to better designed and safer products and ensure that appropriate controls are in place for technologies being used. Submitters who opposed were concerned about the compliance burden associated with the risk assessment.

809. We recommend issuing regulations to require businesses to assess the risks associated with the development of new products and new business practices. This should include new delivery mechanisms and the use of new or developing technologies for both new and existing products. The risk assessment should be conducted prior to implementation of the new product, delivery mechanism or use of new or developing technology. This regulation will then align with the requirements of section 57(1)(f) and (i) of the Act to manage and mitigate risks and prevent new products and technologies being used for money laundering or terrorist financing.

Recommendation

R166. Issue regulations to require businesses to assess the money laundering and terrorist financing risks associated with new products and new business practices. The risk assessment should consider new delivery mechanisms, as well as the use of new or developing technologies for new and existing products. The risk assessment must be conducted before the technology or product is used.

6.8. Wire transfers

810. The FATF Standards for wire transfers are intended to prevent money launderers, terrorist financiers and other criminals having unregulated access to international payment systems, and to detect misuse. The FATF Standards require information on the parties to the wire transfer to be available to all financial institutions in a chain of transactions and to government agencies. This enables transactions to be traced internationally and suspicious transactions to be identified.

6.8.1. Terminology involved in a wire transfer

811. Section 5 of the Act defines a wire transfer, including when it is an "international" wire transfer. Section 5 also provides definitions of the institutions involved in wire transfers (ordering, intermediary, and beneficiary institutions). However, there are various issues with the terminology and definitions. In particular, the definitions do not appropriately reflect the technical, legal, and practical realities of how wire transfers are conducted, including how banks and non-bank reporting entities interact with each other for funds transfers. This in turn causes difficulties for prescribed transaction reporting obligations (*see* Types of transactions requiring PTRs).

812. Given the range of complex issues identified with the terminology, we consider the only feasible option is to repeal and replace it with appropriate terms to reflect the ways that wire transfers are conducted. However, there is an opportunity for regulations to provide some clarity to businesses, as well as capture other transactions that may not clearly fall within the current terminology but should be. One example of the latter is a practice adopted by some MVTS providers that use an informal system of money remittance. This involves directing one customer to transmit funds into an entirely unrelated customer's account to satisfy part of an inbound or outbound remittance.

813. Overall, submitters agreed with the issues identified in the consultation document relating to wire transfers. Submitters noted the various definitions are confusing, unclear, and inadequate in some areas, notably relating to how they apply to DNFBPs and other non-bank financial institutions (other than MVTS providers) and payments using emerging technologies. Submitters noted this in turn causes challenges complying with PTR requirements. Submitters agreed there should be fundamental reforms to the definitions, incorporating a more nuanced approach that ensures both banks and non-bank reporting entities have appropriate obligations.

814. Accordingly, we recommend repealing and replacing the terminology in the Act in the long term. The updated terminology should reflect the technical and practical realities of wire transfers and modern payment systems and be developed in consultation with the private sector to ensure the new definitions are fit for purpose. In the short term, we recommend regulations are issued to clarify whether the wire transfer provisions apply for certain types of transactions. Firstly, the regulations should ensure all transactions occurring as part of informal remittance systems are subject to the wire transfer provisions. Secondly, further analysis should be undertaken to determine whether 'Original Credit Transactions' that enable direct transactions to credit cards should be captured as wire transfers. Thirdly, further analysis should be undertaken to identify and determine whether some types of payment systems can be excluded from some or all of the wire transfer provisions if they are proven to be low risk (such as BPAY, which is excluded from wire transfer obligations in Australia).

Recommendations

R167. Repeal and, in consultation with the private sector, replace all wire transfer terminology with appropriate terms that reflect the reality of wire transfers.

R168. In the short term, explore whether regulations should be issued to carve in or out various transactions as wire transfers and ensure appropriate obligations for the parties involved. In particular:

- issue regulations to ensure all transactions occurring within an include all forms of informal MVTS systems are subject to the wire transfers provisions,
- examine whether 'Original Credit Transactions' should be included prescribed as wire transfers, and
- consider whether BPAY and other similar payment systems should be excluded from the wire transfer provisions on the basis of a low risk of money laundering and terrorist financing.

6.8.2. Ordering institutions

815. An ordering institution is a reporting entity instructed by a person (the payer or originator) to transfer funds to another person (the payee or beneficiary) at a beneficiary institution. Sections 27 and 28 set out the requirements for wire transfers of NZD 1000 or above to be accompanied by specific information about the originator and beneficiary

International wire transfers below the applicable threshold

816. Currently, there are no requirements to identify or transmit originator or beneficiary information for an international wire transfer below NZD 1,000. This does not comply with the FATF Standards, which require an ordering institution to collect and transmit the name

and account or transaction number for both the originator and beneficiary. This presents a vulnerability, noting that some low value payments may be high risk (e.g., terrorist financing, payments for online child sexual exploitation). Accordingly, we considered whether to amend the Act or issue regulations to require an ordering institution to obtain and transmit information to align with the FATF Standards for transfers below NZD 1,000. There would be no requirement to verify the information unless there were grounds to report a suspicious activity as per section 39A of the Act.

817. Most submitters stated they already transmit information about parties to a wire transfer that is below NZD 1,000. This is because most international payment systems, such as SWIFT, require this information regardless of the amount involved. That said, some submitters were concerned about introducing this requirement. This was partly due to compliance cost, but also because they considered the proposal may be ineffective at combatting money laundering and terrorist financing. Notwithstanding these concerns, attendees at targeted engagement workshops in April 2022 broadly agreed these requirements should be introduced.

818. We recommend issuing regulations to require ordering institutions to collect information about parties to an international wire transfer that is below NZD 1,000. This will ensure all international wire transfers contain some identity information, irrespective of the amounts involved, and increase the ability to trace payments. This information will only need to be verified as part of CDD requirements in circumstances where there may be grounds to report a SAR. Noting that most submitters indicated they already collect and transmit this information with a wire transfer, we do not anticipate significant compliance costs resulting from this recommendation. In addition, we note this recommendation will improve New Zealand's compliance with Recommendation 16 of the FATF Standards.

Recommendation

R169. Issue regulations to require ordering institutions to obtain and transmit name and account or transaction numbers for an originator and beneficiary of an international wire transfer below NZD 1,000. The regulation should specify that this information does not need to be verified unless there may be grounds to report a SAR.

Stopping international wire transfers that lack the required information

819. The FATF Standards require ordering institutions to be prevented from executing wire transfers without the required information accompanying the wire transfer. In practice, section 37 prohibits wire transfers from being conducted where CDD has not been conducted and/or there is information missing about the originator. However, there is no explicit requirement preventing an international wire transfer that lacks required beneficiary information (i.e., name and account number), and the existing prohibitions do not apply to wire transfers below NZD 1,000.

820. We considered whether there should be an explicit requirement not to execute international wire transfers that are not accompanied by the required information, and if so, how to achieve this. The only feasible option is to amend section 37 of the Act to include a new prohibition on executing a wire transfer that lacks the required information. This will also apply to international wire transfers below NZD 1,000 in the same way it does to transfers over NZD 1,000 if Recommendation R169 is progressed.

821. Most submitters stated that wire transfers are already stopped if some or all the information is missing about the required parties. This is due to requirements imposed by payment providers such as SWIFT. However, despite this, submitters were split on whether there should be an explicit prohibition on executing wire transfers without the required information. Those submitters opposing the proposal were concerned this may stop legitimate transactions and stifle innovation in payment systems. However, those submitters supporting the proposal noted risks associated with low value payments and considered it appropriate for ordering institutions to have to comply with this requirement.

822. We recommend amending the Act to include an explicit prohibition on executing international wire transfers that are not accompanied by the required information. This will

ensure all international wire transfers have the required information and improve the integrity of New Zealand's payment system. While we acknowledge there will be compliance costs for ordering institutions resulting from this recommendation, we note that it aligns to a significant extent with current requirements of payment networks such as SWIFT.

Recommendation

R170. Amend the Act to explicitly prohibit executing international wire transfers where the required information regarding the originator and beneficiary does not accompany the transfer.

Minor changes to ordering institution obligations

823. We also recommend making the following minor changes to ordering institution obligations:

Issue	Recommendation
There is currently no requirement for an ordering institution to maintain records of a beneficiary's account number or unique transaction reference number.	Issue regulations to require an ordering institution to keep records of then beneficiary account number or unique transaction numbers for five years.
It is currently not clear that the wire transfer obligations provisions apply to an underlying customer for MVTS providers that use agents.	Issue a regulation stating that the originator or beneficiary of a wire transfer is the underlying customer, not the MVTS provider's agent.

6.8.3. Intermediary institutions

824. Some wire transfers include intermediary institutions in the wire transfer chain. Intermediary institutions may receive and transmit the wire transfer on behalf of the ordering and beneficiary institutions. Intermediary institutions play an important role in ensuring the traceability of wire transfers to and from New Zealand. Intermediary institutions are typically the first to receive an inbound wire transfer and the last to send an outbound wire transfer. There may be one or more intermediary institution involved in an international wire transfer, depending on the destination country and the other businesses involved. The main obligation on intermediary institutions is to pass the wire transfer along the chain, including the information about the originator and beneficiary.

825. We identified several issues with the requirements for intermediary institutions:

- **retaining information with the wire transfer:** the Act does not mandate that the information be retained with the wire transfer, but just that the information be provided as soon as practicable (section 27(6)). This is not in line with the FATF Standards and risks transfers being delayed or information being lost about the originator and beneficiary. The Act could be amended to require intermediary institutions to retain the information, which would address this issue and improve compliance with the FATF Standards.

- **keeping records in a specific circumstance:** intermediary institutions are occasionally unable to keep the required information with a related domestic wire transfer, usually due to the technical limitations of the payment or clearance platform. Where this occurs, the FATF expects that the intermediary institution keeps a record of information about the parties for at least five years to ensure the transaction can be reconstructed. The Act does not require intermediary institutions to take this step, but regulations could be issued to address this gap.

- **identifying and responding to incomplete wire transfers:** intermediary institutions are not required to take reasonable measures to identify international wire transfers lacking the required information nor deal with an incomplete wire transfer. This means that wire transfers may be occurring without the required information. This reduces traceability and impacts the ability for the beneficiary institution to comply with its obligations. Regulations

could be issued to require intermediary institutions to take reasonable steps to identify wire transfers lacking required information, as well as to have appropriate policies and procedures to deal with wire transfers lacking required information

826. Several submitters indicated they retain information with the wire transfer (despite there being no legislative requirement to do so) and most submitters thought it should be mandatory to retain information with the wire transfer. Submitters also indicated they already keep records in the specific circumstance identified and/or have risk-based procedures in place to identify and deal with wire transfers lacking the required information. Notwithstanding existing industry practice, submitters were split on whether the regulations should be issued to require intermediary institutions to take additional steps to ensure traceability of wire transfers. However, when we conducted further engagement on this topic in April 2022 the consensus of attendees was supportive of regulations being issued.

827. We recommend issuing regulations to require intermediary institutions to include in their compliance programme:

- the reasonable steps they will take to identify wire transfers lacking required information, and
- risk-based policies and procedures to determine (i) when to execute, reject, or suspend a wire transfer lacking required information and (ii) the appropriate follow-up or remediation action.

828. These requirements will only apply to intermediary institutions in New Zealand. However, we note that several like-minded countries and trading partners have extended these requirements to intermediary institutions or intend to do so. For example, the United Kingdom, China, Japan, and Republic of Korea already require intermediary institutions to take these steps, as does Singapore, Hong Kong, and Malaysia. The Australian statutory review recommended these changes be made following their Mutual Evaluation while the United States have issued non-enforceable guidance recommending these steps be taken. In addition, parent companies of New Zealand institutions based in these jurisdictions typically require all subsidiaries or branches to take the same approach. This effectively imposes these obligations on some institutions in New Zealand already.

829. We similarly recommend issuing regulations to require intermediary institutions to keep a record for five years where technological limitations prevent the relevant information about the parties being transmitted with a related domestic wire transfer. This will ensure that the relevant wire transfers can still be traced should the transactions require reconstruction. We also recommend amending the Act to require intermediary institutions to retain the information with the wire transfer rather than providing the information to the beneficiary institution as soon as practicable.

Recommendations

R171. Issue regulations to require intermediary institutions in New Zealand to include in their compliance programme the reasonable steps they will take to identify wire transfers lacking required information and the risk-based policies and procedures they will apply when a wire transfer lacking the required information is identified.

R172. Issue regulations to require intermediary institutions to keep records for five years where technological limitations prevent the relevant information about the parties from being transmitted with a related domestic wire transfer.

R173. Amend the Act to require intermediary institutions to retain the information about the parties with the wire transfer, rather than provide it as soon as practicable after the transaction occurs.

6.8.4. Beneficiary institutions

830. A beneficiary institution of a wire transfer is a reporting entity that receives funds and makes the money available to the payee or beneficiary. The FATF Standards require

beneficiary institutions to take reasonable steps to identify wire transfers lacking the required information, verify the identity of the beneficiary for wire transfers above the applicable threshold, and have risk-based policies in place to handle wire transfers lacking the required information.

831. The Act mostly complies with the FATF Standards. However, while beneficiary institutions are required to have risk-based policies in place to deal with incomplete wire transfers, there is no explicit requirement to take reasonable measures to identify incomplete wire transfers in the first place. This gap could be rectified through issuing regulations or amending the Act.

832. Most submitters indicated they take measures to deal with wire transfers lacking the required information. This includes having rules and alerts in place to identify payments lacking information, such as wire transfers that have beneficiary names under a certain character limit. These wire transfers are then manually reviewed and either returned or corrected. Most submitters supported regulations being issued to clarify requirements, noting this would ensure a consistent approach, improve alignment with FATF Standards and have no or minimal cost implications. Those submitters opposed preferred guidance being issued.

833. We recommend issuing regulations requiring beneficiary institutions to include in their compliance programme the reasonable measures they will take to identify incomplete international wire transfers. These measures could include post-event or real-time monitoring where it is feasible and aligned with their risks. This will complement the existing requirement under section 27(5)(a), which requires risk-based procedures for handling wire transfers not accompanied by the required originator and beneficiary information.

Recommendation

R174. Issue regulations to require beneficiary institutions to specify in their compliance programme the reasonable steps they will take to identify international wire transfers lacking required originator and beneficiary information. These measures should be risk-based and can include post-event or real time monitoring where feasible and appropriate.

6.9. Reliance on third parties

6.9.1. Effectiveness of reliance provisions

834. A fundamental AML/CFT principle is that each business is responsible and liable for conducting CDD on its customer to the level required by the Act. Each business should identify its customer and understand their risks, based on the nature of their business relationship and unique visibility of their activities or transactions. This ensures that opportunities are maximised to detect and deter money laundering or terrorism financing.

835. That said, both the Act and the FATF Standards include mechanisms for a business to rely on CDD conducted by another party, without needing to conduct it again in full. This includes relying on another unrelated reporting entity (or equivalent business overseas) that already has a business relationship with the customer. This also includes relying on another reporting entity part of a designated business group (DBG) (discussed further below).

836. In both circumstances, the relying party is ultimately responsible and liable for ensuring that CDD is conducted to the level required by the Act. This allows for efficiencies in meeting CDD obligations, while at the same time ensuring reporting entities have the required level of oversight of their customer's identities and risk profiles.

Reliance on other reporting entities

837. Section 33 of the Act includes the provisions for relying on another unrelated reporting entity. This section also allows reliance on another business overseas that is subject to AML/CFT obligations in the other country (that may be known by a term other than "reporting entity"). Subject to certain conditions that must be met in advance, the relying party may obtain a customer's CDD information without needing to also obtain the data or documents that were used to verify it. The relevant verification data or documents are only required in the event the relying party needs it. If so, it must be provided as soon as practicable on request, but no later than within five working days.

838. While these reliance provisions broadly align with the FATF Standards, the FATF identified deficiencies with two aspects of section 33 of our Act. Firstly, there is no requirement for the relying party to consider the level of risk associated with a country if the business being relied on is not in New Zealand. Secondly, there is no requirement for the relying party to take reasonable steps to satisfy itself that the business being relied on has record keeping measures in place, and in turn, will be able to provide verification data or documents as required.

839. We considered whether our reliance provisions under section 33 were fit for purpose, or whether other forms of reliance should be introduced. This included considering how the pending Digital Identity Services Trust Framework and beneficial ownership registers (for legal persons) could be relied on by businesses to assist in meeting their AML/CFT obligations. We also considered whether the deficiencies identified by the FATF should be remedied.

840. Submitters raised various issues impacting on their use the Act's reliance provisions. This included the administrative burden, different interpretation of obligations and liability for ensuring the relied-on party is carrying out CDD as required by the Act. Submitters also identified issues relating to the duplication of CDD when multiple businesses all need to identify the same customer at a similar time. Several submitters suggested increased centralisation through registers or databases, which other businesses could then rely on and would lead to a significant reduction in compliance costs. However, other submitters opposed increased centralisation noting privacy and security concerns. Most submitters supported amending the section 33 provisions to align with the FATF Standards.

841. Overall, we agree that opportunities to reduce duplication of CDD should be progressed. We also note there may be compliance costs savings for businesses once the Trust Framework and beneficial ownership register for legal persons (*see* Beneficial ownership register(s) and Identity Verification Code of Practice) are in place. We therefore recommend agencies undertake further analysis to consider circumstances in which duplication of CDD can be reduced, including information sharing mechanisms for section 33 requirements and reliance on the Trust Framework and beneficial ownership register. In the interim we recommend issuing regulations to remediate the two deficiencies identified by the FATF in relation to section 33. We consider these to be minor amendments that will close a gap while the broader review of section 33 of the Act takes place.

Recommendations

R175. Undertake further analysis to consider circumstances in which duplication of CDD across multiple reporting entities can be reduced. This could include information sharing mechanisms that comply with section 33 requirements, including leveraging the beneficial ownership register and the Digital Identity Services Trust Framework to assist compliance with the Act.

R176. Issue regulations pursuant to section 33(2)(e) to require the relying party to consider the level of country risk if the relied-on party is not in New Zealand.

R177. Issue regulations pursuant to section 33(2)(e) to require the relying party to take steps to satisfy itself that the relied-on party has record keeping measures in place and will make verification information available as soon as practicable on request, but within five working days.

"Approved entities" and liability for reliance

842. Related to the reliance on other reporting entity provisions above, section 33(3A) of the Act enables a business to rely on a government "approved entity" for CDD purposes. If relying on an approved entity, the relying party is not responsible or liable for ensuring CDD is conducted to the level required by the Act. These provisions are inconsistent with the FATF Standards, which require ultimate responsibility and liability to always remain with the relying party. There are currently no entities approved to undertake this function for businesses. We considered whether we should retain the approved entity provisions and if so, how they could be used.

843. Most submitters supported the approved entity provisions, identifying potential efficiencies and reduction in the duplication of CDD across multiple reporting entities. Submitters suggested various options, such as having an approved class of entities or incentives to become an approved entity. Despite support for the provisions, most submitters did not want their business to be an approved entity as it would have compliance cost and risks. Some submitters stated we should repeal the approved entity provisions because they are inconsistent with the FATF Standards.

844. a workable use of them can be found, we agree the provisions may be useful to assist businesses meet their CDD obligations. However, there is no clear option to progress at this time, noting section 33(3A) restricts approved entity status to a reporting entity (rather than another type of business) and no reporting entity is willing to become approved. We also note our recommendation to review the IVCOP to align with the Digital Identity Trust Services Framework, which will incorporate a reliance element and provide safe harbour for businesses (*see* Recommendation R113).

845. Overall, we recommend agencies undertake further analysis to consider if the use of the approved entity provisions is viable. This should include consideration of extending the types of approved entity to include businesses that are not reporting entities. If use of these provisions is viable, they should be activated and if they are not viable, we recommend repealing the relevant provisions.

Recommendation

R178. Undertake further analysis to determine whether the approved entity settings are viable, and if so, identify those circumstances in which it could be used and activate its use. If not, the provisions should be repealed.

6.9.2. Reliance within a group

846. We identified several issues related to the Act's provisions for reliance within a group. The first issue is whether the current process of requiring businesses to form a designated business group (DBG) to share AML/CFT obligations is still the best approach. We also considered if an alternative approach could be taken, such as simply mandating that a group of eligible businesses implement compliance obligations at a group-wide level (without the need for an upfront formation process to establish the group). In addition, we identified specific issues relating to the DBG eligibility criteria and formation process that could be addressed, particularly if DBGs are to remain the preferred approach for reliance within a group for the long term.

Role of a DBG within New Zealand's AML/CFT framework

847. As noted, both the FATF Standards and the Act allow for groups of related businesses to share compliance functions between them. The FATF requires that a group of financial or non-financial businesses must have group-wide AML/CFT policies, procedures, and controls in place and may then rely on each other for CDD and other AML/CFT functions. This ensures that groups of businesses are alive to group-level risks, have processes to address those risks and allow for efficient reliance within the group.

848. In New Zealand, the Act states that businesses may form a DBG if they meet certain criteria. Within a DBG, businesses may then share a risk assessment, parts of an AML/CFT programme and rely on each other for CDD and other AML/CFT functions. Members of a DBG may also share SAR information to decide if a SAR should be submitted. The approach taken in New Zealand is different to the FATF Standards, in that DBGs (and consequently reliance within a group) is optional. The FATF identified this as a deficiency in our AML/CFT framework (*see* Group-wide programme requirements).

849. Given the deficiencies identified by the FATF, we have considered whether a more fundamental overhaul of the DBG provisions is required. This could include repealing the DBG provisions in their entirety and instead prescribing businesses that fall within the FATF definition of group to implement a group-wide AML programme (and on that basis, they are able to rely on each other to meet AML/CFT obligations). This could occur without the involvement or approval of the supervisor upfront or for ongoing administration of a group. This may be more efficient for both businesses and supervisors. The ongoing monitoring of compliance by businesses with these group requirements would then be undertaken as part of supervision.

850. We did not specifically consult on the overall role of the DBG within New Zealand's AML/CFT framework and whether they should be replaced entirely. However, most submitters agreed that groups of businesses should be required to have group-wide programmes, noting that this would ensure a common approach to risks across the group. Those opposed were concerned that this requirement could discourage international businesses from entering New Zealand, increase compliance costs, and result in businesses being required to manage risks to which they are not exposed.

851. Overall, we agree the ability to rely on, and share compliance resource within, members of a group provide significant opportunity to mitigate risks, while also reducing the compliance burden. We also consider there may be opportunities to improve or change the current provisions, so they are more efficient to use. That said, we consider any changes would create significant disruption and change for the many businesses that are currently in DBGs.

852. Accordingly, we recommend agencies undertake further analysis to determine whether the current DBG settings are fit for purpose (for financial institutions and DNFBPs respectively) for the longer term. In conjunction with consultation with the private sector, this should include consideration of the effectiveness of DBGs in mitigating the risks, whether there are improvements that could be made, other options and the potential compliance cost savings for each. This review should consider the option of simply prescribing group-wide compliance requirements for financial and non-financial groups (without any need for an upfront approval or amendment process with the supervisor).

Recommendation

R179. Undertake a review of the Act's DBG provisions, including whether they are fit-for-purpose, mitigate money laundering and terrorism financing risk and provide cost saving for businesses. This should inform whether any changes are required, including considering an alternate option of prescribing group-wide compliance requirements (within which businesses are able to rely on each other for CDD and other AML/CFT functions) without need for an upfront election process, eligibility to form, supervisor consideration etc.

6.9.3. Current challenges with DBG provisions

853. We identified two issues with the current DBG provisions that should be addressed irrespective of whether DBGs continue to be a feature of New Zealand's AML/CFT framework. This relates to the eligibility criteria to join a DBG and the current process for forming, or amending, a DBG.

Criteria for forming a DBG

854. The policy intent for reliance by DNFBPs within a DBG was broader than for financial institutions. Particularly, it was anticipated that DNFBP franchisees within the same franchise may be able to join a DBG and share AML/CFT programme and compliance functions. Accordingly, the DIA has taken a view that "related" means 'associated or connected'. These criteria are broader than permitted under the FATF Standards for a non-financial group. The DBG provisions for DNFBPs are used widely by real estate agents, with many members of a franchise often sharing AML/CFT programme and compliance functions. To a lesser extent, the provisions are used in other DNFBP sectors where there are commercial agreements or alliances between businesses.

855. Due to the range of different franchise models or commercial agreements in place in the DNFBP sectors, the extent to which there is a connection or association between businesses varies. Consequently, and to mitigate the risks associated with reliance on other parties, the DIA takes a case-by-case approach to determine if each DBG election is suitably 'related'. Considerations include the geographical location of businesses, whether services are provided in conjunction with each other, any proposed sharing of compliance function and how this will operate in practice.

856. We considered whether the criteria for forming a DBG were appropriate and whether any changes should be made. This includes an option of expanding the DBG eligibility criteria for financial institutions to align with the broader criteria available to DNFBPs. Or alternatively, we could reduce the eligibility criteria for DNFBPs to align with those for financial institutions. Some submitters thought the criteria to form a DBG should be expanded further to reduce compliance costs, such as for DNFBPs, small businesses or low-risk businesses. Other submitters considered the criteria for forming a DBG should not be changed.

857. We recommend agencies review the eligibility criteria for financial institution and DNFBP DBGs respectively. This review should be undertaken alongside the recommendation above to consider whether DBGs remain a reliance option under the Act. Bespoke reliance provisions may be needed for groups of DNFBPs (that have eligibility criteria broader than the FATF definition of group).

Recommendation

R180. In conjunction with the recommendation above, undertake a review of the appropriate eligibility criteria for financial institution and DNFBP DBGs respectively. If DBG provisions are to be repealed and replaced by prescribing requirements at a group level, consider whether separate provisions are required for reliance within a group of DNFBPs that is broader than the FATF Standards (e.g., members of a real estate agency franchise).

Process for forming a DBG

858. To form a DBG, each business must elect in writing to do so, notify its supervisor, and agree to comply with information privacy principles in the *Privacy Act 2020* (or the equivalent overseas). Regulations state the DBG takes effect 30 days after notification unless the supervisor requires further information within that period.

859. These automatic DBG formation provisions are inconsistent with section 132(2)(f) of the Act, which states a supervisor's function is to approve formation and additional members of a DBG. This is an issue particularly for DIA for the DNFBP sectors, noting the more expansive eligibility criteria (i.e., broader interpretation of the word 'related') and the case-by-case approach the DIA takes when considering eligibility (as outlined above). The DIA may need to request further information and documents from businesses to determine whether a proposed DBG is sufficiently 'related'.

860. Given the inconsistency between section 132(2)(f) and the regulations, we considered whether the DBG formation process is fit-for-purpose. We considered whether section 132(2)(f) of the Act mandated supervisors with authority to approve DBGs despite the

regulations, or whether this should be clarified. This change could be achieved through regulations for the shorter term, until such time as the review of the substantive DBG provisions in the Act have been completed.

861. Most submitters considered that supervisors should not have the ability to approve the formation of a DBG and the current process set out in regulations is appropriate. Only a small number supported the proposal. Notwithstanding this, we recommend issuing regulations to clarify that the AML/CFT supervisors are required to approve the formation of a DBG. This aligns with section 132(2)(f) of the Act, the fact that "related" is not defined for DNFBP DBGs, the function of supervisors to provide guidance, and the AML/CFT supervisor's role in the DBG election process. We consider the alternative, by which the AML/CFT supervisors are only able to request further information but not decline a DBG, poses significant risks if proposed members are not sufficiently related.

Recommendation

R181. Issue regulations to prescribe that the relevant AML/CFT supervisor is required to approve formation of a DBG.

Minor changes to designated business group provisions

862. We recommend making the following minor changes to DBG provisions:

Issue	Recommendation
Currently there is a Ministerial Exemption in place allowing members of a DBG to share a compliance officer. This expires on 30 June 2023.	Issue regulations to enable members of a DBG to share a compliance officer.
The FATF noted that there is no explicit requirement in section 32 of the Act requiring an overseas member of a DBG to conduct CDD to the level required by the Act.	Issue regulations to prescribe that an overseas member of a DBG must conduct CDD to level required by the Act.
Sections 31(1)(a)(ii) and 32(1)(a)(ii) require "verification information" to be provided on request. It is not explicitly clear that this requires the relied-on party to provide the relying party with copies of the records that were used to verify the customer's identity.	Issue regulations to clarify that 'verification information' (for the purposes of these sections of the Act) means a copy of the records used by the relied-on party to verify customer identity.

6.10. Internal policies, procedures, and controls

863. Section 57 of the Act sets out the minimum requirements for a business' compliance programme. This includes having adequate and effective PPCs for vetting and training staff, complying with CDD, account monitoring, record keeping and reporting obligations.[52]

6.10.1. Compliance officers

864. We considered whether the Act should mandate that compliance officers must be at the senior management level of the business. This is in line with the FATF Standards and identified as best practice. It enables the compliance officer to influence higher level decisions and ensures a senior manager is involved in the AML/CFT programme. That said, we also recognise many businesses in New Zealand are structured in a way that having a senior manager compliance officer may be inappropriate.

[52] Note that independent audits are discussed separately in the Regulating Independent Auditors section, *see* Regulating independent auditors.

865. Most submitters opposed mandating that the compliance officer be a senior manager, noting this is not always possible depending on the size of the business. Submitters considered the existing requirement for the compliance officer to report directly to a senior manager mitigates any potential risks or concerns. Some submitters considered it more important the compliance officer has sufficient experience and resources to undertake their duties, and that in some circumstances a non-employee natural person could be a compliance officer (if the reporting entity lacks an appropriate employee). During targeted engagement workshops in April 2022, there was consensus for prescribing that the compliance officer is either a senior manager or reports to a senior manager.

866. In line with submitter feedback, we recommend amending the Act to require the compliance officer to either be a senior manager or an to report directly to a senior manager. We consider this provides flexibility and will allow a business to choose the appropriate person as compliance officer within their organisational hierarchy.

Recommendation

R182. Amend the Act to require compliance offices to be either a senior manager or report to a senior manager.

6.10.2. Group-wide programme requirements

867. he FATF Standards require groups of financial or non-financial businesses to implement groupwide programmes against money laundering and terrorist financing. This requirement should apply to all branches and majority-owned subsidiaries of the group, e.g., multi-national companies with branches in multiple countries. The group-wide programme should require what is normally required by a compliance programme, but also set out policies and procedures for information sharing within the group, how group-level compliance, audit, and/or AML/CFT functions should be provided (e.g., group-level transaction monitoring), and adequate safeguards to ensure confidentiality of information exchanged.

868. The Act currently has no specific requirements requiring DBGs to implement group-wide programmes. This means that groups may not be mitigating their group-wide risks and implementing appropriate controls. While DBGs may rely on one member's individual compliance programme or risk assessment, there are no requirements for group-level risks to be assessed or mitigated against. This can also pose challenges for supervision to ensure both group and individual level risks are being managed. This can also pose challenges from a privacy perspective, with difficulties ensuring the group has appropriate policies for sharing and protecting personal information in accordance with the *Privacy Act 2022*.

869. We considered whether we should require groups of financial and non-financial businesses to implement group-wide programmes to address the risks groups are exposed to. We could amend the Act to require DBGs to have group-wide programmes in place. In addition, we would need to consider whether DBGs should continue to be optional for businesses to form, or whether there should be a mandatory obligation to do so. A mandatory obligation would align with the FATF Standards (*see* Role of a DBG within New Zealand's AML/CFT framework).

870. Most submitters agreed that groups of businesses should have group-wide programmes, noting this would ensure a common approach to common risks. Those submitters that were opposed were concerned this could discourage international businesses from entering New Zealand, increase compliance costs, and result in businesses being required to manage risks to which they are not exposed. Accordingly, we recommend amending the Act to introduce group-level compliance programme requirements for DBGs and/or financial or non-financial groups, depending on the outcome of the review of group reliance settings (*see* Recommendation R180). We anticipate that the precise details of group level compliance requirements will be developed in consultation with the private sector to ensure groups adequately address group-level risks but without imposing undue compliance obligations on those groups.

Recommendation

R183. Amend the Act to introduce group-level compliance requirements for financial and non-financial groups (e.g., consisting of a parent company or equivalent legal person exercising control and coordinating functions over the rest of the group) in consultation with the private sector.

6.10.3. Minor changes to internal policies, procedures, and controls

871. We recommend making the following minor changes to compliance officer requirements:

Issue	Recommendation
Some reporting entities have appointed legal persons as compliance officers where they do not have an employee who can fulfil the role. This is not the intention of the Act.	Amend the Act to specify that compliance officers must be natural persons.
There is a current Ministerial exemption in place that enables members of a DBG (that are reporting entities) to share a compliance officer, subject to certain conditions. The intent is to reduce compliance burden across members of a DBG.	Amend the Act to allow members of a DBG to share a compliance officer.

6.11. Higher-risk countries

872. The Act requires, in various places, businesses to understand the risks of the countries they deal with. In some situations, a customer based in a particular country will elevate the risk of that customer and require additional measures to be taken. In other situations, businesses cannot rely on reporting entities in countries with insufficient AML/CFT controls for CDD. Finally, some countries are such high risk that the FATF has named them, including asking countries to mandate additional measures to business relationships and transactions with persons from the country in order to counter the global risks they pose.

6.11.1. Understanding and identifying country risk

873. The Act requires businesses to have regard to the countries they deal with as part of their risk assessment and include measures in their programmes to mitigate risks associated with those countries. However, it can be challenging for businesses to understand whether a country should be treated as high risk beyond referring to the FATF's grey and blacklists (*see* Dealing with countries on the FATF's greylist or blacklist). Consequently, countries that may be high risk for other reasons may not be identified, including countries with small economies and weak AML/CFT systems that are not publicly identified by the FATF.[53] An additional challenge arises determining whether a country being high risk means a customer from that country should be treated as high risk; countries may have strong controls in one sector with vulnerabilities in another sector.

874. We considered whether the current requirements regarding high-risk countries are fit for purpose, including whether further support should be provided to businesses to ensure they can accurately and efficiently assess country risk. We identified various ways the current settings could be improved, including through more guidance, prescribing countries that should be treated as high risk, prescribing a process for assessing country risk, or providing more granular information about country risks as part of National or Sector Risk Assessments

[53] There are several examples of such countries in the Asia-Pacific region.

875. Submitters indicated determining if a country is higher risk is challenging, with the grey or blacklists generally used for a default assessment of the highest risk countries. Several submitters considered more support was required and suggested a code of practice with options and steps for businesses to follow. Submitters also suggested a central source or register containing information on country risk from a New Zealand perspective. Similarly, several submitters suggested a list of countries be published by supervisors, containing information such as risk ratings. Submitters noted that this would ensure greater cohesion in assessing and responding to country risk

876. We recommend updating existing guidance to provide further and more tailored information about the risks associated with dealing with businesses and customers located in other countries. This guidance should assist businesses understand what makes a country lower or higher risk, as well as the extent to which those risks are relevant to its dealings with that country. We anticipate more detailed guidance will support businesses in taking a more nuanced and risk-based approach.

Recommendation

R184. AML/CFT supervisors should update existing country risk guidance to provide further detail about the risks that can emerge when dealing with customers from or businesses involved other countries. This will enable businesses to take a more nuanced and risk-based approach.

6.11.2. Dealing with countries on the FATF's greylist or blacklist

877. The FATF maintains two public lists of high-risk and other monitored jurisdictions. These are the lists of:

- **high-risk jurisdictions subject to a Call for Action**, which identifies countries or jurisdictions with serious strategic deficiencies to counter money laundering, terrorism financing, and financing of proliferation. This list is often externally referred to as the 'blacklist', and currently lists two countries (the Democratic People's Republic of Korea and Iran).

- **jurisdictions under increased monitoring**, which identifies countries that are actively working with the FATF to address strategic deficiencies in their regimes to counter money laundering, terrorism financing, and proliferation financing. This list is often externally referred to as the 'greylist', and currently identifies twenty-three different countries, including several in the Asia-Pacific region (Cambodia, Myanmar, Pakistan, and the Philippines).

878. For countries on the blacklist, the FATF Standards require businesses to apply enhanced CDD to business relationships and transactions with natural and legal persons in that country. In serious cases, the FATF also calls upon countries to apply countermeasures against those countries, such as requiring enhanced scrutiny of branches in that country or prohibiting businesses to operate or have business relationships with people in those countries. The FATF does not expect countries to take any further steps with respect to countries that are on the greylist, although it anticipates that businesses will reflect the fact that a customer is in a greylisted jurisdiction as part of any risk assessment (*see* Risk-rating of customers).

Requiring businesses to apply enhanced CDD measures

879. In addition to the issues above relating to country risk generally, the Act imposes mandatory enhanced CDD on a non-resident customer from a country that has insufficient AML/CFT systems or measures in place (section 22(1)(a)(ii) and (b)(ii)). The Act also requires all businesses to have policies, procedures, and controls in place to monitor businesses relationships and transactions from or to countries that have insufficient AML/CFT systems (section 57(1)(h)). The FATF determined these provisions do not comply with the FATF Standards that business relationships and transactions from blacklist countries are subject to enhanced CDD.

880. We recommend issuing regulations to specify that "countries with insufficient AML/CFT systems or measures in place" refers exclusively to countries on the FATF blacklist. This will ensure the FATF Standards are met, while also clarifying that countries on the FATF's grey list should not be automatically subject to enhanced CDD. Businesses may still need to conduct enhanced CDD on a customer from a country on the FATF's grey list, but this will be because the business has determined that the level of risk involved is such that enhanced CDD should apply. This will also provide further clarity regarding the scope of section 57(1)(h).

Recommendation

R185. Issue regulations to specify that the references to countries with insufficient AML/CFT systems or measures in place in sections 22(1)(a)(ii), 22(1)(b)(ii), and 57(1)(h) refers exclusively to those countries identified by the FATF as being high-risk jurisdictions subject to a Call to Action.

Imposing countermeasures when called for by the FATF

881. As a result of the FATF blacklisting DPRK and Iran, New Zealand is expected to identify and implement appropriate countermeasures against these countries in order to combat the global risks they pose:

- **with respect to DPRK**, the FATF expects that countries should take the necessary measures to close existing branches, subsidiaries, and representative offices of DPRK banks within their territories and terminate correspondent relationships with DPRK banks.
- **with respect to Iran**, the FATF expects countries to require increased supervisory examination for branches and subsidiaries of financial institutions based in Iran; introduce enhanced relevant reporting mechanisms or systematic reporting of financial transactions; and require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in Iran.

882. Submitters generally supported regulations to impose countermeasures against countries on the FATF's blacklist. There was no clear preference for what countermeasures could be imposed, with some submitters suggesting business relationships with persons in these countries should be prohibited while others considering enhanced CDD should be required. However, submitters also noted that care should be taken to ensure that immigrants or refugees from those countries are not discriminated against as a result of countermeasures being imposed

883. We consider the existing power in section 155 is not sufficiently broad to meet the FATF Standards in that it is specific to prohibiting or regulating business relationships and transactions with persons in a specific country. It does not extend to prohibiting or regulating various business activities in or with a specific country, such as prohibiting New Zealand businesses from establishing branches or subsidiaries in the country or prohibiting businesses from that country from establishing branches or subsidiaries in New Zealand. As such, we recommend amending the Act to ensure the power in section 155 is sufficiently broad to enable the full range of countermeasures to be imposed if required.

884. With respect to implementing countermeasures against DPRK and Iran, we recommend agencies identify what countermeasures should be imposed to combat the threats posed by these countries. In particular, we recommend issuing regulations to prohibit businesses from establishing correspondent relationships with DPRK banks. We note there are no branches, subsidiaries, or representative offices of DPRK banks within New Zealand.

885. With respect to Iran, we note the existing PTR regime provides for the automatic reporting of transactions with people or businesses in Iran. If the threshold for reporting is lowered to NZD 0 (*see* Applicable threshold for reporting prescribed transactions), the PTR framework will provide full visibility of transactions involving Iran. The other countermeasures identified by the FATF either do not require regulatory changes (increased supervisory examination) or are not possible within the current settings of the Act (increased external audits for groups – *see* Group-wide programme requirements).

Recommendations

R186. Amend the Act to ensure the power in section 155 is sufficiently broad to enable the full range of countermeasures to be imposed if required.

R187. Agencies should undertake further analysis to identify what countermeasures are required to mitigate risks posed by DPRK and Iran. With respect to DPRK, regulations should be issued to prohibit businesses from establishing correspondent relationships with DPRK banks.

6.11.3. Imposing countermeasures on specific individuals or entities

886. Section 155 allows regulations to be issued that prohibit transactions and business relationships between reporting entities. These regulations can be of general application or can apply to specific parties or countries. New Zealand is seen as an attractive place to do business and enjoys a strong international reputation for low corruption and high levels of integrity. As such, individuals involved in significant criminality, including corruption, may see New Zealand as an attractive destination country for their illicit wealth.

887. Accordingly, we considered whether the regulation making power in section 155 could be used to prohibit business relationships or transactions with specific individuals (such as identified heads of organised crime networks). Regulations of this kind could further protect New Zealand from the money laundering risks such individuals present. However, we also note the current power lacks any human rights or natural justice protections to ensure the power is used only in appropriate circumstances. For example, there are no criteria specified for when the power can be used, or the level of proof needed before a countermeasure of this nature could be issued. In addition, there are no procedures for requesting a review or revocation of the power beyond a judicial review, including where bona fide third parties are incorrectly impacted by the countermeasure.

888. Some submitters supported regulations to impose proportionate and appropriate countermeasures on specific individuals or entities to mitigate the risk posed. Submitters agreed there should be strict controls on the power, such as requiring a court to approve the countermeasure before it is issued and be satisfied that the relevant threshold is met. However, other submitters were unsure or opposed to countermeasures being issued against individuals as the Act would become a de facto autonomous sanctions regime.

889. We recommend agencies explore the feasibility of issuing countermeasures against specific organised crime groups (e.g., South American cartels, Asian organised crime groups) to combat the transnational organised crime that these groups pose. In particular, agencies should explore the effectiveness of these types of countermeasures, as well as understand what amendments to the section would be required in order to ensure any countermeasures are appropriate and proportionate

Recommendation

R188. Explore the feasibility of issuing countermeasures against specific transnational organised crime groups to combat the threat that those groups pose to New Zealand.

CHAPTER 7

Financial intelligence

Summary

890. The collection, analysis, and dissemination of financial intelligence is a fundamental purpose of the Act. By requiring businesses to report suspicious or routine transactions, the FIU can produce tactical intelligence about suspicious or illicit activity to which law enforcement agencies can respond (e.g., through prosecution or asset recovery). However, the collection of financial intelligence also supports the risk-based approach, as it enables the FIU to develop strategic or operational intelligence about trends, typologies, and new or emerging risks that may prompt additional reforms or changes in resource deployment.

891. This chapter focuses on the relevant requirements for three types of report required to be submitted under the Act:

- **suspicious activity reports (SARs),** which businesses are required to submit no later than three working days after they have reasonable grounds to suspect that a transaction, activity, or inquiry may be relevant to the investigation or prosecution of any offence, including money laundering or terrorism financing (sections 39A and 40)
- **prescribed transaction reports (PTRs),** which businesses are required to submit within ten working days where someone conducts an international funds transfer exceeding NZD1,000 or large cash transaction exceeding NZD 10,000 through their business (section 48A)
- **border cash reports (BCRs),** which every person is required to submit if they move more than NZD 10,000 in cash or certain cash-like equivalents into or out of New Zealand (section 68).

892. We have made several recommendations throughout this report that will have an impact on the effectiveness of the Act's financial intelligence framework. In particular, we have recommended independently constituting the FIU separate from the Police and further exploration of the role it could or should play within the regime (*see* Position of the FIU within the regime). We have also recommended that the FIU be provided with further intelligence collection powers (*see* Financial intelligence), as well as greater ability for the FIU to share its intelligence with AML/CFT agencies (*see* Direct data access to FIU information for other agencies).

893. Notwithstanding the above, we also make several recommendations to enhance suspicious activity reporting, prescribed transaction reporting, and border cash reporting. With respect to SARs, we recommend providing further guidance about submitting these reports, reviewing the legislative requirements for submitting SARs, and reviewing and potentially replacing goAML with an appropriate system if it is not possible to make goAML more user friendly. We also recommend adjusting the requirements for lawyers to ensure they can appropriately navigate their legal privilege and SAR obligations as well as considering amending the information sharing provisions for SARs to enable a more collaborative approach to be taken by industry.

894. With respect to PTRs, we note that many of the challenges with these reports result from the wire transfer terminology in the Act, which we recommend repealing and replacing in consultation with industry (*see* Wire transfers). In the interim, we recommend issuing regulations to clarify the types of transactions that should be reported as well as tailoring obligations when non-financial businesses are involved with sending or receiving wire transfers on behalf of an underlying customer. In the long term, and once known issues are satisfactorily resolved, we recommend lowering the reporting threshold for international

funds transfers (i.e., to NZD 0) and large cash transactions (e.g., to NZD 5,000) if the costs of these changes are justified by the benefits.

895. Finally, we recommend amending the Act and issuing regulations to require BCRs in respect of other forms of value, such as casino chips and precious metals. This will ensure that BCRs continue to provide valuable intelligence about cross-border value movements and enable broader detection and deterrence of money laundering and terrorism financing. We also recommend increasing the penalties that can be imposed by Customs and the courts in respect of falsely declared or uncleared cash movements, as well as providing Customs with the power to investigate whether a person has provided false or misleading information in connection with a BCR.

7.1. Suspicious activity reports

896. Suspicious activity reports are a core part of any effective AML/CFT regime and a crucial source of information for the FIU. Information contained in SARs is combined with other sources of information to provide an intelligence picture to law enforcement and regulatory agencies. In turn, SARs can lead to the detection and disruption of serious offending, including money laundering and terrorism financing.

897. Criminals often seek to evade detection and avoid arousing suspicion, such as by transacting below any reportable thresholds (*see* Applicable threshold for reporting prescribed transactions). However, by requiring businesses to identify and report on any suspicious activity irrespective of the amount, it becomes increasingly harder for criminals to conduct their illicit activity in New Zealand. As such, SARs help to make New Zealand a hostile environment for organised criminals and terrorists.

7.1.1. Ensuring the FIU receives high-quality and accurate SARs

898. On average, New Zealand businesses submitted approximately 14,700 SARs per year between 2017 and 2021, with banks and remitters responsible for submitting almost of the reports received. However, the FIU sometimes receives SARs with limited or no useful intelligence. This may be a result of "defensive reporting" or uncertainty as to what constitutes suspicion, what the threshold is, and when the three-day timeframe is triggered. We also understand, based on submitter feedback, that the lack of clear guidance, lack of feedback, and the use of goAML can be barriers to reporting entities understanding how to produce a high-quality or useful SAR.

899. There are several legislative and non-legislative options that could be considered to make improvements to the SAR regime, including:

- **amending legislative requirements for SARs** so they are sufficiently clear and better enable businesses to provide high quality reports. Options include removing or allowing a longer timeframe to submit a SAR and/or prescribing the steps businesses that must be taken to prepare a SAR. We note that many countries do not prescribe a timeframe for submitting a SAR, instead adopting a more flexible requirement to submit the SAR as soon as reasonably practicable. We also note that some other countries have phased SAR reporting requirements, which differentiate between forming the initial suspicion and having grounds to report.

- **implement a SAR feedback mechanism** to require the FIU to provide feedback to individual businesses or industry. This would outline how SARs have been used by the FIU or law enforcement agencies.

- **making it easier for businesses to submit a SAR:** in the short term, we could update guidance on suspicious activity reporting and provide examples of best practice. In the longer term, we could review and update goAML to ensure it is fit for purpose and user friendly. If this is not possible, we could replace the goAML system.

900. Submitters noted that the low quality of SARs may be driven by businesses submitting SARs defensively and focusing on technical compliance at the expense of effective reporting. They also noted that low quality/high volume reporting may be occurring because businesses are not confident in applying the "reasonable grounds for suspicion" test or due to regulatory action against businesses who have not submitters SARs. Submitters noted that the current guidance was outdated and there needed to be a more collaborative approach across the supervisors and the FIU regarding supporting businesses to identify and report suspicions. Submitters also noted that goAML was onerous to use and a detriment to the regime. These views were reiterated during targeted engagement workshops in April 2022.

901. We recommend updating and reissuing guidance on SARs. The AML/CFT supervisors and FIU should take a collaborative approach when issuing relevant guidance as we consider this would likely provide the best improvement to the regime and support businesses in identifying and reporting suspicious activity. This could be done through a series of interagency and industry workshops. Agencies should also consider including examples of best practices and further examples about the use and value of SARs for law enforcement and regulatory purposes. We also note that our recommendation to create a framework for sharing dynamic or live risk information would help businesses in implementing a risk-based approach (*see* Framework for understanding and sharing risk information)

902. We also note that businesses are technically required to report all suspicious behaviour, irrespective of the value or significance. Some types of criminality, such as fraud, can involve a large number of offending involving low value amounts. Under the current requirements, businesses are required to report each transaction individually if they have reasonable grounds to suspect they are fraudulent. This imposes significant compliance costs on businesses and increases the volume of financial intelligence reported but can also lead to the identification of large-scale (but low value) frauds or scams. We recommend exploring whether regulatory exemptions can be used to reduce or remove the requirement to submit a SAR in instances where there is little intelligence value to be gained.

903. In the long term, we recommend reviewing the legislative requirements for submitting SARs to ensure they appropriately facilitate the provision of accurate and high-quality intelligence. Given the challenges that have been identified with lawyers being able submit SARs in time, it is possible that other sectors are also finding the three-day timeframe challenging. We note that most other FATF countries do not prescribe a specific timeframe by which to submit a SAR, opting instead to use a more flexible timeframe such as a requirement to submit as soon as reasonably practicable. We also note that other countries have separate requirements for businesses that distinguish between initial suspicions and grounds to report a SAR, and this approach could be explored as part of amending the relevant timeframes in the Act.

904. Finally, we recommend reviewing goAML's functionality to determine whether it can be made sufficiently user friendly and meet industry needs. We note that goAML continues to receive updates, but also recognise that most other developed countries use their own bespoke systems or platforms. If it is not possible to improve the functionality of goAML, we recommend replacing goAML with an appropriate system.

Recommendations

R189. Review and update suspicious activity reporting (SAR) guidance in collaboration with the private sector to ensure it is fit for purpose and meets the needs of reporting entities. This guidance should include examples of best practice and explain how SARs are used by law enforcement agencies.

R190. Explore options for issuing regulations to reduce or remove the requirement to submit a SAR in instances where there is little intelligence value to be gained, such as low value frauds.

R191. Review the legislative requirements for submitting SARs to ensure they appropriately facilitate the provision of accurate and high-quality intelligence. In particular, agencies should consider whether a strict legislative timeframe is the best approach, as well as whether the Act should differentiate between forming an initial suspicion (which requires further investigation) and having reasonable grounds to suspect (which requires a SAR).

R192. Review goAML's functionality to determine whether it can be made sufficiently user friendly and meet industry needs. If it is not possible to improve the functionality of goAML, agencies should work towards replacing goAML with an appropriate system.

7.1.2. Navigating legal privilege and SAR obligations

905. Lawyers are subject to unique ethical and legal obligations because of their role within the justice system, the work they undertake, and consequently the nature of their relationship with a client. Consequently, the responsibility to maintain client confidentiality and protect privileged communications may sometimes conflict with the obligations to submit a SAR. This can sometimes be challenging to navigate.

906. Lawyers are not required to disclose any information where they believe on reasonable grounds that it is legally privileged information, but there are instances where privilege does not apply (e.g., if the information was provided for a dishonest purpose). However, applying the relevant tests in the Act can be challenging, especially considering the requirement to submit a SAR within three working days of forming reasonable grounds to suspect. In addition, while there are some protections for disclosing information in a SAR, section 44(4)(b) states that protections do not apply if there were reasonable grounds to believe the information was privileged, irrespective of whether the lawyer had, in fact, identified those grounds when submitting the SAR.

907. We note that there have been relatively low numbers of SARs submitted by law firms, which does not appear to be in line with the risks that the legal sector is exposed to. Submitters suggested the low numbers of SARs could be driven by the complex test lawyers are required to apply, and the lack of statutory protections should they fail to apply the tests correctly. Further, determining whether information is privileged may not always be straightforward, and may require a lawyer to seek external legal advice.

908. We recommend reviewing the settings regarding legal privilege relating to the submission of SARs by law firms. In the short term, we recommend DIA and the FIU prepare further guidance to support law firms in navigating their competing obligations. We also recommend issuing regulations to provide law firms with a slightly longer timeframe to submit a SAR (e.g., increasing the timeframe from three working days to five working days). This will ensure that law firms have enough time to apply the relevant tests, while also ensuring lawyers are promptly reporting suspicion.

909. For the longer term, we recommend reviewing and amending or repealing section 44(4)(b) to ensure that, like every other sector, lawyers are protected if they provide information in a SAR in good faith. Given industry feedback, we are concerned the current lack of protection may ultimately be undermining their ability to provide actionable intelligence to the FIU. However, we also recognise the need to ensure that any SAR obligations do not undermine a lawyer's fundamental ethical obligation to ensure legal privilege is maintained.

Recommendations

R193. The FIU and DIA should review and update existing guidance to ensure that lawyers are able to navigate their competing obligations of legal privilege and suspicious activity reporting.

R194. Issue regulations to extend the timeframe for law firms to submit a SAR (e.g., from three working days to five working days) to allow enough time for law firms to determine whether any information within a SAR is privileged.

R195. Review and amend the legal privilege settings in the Act regarding SARs, in particular whether section 44(4)(b) should be repealed so that law firms can rely on a statutory defence to any prosecution if they have provided the information in good faith.

7.1.3. Enabling a more collaborative approach to reporting suspicions

910. The Act strictly limits the circumstances in which SAR information can be shared. For example, a reporting entity cannot disclose SAR information to anyone other than a lawyer, the Police, its AML/CFT supervisor or other members of a DBG, and the Police can only share SAR information for law enforcement purposes. These measures protect individuals and businesses that submitted a SAR, while also ensuring the subject of a SAR is not tipped off about its existence.

911. While controls on sharing SAR information are vital to the integrity of the AML/CFT regime, our current provisions may be overly restrictive and not consistent with the Act's purpose to detect and deter money laundering and terrorist financing. In particular, increased ability to share SAR information in some circumstances may enable businesses to leverage each other's findings resulting in higher quality reports overall. We note that some adjustment to these settings would likely be required to effectively implement a framework for sharing dynamic or 'live' risk information (*see* Framework for understanding and sharing risk information).

912. Aside from maintaining the status quo, we considered the option of amending section 46 of the Act to expand the circumstances in which SAR, or SAR information, can be shared at a reporting entity and agency level. This could include allowing Police employees to share SAR information for specified non-law enforcement purposes, such as for tax administration purposes, or providing information about bankrupt companies going through insolvencies. It could also include allowing businesses to disclose to offshore parent companies where there is no DBG formed, to enable the parent company to be aware of the risks the subsidiary is exposed to. Finally, this could include allowing businesses to share SAR information with each other in certain circumstances, such as with another business involved in a transaction or activity to ensure that all relevant information is provided to the FIU, including through a single SAR.

913. Submitters largely agreed the current restrictions impact on the ability to detect money laundering, terrorist financing and other criminal activity. Submitters supported expanding the circumstances in which SAR information could be shared, noting this would ensure a more holistic approach to financial crime risk management and improve SAR processes between reporting entities. Submitters also acknowledged the potential benefit of a single report combining information from both reporting entities rather than double reporting.

914. Accordingly, we recommend progressing options to expand the circumstances in which SAR information can be shared. In consultation with the private sector, agencies should undertake analysis to progress options for businesses to be able to share information before submitting a SAR and/or work together to produce a SAR. This will ensure the origin of suspicious funds are properly identified and that SARs are of maximum use to the FIU and law enforcement agencies. This is in line with our general recommendation to create a framework for sharing dynamic information about risks and threats (*see* Recommendation R10).

915. We recognise this recommendation has substantial privacy impacts. As such, it should only be progressed subject to a full privacy impact assessment and consultation with the Privacy Commissioner. In particular, the assessment should identify what safeguards are required to ensure that SAR information is shared and used appropriately, with those safeguards balanced against the potential benefits of a more collaborative approach between agencies and businesses.

Recommendation

R196. Progress options for amending section 46 of the Act to expand the circumstances in which SAR information can be shared between agencies and reporting entities. This should be subject to appropriate conditions determined by analysis of the privacy risks and impacts and in consultation with the private sector and the Privacy Commissioner.

7.2. Prescribed transaction reports

916. Prescribed transaction reports (PTRs) were introduced in 2017 to collect financial intelligence on the use of cash and the movement of funds in and out of New Zealand. Unlike SARs, PTRs are a "bulk" information gathering process: businesses are required to submit a PTR for all relevant transactions exceeding a specified threshold – NZD 1,000 for international wire transfers and NZD 10,000 for cash transactions. Reports include details of the transaction, including the customer, the amount, or the name and location of parties to the wire transfer.

917. PTRs contribute to the intelligence picture across the entire financial system, providing necessary statistics and useful intelligence on the flow of cash and money in and out of New Zealand. PTRs also make certain money laundering and terrorist financing typologies more difficult to hide, and in turn, improve the detection and disruption of organised crime, fraud, and tax evasion

7.2.1. Types of transactions requiring PTRs

918. Two types of transactions are currently declared as "prescribed transactions": international wire transfers exceeding NZD 1,000 and domestic physical cash transactions exceeding NZD 10,000.

919. For international wire transfers, the PTR reporting requirements apply to an ordering and beneficiary institution of an international wire transfer, utilising the definitions in section 5 of the Act. However, and as discussed in the Preventive Measures section, these definitions do not reflect the technical and practical reality of wire transfers (*see* Terminology involved in a wire transfer). This creates uncertainty about the application of the provisions and in turn about whether a PTR is required in some circumstances, including certain currency exchange transactions. This has significant compliance impact on businesses, has led to inconsistent approaches being taken by government and industry, and ultimately undermines the effectiveness of the PTR regime.

920. We have recommended repealing and replacing the wire transfer provisions entirely (*see* Recommendation R167). which will also clarify the circumstances in which a PTR is required. However, these legislative changes are likely to take several years. We therefore considered whether we should issue regulations in the interim to bring clarity to businesses to the application of PTR requirements. This includes clarifying PTR requirements for certain types of transaction in the banking sector, such as MT202 transactions and some currency exchange transactions, as well as banks transacting with each other. In addition, regulations could clarify that PTR is required in the MVTS sector when a provider's business model involves making cash deposits into a customer's bank account to settle inbound remittance.

921. In the short term, we therefore recommend issuing regulations to prescribe PTR requirements for those circumstances where it is currently unclear. This includes the application of PTRs to MT202 transactions, some types of currency exchange transactions and settling inbound remittances by cash payments into the bank account of a beneficiary. This will provide clarity to businesses until such as time as all definitions are repealed and replaced.

Recommendation

R197. In consultation with the private sector, issue regulations to carve in or carve out prescribed transaction reporting (PTR) obligations in respect of specific transactions, e.g., MT202s and certain currency exchange transactions. This should include requiring PTRs when an MVTS provider deposits cash into a beneficiary's bank account to settle an inbound remittance.

7.2.2. Who is required to submit a report?

PTR obligations for non-bank financial institutions and DNFBPs

922. Due to issues with the wire transfer definitions, it is currently unclear whether DNFBPs and non-bank financial institutions (NBFIs) are required to file a PTR when they transfer or receive funds internationally through the banking system for an underlying client. This means the FIU may not receive valuable information about underlying parties to a wire transfer. For example, if a law firm receives funds into its trust account from offshore to settle a property sale for its client, the bank will file a PTR reporting the law firm as the beneficiary. However, the actual beneficiary is the law firm's underlying client. If only the bank is required to submit a PTR in this situation, the FIU does not receive a report identifying the underlying party. Conversely, if only the law firm had to submit a PTR in this situation identifying the underlying party, the FIU would not receive the information that the bank has about the originator of the transaction offshore.

923. We identified two options to improve visibility and PTR reporting of underlying parties to wire transfers (when a DNFBP or NBFI is involved in the payment):

- **require one party to report:** this option would require either the bank or the NBFI/DNFBP to submit the PTR, with the other party then required to provide the relevant information about the transaction or customer which is required to submit a comprehensive report.
- **both parties report their relevant information:** this option would require both the bank and the NBFI/DNFBP to submit a PTR but with the relevant information they hold about the transaction. The FIU would then combine the two reports in its systems to obtain a complete picture about the transaction. Practically, this could involve the bank submitting most of the transactional information, while the NBFI/DNFBP may only need to submit information about the customer as well as some information about the transaction necessary for the FIU to link the transactions together.

924. Almost all submitters agreed that it is unclear who is required to file a PTR when a NBFI or DNFBP is involved in the payment chain, with submitters noting that this uncertainty is driven in part by differences in interpretation by the supervisors. Submitters considered that legislation or regulatory change is required in order to resolve the issue. We outlined the above options when we conducted targeted engagement workshops in April 2022, and the consensus from attendees was to take a 'both report' approach for DNFBPs given the risks identified in that sector regarding real estate. Attendees were also supportive of agencies exploring whether the same approach should be taken for NBFIs if there are transactions occurring in that sector where this change would provide valuable intelligence.

925. Accordingly, we recommend taking a 'both report' approach to international wire transfers where a DNFBP or NBFI is involved in the payment chain. However, we recommend implementing this approach for DNFBPs and NBFIs separately:

- **for DNFBPs,** we recommend issuing regulations that clarify that a DNFBP is required to submit a PTR with the information they have about their customer when sending or receiving wire transfers with any additional information that is necessary to facilitate FIU linking the DNFBP's report with the bank's report. In addition, these regulations should exempt DNFBPs from complying with the requirements of section 27 and 28 for the transaction.

- **for NBFIs,** in consultation with the private sector, that agencies identify what, if any, wire transfers involving NFBIs should incur separate PTR obligations. Agencies should consider the financial intelligence benefit from requiring NBFIs to separately submit PTRs, balanced against the accompanying compliance costs. For those sectors and types of wire transfer where a separate PTR is justified by the benefit, similar regulations should be issued to those for DNFBPs.

926. We note the "both report" option is less efficient for the FIU, who will need to match the two reports together. We carefully considered the alternative "one report" approach. However, based on feedback from the private sector, we determined this would be unworkable, in particular for banks who rely on automated solutions.[54] As such, we consider the "one report" approach would impose significant and disproportionate compliance costs compared to the "both report" option.

Recommendations

In respect of DNFBPs:

R198. Require DNFBPs to submit a PTR when undertaking or receiving international wire transfers through another reporting entity on behalf of an underlying client. The DNFBP should only be required to submit the relevant information it holds as well as information (e.g., a unique reference number) necessary to enable the FIU to match the complimentary PTR from the other reporting entity.

R199. Declare that the DNFBP is not the ordering or beneficiary institution of a wire transfer when undertaking or receiving international wire transfers through another reporting entity on behalf of an underlying client.

In respect of NBFIs:

R200. In consultation with the private sector, undertake further analysis to identify what, if any, wire transfers involving NBFIs (on behalf of underlying clients) should attract PTR obligations. Then issue appropriate regulations if the benefit of the additional reporting is justified by the costs. If it is not, exempt NBFIs from PTR wire transfer obligations.

PTR obligations for remittance businesses

927. An intermediary institution of an international wire transfer is exempt from the requirement to submit a PTR. Due to the complex ways remitters deliver their services, some remitters are able to argue they are only an intermediary of an international wire transfer and therefore not required to submit a PTR, even though they may be the only party to the transaction that has visibility of the underlying customer. This is because intermediary institutions are currently exempt from submitting PTRs (Regulation 6A of the *AML/CFT (Exemptions) Regulations 2011*), but this exemption may result in unintended gaps in PTR obligations and result in the FIU missing important intelligence about cross border financial flows. In addition, banks also may not realise that a payment into a customer's bank account from a remitter is an incoming international wire transfer and, as a result, not submit a PTR.

928. We recommend removing remitters from the scope of the intermediary institution exemption to ensure that there are no unintended gaps in PTRs in the remittance sector. This recommendation is in line with the limited feedback we received from submitters, which was that remitters should be included in the scope of all relevant requirements relating to PTRs and wire transfers.

[54] Feedback from the banking sector on this alternative was that it would be impossible for automated solutions to distinguish between transactions for their customer and transactions for a customer of their customer.

Recommendation

R201. Amend Regulation 6A AML/CFT (Exemptions) Regulation 2011 to exclude remitters or money or value transfer service businesses from the scope of the exemption.

7.2.3. Applicable threshold for reporting prescribed transactions

929. PTRs are currently required for international funds transfers exceeding NZD 1,000 and large cash transfers exceeding NZD 10,000. These thresholds may no longer reflect New Zealand's risk profile and mean that the FIU does not receive intelligence about risky transactions below the relevant threshold, e.g., terrorism financing or payments for child sexual exploitation.

930. The main options for lowering the applicable threshold for PTRs are to lower the international funds transfer threshold from NZD 1,000 to NZD 0, while the large cash transaction threshold could be lowered from NZD 10,000 to NZD 5,000, NZD 1,000, or NZD 0. A lower transaction threshold increases the volume of transactions that require reporting, particularly for international funds transfers. We estimate that lowering the threshold of NZD 0 for international funds transfers would result in a fifty-fold increase in the number of reports the FIU receives; by contrast, lowering the large cash transaction threshold to NZD 5,000 would likely double or triple the number of relevant PTRs filed. The increase in PTRs will increase costs for some businesses depending on how they are currently submitting PTRs, especially if they are not currently using automated solutions. Even if the businesses are currently using automated solutions, there is still likely to be some costs associated with the change to ensure that the solution is working correctly. There would also be additional public sector costs for the FIU resulting from the significant increase in intelligence received.

931. Submitters were generally unsupportive of a lower threshold for both international funds transfers and large cash transactions. They noted that a lower threshold would significantly increase the number of transactions being reported which would in turn create an operational burden for agencies to use those reports to generate actionable intelligence. Submitters also queried whether there is sufficient justification for a lower threshold, especially given the privacy implications. Submitters also suggested that any changes to the threshold should only be progressed after existing operational challenges with PTRs are resolved.

932. We appreciate the concerns that submitters raised. However, we nevertheless recommend lowering the international funds transfers threshold to NZD 0, as this will ensure that there are no intelligence gaps and will actually make operational analysis more efficient by ensuring the FIU has the full picture of cross border value movement. There have been instances where the NZD 1,000 threshold has limited the ability of the FIU to quickly produce actionable intelligence in high-risk situations, and they have had to rely on information from international partner agencies to obtain a full intelligence picture. A lower threshold may also serve as a deterrent on conducting some transactions, such as payments for online child exploitation, as their involvement in the transaction would be reported automatically to the FIU. Accordingly, we consider that a lower threshold would improve the effectiveness of the regime overall.

933. However, we recognise that there are a number of existing operational challenges with the PTR regime that would be significantly exacerbated by a lower international funds transfer threshold. Accordingly, we consider that the threshold should be lowered only once these challenges are resolved and that sufficient time is provided for businesses to implement the required changes to their systems. This approach will also ensure that the FIU has enough time to build up its capacity and capability to receive the increased volume of reports.

934. With respect to large cash transactions, we recommend conducting an assessment to identify what intelligence value an NZD 5,000 threshold would provide compared to an NZD 10,000 threshold as well as the associated cost to industry. While we agree that cash transactions can be high risk, we note that risk typically increases with the size of the transaction, and lower-value cash transactions may not be as inherently risky as larger

transactions (with the exception of structuring transactions to avoid the threshold). In addition, a lower reporting threshold would require the occasional transaction and high-value dealer thresholds to be lowered, which would impose additional compliance costs on businesses to adapt their systems and conduct CDD on more transactions (*see* Appropriate cash transaction threshold).

Recommendations

R202. In the long term, reduce the PTR threshold for international funds transfers to NZD 0. This change should only be made once operational challenges with the PTR regime are resolved and the FIU has sufficient capability and capacity to receive the increased number of PTRs.

R203. Agencies conduct a cost/benefit assessment to identify what intelligence value a lower large cash transaction threshold (e.g., NZD 5,000) would provide and whether the costs of the change are justified. If the costs are justified, consider lowing the threshold to the appropriate level and adjusting other settings (e.g., occasional transaction thresholds) appropriately.

7.2.4. What PTRs should contain

935. Adjusting the settings for PTRs provides an opportunity to consider the utility of the information being reported to the FIU, particularly if the thresholds for PTRs lowered. Accordingly, we recommend reviewing and, if necessary, adjusting reporting requirements for transactions to ensure appropriate and relevant information is being gathered and reported. If there are changes made, they could be to all PTRs or to a subset of PTRs (e.g., different requirements depending on the value of the transaction). A review of this kind also provides an opportunity for the PTR requirements to reflect and accommodate the incoming ISO 20022 standard, which overhauls the SWIFT messaging system that is used by banks to conduct international wire transfers. It also provides an opportunity to ensure all relevant country information is collected for international funds transfers by requiring the location of the originator's account as well as their address and whether any other information, such as IP addresses, should be provided where relevant.

Recommendation

R204. Review the current requirements specified in the *AML/CFT (Prescribed Transaction Reporting) Regulations 2016* to ensure that only information that is necessary for the FIU to produce relevant intelligence products is reported. This review should also ensure PTR obligations are aligned with ISO 20022 standards as well as ensuring that all relevant country information is collected by requiring the originator's address and location of their account to be collected.

7.2.5. Ensuring quality PTRs are submitted within statutory timeframes

936. PTRs are required within ten working days after the transaction occurs. However, as noted, businesses (particularly banks) rely on automatic reporting solutions to submit their PTRs within the required timeframe. Submitters indicated that automated systems can occasionally encounter technical issues. However, it can be challenging, if not impossible, to resolve technical issues with automated solutions within the current timeframe of ten working days. In addition, some PTRs may require manual intervention and resolution by compliance staff. This can also be challenging within the current timeframe. These issue ultimately impact on the quality of PTR that are submitted to the FIU.

937. We identified two options to address the issues raised by submitters. One option is to extend the statutory timeframe from ten days to provide enough time for any necessary manual intervention on a PTR by compliance staff. Another option is to issue an exemption that businesses can rely on when a technological issue requiring resolution is identified. The business would not be required to continue to submit inaccurate PTRs while they are fixing the technological issue.

938. We did not specifically engage on either of these options in the Discussion Document, but they were discussed as part of the targeted engagement workshops in April 2022. Attendees were broadly supportive of a slight extension in the timeframe for reporting from 10 to 20 working days but had mixed views on a potential exemption. Attendees noted that an exemption may be useful in some circumstances but may inadvertently increase the complexity of the regime and make it less workable overall. Attendees suggested that we continue to explore the option of an exemption with businesses that rely on automated solutions to ensure that it provides the desired regulatory improvements.

Recommendations

R205. Extend the timeframe for submitting PTRs from 10 to 20 days.

R206. Explore the feasibility of a targeted exemption which could apply when businesses identify a technological issue which undermines the accuracy of reports being submitted.

7.3. Border cash reports

939. The Act sets out requirements relating to movements of cash, including bearer negotiable instruments (e.g., cheques, bearer bonds, money orders), into or out of New Zealand. In particular, the Act requires a Border Cash Report (BCR) to be completed and submitted to customs in respect of all importations or exportations of cash exceeding NZD 10,000, which includes cash in the possession of a traveller or cash consigned as mail or cargo. People who fail to declare (or make a false declaration e.g., by entering the wrong amount) commit a strict liability offence.

940. BCRs play a crucial role in preventing terrorists and other criminals from financing their activities or laundering the proceeds of their crimes through the physical cross-border transportation of currency or bearer negotiable instruments. They also improve transparency of cross-border cash movements and add to New Zealand's ability to develop intelligence products regarding threats to the financial system.

941. The Act currently allows for a term of imprisonment of up to three months or a fine of up to NZD 10,000 (or NZD 50,000 for bodies corporate or partnerships) for not declaring or falsely declaring a movement of cash. The Act also allows for the Chief Executive of Customs to summarily dispose of false or undeclared cash by accepting a sum of NZD 500 from the person who failed to comply with their obligations to report the cross-border movement of cash.

7.3.1. Requiring BCRs for other forms of value movement

942. Movements of value across the border that do not involve currency or bearer-negotiable instruments, such as vouchers, casino chips, or precious metals and stones, do not require a BCR. This represents a potential vulnerability that could be exploited, particularly if penalties for falsely or undeclared cash are increased (*see* Recommendation R213). If more dissuasive penalties deter illicit transportation of cash, it is likely movements of value through alternative means will become more common.

943. BCRs in respect of other forms of value movement could be required through issuing regulations and/or amending the Act. For example, regulations could be issued to declare stored value instruments and casino chips as bearer negotiable instruments, which would attract BCR obligations, while the Act could be amended to require BCRs in respect of precious metals and stones. However, requiring a BCR for other forms of value movement may present challenges for detection when moving them across the border and determining the amount of value being moved.

944. Submitters largely supported expanded BCR requirements to other forms of value movement. As such, we recommend amending the Act to require BCRs for stored value instruments (excluding debit and credit cards), casino chips, and precious metals and

stones. While there are challenges for detection of some forms of value movement, we believe this will improve the transparency of cross-border value movement and Customs' enforcement capabilities by allowing them to act where a person is suspected of moving particular items as a form of value movement.

945. We recommend issuing regulations in the short term to address as much of this gap as possible. While this vulnerability will only be fully addressed through legislative change, issuing regulations will partially address the vulnerability, improve Customs' enforcement capabilities, and restrict money laundering and terrorism financing opportunities in the short term. Specifically, regulations should be issued to define stored value instruments and casino chips as bearer-negotiable instruments, which would then trigger BCR obligations if more than NZD 10,000 is moved into or out of New Zealand.

946. We further recommend amending the Act to give Customs a power that provides discretion to prove that a particular form of item located in possession of or consigned by a person is being used for value movement purposes and to investigate whether it is happening or not (e.g., investigating if a flight passenger with a high-risk profile for cash courier movement carrying several high-value watches purchased them legitimately). This will enable Customs to respond to new forms of value movement in the future.

Recommendations

R207. Issue regulations to require border cash reports (BCRs) for stored value instruments and casino chips in the short term.

R208. Amend the Act to require BCRs for stored value instruments, casino chips, and precious metals and stones.

R209. Amend the Act to give Customs the power that provides discretion to prove that a particular form of item located in possession of or consigned by a person is being used for value movement purposes and to investigate whether it is happening or not.

7.3.2. When BCRs should be filed for unaccompanied cash

947. Currently, a BCR is required before cash arrives or leaves New Zealand or is received by a person in New Zealand. The point at which cash is considered brought into or taken out of New Zealand is not defined in the Act, and Customs instead relies on the definitions of import and export in section 5 of the *Customs and Excise Act 2018*. Under this approach, cash leaving New Zealand must pass the 12 nautical mile limit contiguous zone to become an export, but this can cause difficulties for Customs' enforcement of BCR obligations where cash has been intercepted and seized before it has left Customs' control and no report has been filed. Furthermore, the timing of requirements to complete and submit a BCR for unaccompanied cash is not set in the Act. This makes it difficult for Customs to get cash verification processes in place, if needed.

948. There are two options that could address this challenge, which are not mutually exclusive. One option is to define import and export in the Act, rather than rely on the definitions in the *Customs and Excise Act 2018*. Alternatively, and in respect of unaccompanied cash, the Act could require that BCRs are submitted before the cash arrives in or leaves New Zealand. Most submitters were supportive of defining import and export in the Act, with a small number preferring the terms to be defined in other legislation, such as the *Customs and Excise Act 2018*.

949. We recommend defining import and export in the Act. This will improve Customs' enforcement capabilities by allowing them to intervene where they are currently unable to intervene. This change would align these definitions with how Australia has defined import and export in section 57 and 58 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Aus). We also recommend setting the timing of the requirements to complete and submit a BCR for unaccompanied cash movement to 72 hours before the cash arrives in, or departs, or is received from outside New Zealand. This would allow Customs to get cash verification processes in place, if needed. We recommend addressing this issue through regulations in the short term.

Recommendations

R210. Define import and export in the Act.

R211. Set the timing in the Act of the requirement to complete a BCR for unaccompanied cash movement to 72 hours before the cash arrives in or leaves New Zealand and address this through regulations in the short term.

7.3.3. Powers to search and seize cash to investigate its origin

950. Where cash is not declared or falsely declared, Customs officers are able to seize the cash as it becomes a 'prohibited good' under the *Customs and Excise Act 2018*. However, these powers do not apply when the cash has been properly declared, unless the Customs officer forms a suspicion that it is an instrument of a crime or tainted property. This means Customs does not have the ability to investigate when people are attempting to move cash in a suspicious way, despite the risk that they have stated a false purpose or source of funds.

951. To address this gap, the Act could be expanded to include a power, similar to an unexplained wealth order, which requires a person moving suspiciously large volumes of cash over the reporting limit in a suspicious manner or other forms of value (*see* Recommendation R207) to prove that the cash or items being moved have a legitimate origin and for it to be detained in the interim. The Act could also give Customs the power to investigate whether a false declaration has been made. Submitters were generally supportive of allowing Customs officers to search and seize cash to investigate its origins. Some submitters noted that the Customs officer should be required to have formed a reasonable suspicion before being able to exercise the power.

952. We recommend amending the Act to give Customs the power to investigate whether a person has provided false or misleading information in connection with a BCR (section 110 offence) without seizing the cash or item. This would improve Customs' enforcement capabilities by enabling them to investigate whether a false purpose or source of funds has been declared. We believe a power to seize the cash or valuable item(s) is unnecessary and could, without constraints, constitute an unreasonable search and seizure power and unjustifiably limit rights protected by the *New Zealand Bill of Rights Act 1990*.

Recommendation

R212. Expand the Act to give Customs the power to investigate whether a section 110 offence has been committed.

7.3.4. Sanctions for falsely declared or undeclared cash

953. We considered how we can ensure the penalties for non-declared or falsely declared transportation of cash are effective, proportionate, and dissuasive. For larger sums of cash, the existing NZD 500 to NZD 50,000 penalty could be viewed as a 'cost of doing business.' The FATF did not consider the penalty for summary disposal to be sufficiently proportionate or dissuasive and recommended change.

954. There are several ways the penalty for false or undeclared movements of cash could be more proportionate and dissuasive:

- **link the penalty to the amount of cash:** the penalty (or portion of the penalty) could be explicitly linked to the amount of non-declared or falsely declared cash. This would mean that penalties are always in proportion to the seriousness of the offending.
- **increase the overall penalty levels:** the overall penalty levels available in the Act could be increased to ensure that the judiciary can impose more proportionate penalties in respect of undeclared or falsely declared cash movements. However, it will not address the penalty

for where Customs summarily disposes of the matter, and there is a risk that an appropriate penalty cannot be imposed for large cash movements.

- **replace the penalty regime with an infringement regime:** the current penalty regime under section 113 could be replaced with an infringement regime to increase the immediacy of the penalty for those not complying. However, the penalties for infringement offences tend not to be significant and may not allow for proportionate, effective, and dissuasive penalties to be imposed.

955. Most submitters were supportive of the options identified to make the penalty more proportionate and dissuasive. Some specifically called for measures to allow for undeclared cash to be forfeited, generally increase the penalties available, or allow for non-New Zealanders to be deported.

956. We recommend explicitly linking the penalty to the amount of cash that has been falsely or not declared by allowing a penalty of between 15 percent to 200 percent of the falsely or undeclared amount to be imposed by the Chief Executive of Customs and the Court. Specifically, we recommend amending the Act to allow the Chief Executive of Customs to impose penalties of up to 100 percent, with the judiciary able to impose penalties of more than 100 percent following a successful prosecution. Customs and the judiciary would determine the appropriate penalty by considering any aggravating circumstances, including the mode of concealment, amount undeclared, lack of proof of the origin of the funds, and intentionality or repetition of the conduct.

957. We consider that increasing the penalty amounts in this way will help to ensure that penalties are effective and proportionate enough to dissuade offending, irrespective of the amount of cash that is undeclared or falsely declared. This approach will also enable Customs to effectively seize entire amounts of undeclared/falsely declared cash in serious instances by imposing a penalty for the full amount of cash.

Recommendation

R213. Amend the Act to explicitly link the penalty for falsely/undeclared cash to a range of between 15 percent to 200 percent of the falsely/undeclared amount. Penalties of up to and including 100 percent should be imposed at the discretion of the Chief Executive of Customs, with penalties of more than 100 percent to be imposed at the discretion of the judiciary.

7.3.5. Minor changes to border cash reporting

958. We recommend making the following minor changes to border cash reporting:

Issue	Recommendation
BCRs are not necessary for cash on board vessels, such as cruise ships, that is for vessel-related purposes where the cash does not leave the vessel.	Exempt certain vessels, such as cruise ships, from BCR requirements for cash being carried for vessel-related purposes that does not leave the vessel. Address this through regulations in the short term.
Section 69 of the Act requires that a person must not receive cash moved to the person from outside New Zealand. This section is intended to apply only to unaccompanied cash movements, but the current drafting is unclear. Furthermore, it is unclear how practical this reporting requirement is, and also unclear what intelligence value it provides.	In the short term, issue regulations to exempt a person from being required to submit a BCR if they have received an accompanied cash movement so that the obligation only applies in respect of unaccompanied cash. In the long term, consider the practicality of section 69 and the intelligence value provided by these reports; if there is limited value provided, consider amending the Act to remove the obligation to submit a BCR when a person receives a cash movement.

7.4. Privacy and protection of information

959. The Act requires significant personal and private information to be collected, stored, and in some circumstances, provided to AML/CFT supervisors or other agencies. As such, it is important that the Act's purposes do not undermine the public's right to privacy, particularly with respect to the collection of financial intelligence

7.4.1. Requiring mandatory deletion of financial intelligence

960. There is no retention period specified in the Act for how long the FIU can hold financial intelligence reports. This means that agencies may not be complying with Privacy Principle 9 of the *Privacy Act 2020*, which states that organisations should not keep personal information for longer than it is required for the purpose it may lawfully be used. The Act could be amended to state a retention period for reports received by the FIU, which could specify different periods based on the type of report received. In addition, the FIU could update its privacy procedures to specify when and how financial intelligence will be deleted.

961. Most submitters agreed information held by the FIU should be subject to a retention period. However, there was no consensus on timeframe with submitters suggesting between three and ten years. Some submitters considered information should be deleted once the purpose for collection is over, while others noted it can be difficult and operationally burdensome to comply with deletion requirements.

962. In line with feedback, we recommend amending the Act to include a retention period for reports received by the FIU. An appropriate retention period should be developed in consultation with the FIU and the Privacy Commissioner and may be different for PTRs, BCRs and SARs respectively. PTRs and BCRs indiscriminately collect personal information relating to transactions or cross-border movements of cash. By contrast, the receipt of a SAR indicates that a business has become suspicious about a customer's activities – serious offences, including money laundering, have no limitation for when a prosecution could be brought meaning that SARs may be valuable many years after they were received. As such, we suggest that the FIU should not be able to keep PTRs and BCRs (or the personal information within those reports) for as long as they can keep a SAR.

963. In the interim, we recommend the FIU, in consultation with other agencies and the Privacy Commissioner, review and update its privacy policies to specify when it will destroy reports received or remove the information within those reports. These operational policies should then be amended in the Act itself.

Recommendations

R214. In consultation with the FIU and the Privacy Commissioner, amend the Act to specify the length of time personal information received in a SAR, PTR, or BCR can be held by the FIU. This timeframe will likely be different for PTRs and BCRs compared to SARs, due to the different nature of the reports.

R215. In the interim the FIU should, in consultation with other agencies and the Privacy Commissioner, review and update its privacy policies to specify when it will destroy reports received or remove personal information within those reports to comply with Privacy Principle 9 of the *Privacy Act 2020*.

Ministry of Justice
Tāhū o te Ture

justice.govt.nz

info@justice.govt.nz

0800 COURTS
0800 268 787

National Office
Justice Centre | 19 Aitken St
DX SX10088 | Wellington | New Zealand