MINISTRY OF JUSTICE
Tāhū o te Ture

Regulatory Impact Statement: AML/CFT Statutory Reform

Decision sought	*Final Cabinet decisions on amendments to the Anti-Money Laundering and Countering Financing of Terrorism Act 2009*
Agency responsible	*Ministry of Justice*
Proposing Ministers	*Hon Nicole McKee, Associate Minister of Justice*
Date finalised	*18 June 2025*

Contents

s9(2)(d)

Acronyms and terms used in this paper

The Act	The AML/CFT Act 2009
AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism
AML/CFT Supervisors	The Department of Internal Affairs (DIA), the Financial Markets Authority (FMA), and the Reserve Bank of New Zealand (RBNZ), are the entities which regulate reporting entities covered by the Act
AUSTRAC	Australian Transaction Reports and Analysis Centre (Australian supervisor and FIU equivalent)
BO	Beneficial Ownership
CDD	Customer Due Diligence
DBG	Designated Business Group
DNFBP	Designated Non-Financial Business or Profession
FATF	Financial Action Task Force (intergovernmental AML/CFT body and standard setter)
FATF Recommendations / Standards	The international standards on combatting money laundering and the financing of terrorism and proliferation
FIs	Financial Institutions
FIU	Financial Intelligence Unit (within the NZ Police)
s9(2)(d)	s9(2)(d)
IAG	Industry Advisory Group
MER	Mutual Evaluation Report (undertaken by the FATF)
ML/TF	Money Laundering/Terrorism Financing
NRA	National Risk Assessment on Money Laundering, Terror Financing and Proliferation Financing 2024
NCC	National Coordination Committee established under the Act
PF	Proliferation Financing
PAOB	Person acting on behalf (of a customer)
PPR	Policies, procedures and controls
Programme	AML/CFT Compliance Programme
PTR	Prescribed Transaction Report
RE	Reporting Entity
RIS	Regulatory Impact Statement
RSA	Russian Sanctions Act 2022
SAR	Suspicious Activity Report
Statutory Review	2022 Statutory Review of the AML/CFT Act 2009
TCSP	Trust and Company Service Provider
TFS	Targeted Financial Sanctions
TSA	Terrorism Suppression Act 2002
VASPs	Virtual Asset Service Providers (e.g. virtual currency exchanges)

Summary: Problem definition and options

What is the policy problem?

There are deficiencies and gaps in the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) that reduce its effectiveness and efficiency in deterring, detecting, and preventing money laundering and terrorism financing and tackling wider crime. Without intervention to address these issues businesses will continue to face unnecessary costs and S9(2)(d) [redacted].

What is the policy objective?

The work programme seeks to meet three high-level policy objectives:

- Ensuring the AML/CFT system is effective in meeting the purposes of the AML/CFT Act
- Reducing unnecessary compliance costs for businesses.
- S9(2)(d) [redacted]

What policy options have been considered, including any alternatives to regulation?

Policy options have been considered in the following five areas, identified by Cabinet as providing the greatest potential to achieve the objectives within time and resource constraints:

- **Customer due diligence (CDD)** – options to enable businesses to take a more risk-based approach to CDD obligations, while not compromising the requirement to apply robust AML/CFT controls to high-risk situations.
- **Designated Business Groups (DBGs)** – options to ensure reporting entities can take advantage of the efficiencies of operating in groups while effectively managing associated group risks.
- **Agency Powers** – options for improving the effectiveness of the Police Financial Intelligence Unit.
- **Offences and penalties** – improving the Act's effectiveness by proposing new and updated offences and penalties.
- **Targeted financial sanctions (TFS) and proliferation financing** – supports access to the international financial system through the establishment of a statutory supervision regime for TFS compliance.

The Minister has recommended a package of options across all five areas in the attached Cabinet paper.

The status quo or "do nothing" option would leave the gaps and deficiencies in these areas unaddressed resulting in a less effective and efficient AML/CFT system. This would negatively affect our ability to detect, deter and prevent money laundering and terrorism financing

(ML/TF), erode New Zealand's international reputation S9(2)(d) [redacted]

What consultation has been undertaken?

The Ministry of Justice (Ministry) undertook a statutory review of the Act in 2022, which informed Cabinet decisions on the legislative work programme and subsequent scope of issues and options. The review consulted with a representative Industry Advisory Group (IAG) of stakeholders and peak bodies from across the AML/CFT system and across government.

We have subsequently consulted with the IAG on the proposed options under each issue through a series of workshops and discussion documents in late 2024-early 2025. Sector supervisors and relevant agencies have also been consulted. Broader public consultation has not been undertaken due to time constraints in meeting legislative timelines and objectives.

Is the preferred option in the Cabinet paper the same as preferred option in the RIS?

The preferred options for changes to agency powers in the Cabinet paper differ from those in the RIS:

- Gathering intelligence from non-reporting entities – the Ministry prefers *Option Two: List of prescribed entities*, the Minister prefers *Option One: FIU discretion*.
- Monitoring order conditions – the Ministry prefers *Option One: authoriser uses discretion* while the Minister prefers *Option Three: mirroring a production order*.
- Freezing powers – the Ministry prefers *Option One: FIU discretion* while the Minister prefers *Option Three: Judicial approval*.

All other preferred options are the same.

Summary: Minister's preferred option in the Cabinet paper

Costs (Core information)

Outline the key monetised and non-monetised costs, where those costs fall (e.g. what people or organisations, or environments), and the nature of those impacts (e.g. direct or indirect)

Regulated groups (reporting entities):

- One-off and ongoing costs associated with changes to AML/CFT programmes to consider new customer due diligence (CDD) settings, the addition of TFS compliance requirements and group-wide programmes (for a subset of reporting entities operating in designated business groups (DBGs)).
- Costs associated with supporting information requests from the FIU under new powers.
- Higher penalties for non-compliance with the provisions of the Act.

Regulatory (single supervisor):

- One-off implementation costs to produce guidance and upskill staff on new requirements.
- The establishment of a TFS supervisory capability.

Police (FIU)

- Additional resourcing to analyse data and investigate cases generated by the introduction of TFS requirements on reporting entities.

All costs are direct costs.

Benefits (Core information)

Outline the key monetised and non-monetised benefits, where those benefits fall (e.g. what people or organisations, or environments), and the nature of those impacts (e.g. direct or indirect)

AML/CFT System:

- A more effective and efficient AML/CFT system which reduces unnecessary costs on businesses and enables government and private sector resource to be directed towards the areas of highest ML/TF risk.
- s9(2)(d) [redacted].

Regulated groups (reporting entities):

- Significant ongoing reduction in CDD costs associated with a more risk-based approach.

Regulator (single supervisor):

- More efficient supervision of business groups.
- Key information and intelligence improvements due to the collection of information related to the TFS risk environment.

Police (FIU)

- More effective and efficient FIU resulting in greater ability of Police to investigate and prevent ML/TF activity, including sanctions related cases.

Other:

- Improved sanctions oversight for MFAT from greater TFS information collection and supervision.
- The New Zealand public have improved access to banking products and financial inclusion as a result of CDD reforms.

Balance of benefits and costs (Core information)

Does the RIS indicate that the benefits of the Minister's preferred option are likely to outweigh the costs?

We consider that the combined benefits of these proposals to New Zealand's AML/CFT system and reputation outweigh the costs imposed on government and reporting entities.

The proposed interventions will improve the effectiveness and efficiency of our AML/CFT system – ultimately strengthening our ability to prevent money-laundering and the harm it, and the criminal activity it fuels, impose on our society.

Reporting entities will face some additional costs to comply with the introduction of TFS compliance and other changes to DBGs and CDD. We consider these are partially offset by the reduction in costs associated with more risk based CDD and other minor technical changes that will provide relief to industry.

s9(2)(d) [redacted]

Implementation

How will the proposal be implemented, who will implement it, and what are the risks?

Cabinet has agreed to structural changes to the AML/CFT System including the establishment of a single supervisor (the current supervisors are the Department of Internal Affairs (DIA), Reserve Bank of New Zealand (RBNZ) and the Financial Markets Authority (FMA)) and introduction of an industry levy. The single supervisor will be the central regulatory agency in the AML/CFT system and will implement the new arrangements for TFS, CDD and DBGs.

Police will be key to the implementation of TFS and use the expanded agency powers. The FIU expects it will require additional resource to fulfil its intelligence functions in relation to TFS and to make full use of its information gathering powers.

Legislation is required to give effect to these proposals. The Government intends to introduce a Bill in Q2 2026 with the intention of enactment by Q2 2027. There will be a one-year transition period (Q2 2027 – Q2 2028) for reporting entities to become familiar with the changes and make the necessary transition. If the supervisor considers additional implementation time is required for businesses, they will be able to take an "assisted compliance" approach for a period of time or for specific issues as appropriate.

The proposed funding model (being progressed separately to the proposals in this RIS) will see the industry regulation component of the system funded out of a levy, whilst the criminal justice component remains Crown funded. The levy is anticipated to begin collection in mid-2027 in time to support the implementation of these proposals and the transition period.

Limitations and Constraints on Analysis

Analysis has been constrained by the limited time available for consultation prior to the next FATF assessment period. This constraint is partially mitigated through the 2021 MER and 2022 Statutory Reform processes which undertook extensive reviews of the AML/CFT Act and informed Cabinet decisions on the legislative work programme and subsequent scope of issues and options.

I have read the Regulatory Impact Statement and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the preferred option.

Responsible Manager(s) signature:

Carole Greaney

Caroline Greaney
Deputy Secretary, Policy Group
Ministry of Justice
18 June 2025

Quality Assurance Statement	
Reviewing Agency: Ministry of Justice	**QA rating:** Meets
Panel Comment: The Ministry of Justice Regulatory Impact Analysis Quality Assurance Panel has reviewed the Regulatory Impact Statement (RIS) - AML/CFT Statutory Reform - prepared by the Ministry of Justice and consider that the information and analysis summarised in the RIS **meets** the Quality Assurance criteria.	

Section 1: Diagnosing the policy problem

What is the context behind the policy problem and how is the status quo expected to develop?

AML/CFT system

1. Money laundering enables and incentivises offending that adversely impacts on New Zealand communities. The Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) System plays a pivotal role in detecting and deterring money laundering and terrorism financing (ML/TF) and is a crucial element in New Zealand's effort to combat serious and organised crime as well as terrorism.

2. The AML/CFT System is primarily set out in the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the Act) and accompanying regulations. The Act is intended to enable a risk-based regime that focuses government and private sector resources on the areas of highest risk. The purposes of the Act 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).
   - Contribute to public confidence in the financial system.

A risk-based approach

3. A risk-based AML/CFT system assesses money laundering and terrorism financing risks at the national, sectoral, and business levels. Government resource and regulation are then targeted to those risks identified through the national and sectoral assessments. A risk-based approach helps ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified and that government and business resources are allocated efficiently.

4. The Act imposes obligations on businesses that are intended to help them to identify the risks of ML/TF that they might face and to put measures in place to mitigate those risks. Effective preventive measures should 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 businesses to take innovative approaches to managing their risk.

Two reviews of our AML/CFT system found issues in our statutory framework

5. The 2021 FATF Mutual Evaluation Report[1] (MER) on New Zealand's AML/CFT measures and the 2022 Statutory Review of the Act (the Statutory Review),[2] have identified deficiencies within the Act that create unnecessary regulatory burden and do not comply with international standards.

[1] New Zealand's measures to combat money laundering and terrorist financing.

[2] Report on the review of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.

FATF Mutual Evaluation Report

6. The FATF sets international standards to prevent ML/TF and evaluates how members have implemented those standards, including whether countries have enacted the necessary laws to give effect to the standards. New Zealand is a member of the FATF and engages at the regional and plenary level to update standards and contribute to mutual evaluations of other members.

7. The 2021 MER identified 12 areas where New Zealand only partially complied[3] with the standards and recommended seven priority actions, of which, the following four have direct regulatory implications:[4]

   - Improve the availability of accurate and current beneficial ownership information on legal persons.

   - Ensure that supervisors have a sufficient range of sanction powers and sanctions that are effective, proportionate, and dissuasive.

   - Give clear powers and mandates to appropriate agencies to supervise and enforce targeted financial sanctions (TFS) obligations.

   - Update New Zealand's laws and regulations to address gaps and vulnerabilities including shortcomings relating to licensing and registration of financial institutions (FIs) and designated non-financial businesses or professions (DNFBPs).

8. In 2028-29, the FATF will conduct the next evaluation of New Zealand's AML/CFT system. New Zealand will be assessed against new and updated standards,[5] and will be expected to have acted on, if not completed, all of the 2021 MER recommended actions.

9. S9(2)(d) [redacted]

10. The FATF MER will also consider effectiveness, i.e. how well does our AML/CFT system achieve its stated outcomes and prevent, detect and deter money laundering. Compliance with technical standards and effectiveness are strongly linked (a

---

[3] Partially compliant and non-compliant outcomes are counted as "fails" for the purposes of the MER.

[4] The remaining three actions are to consolidate implementation of Phase 2 of the AML/CFT Act, improve the FIU's tools for prioritisation, database integration and analysis of financial intelligence and to take steps to sustain the recent increase in money laundering prosecutions.

[5] Eight FATF recommendations have been updated since New Zealand's last MER in 2021.

S9(2)(d) [redacted]

jurisdiction's system is very rarely, if ever, assessed as effective without also demonstrating strong compliance with standards).

11. The MER will assess effectiveness through 11 "immediate outcomes" (IOs)[7]. Much like the FATF Standards, the IOs incorporate the entire AML/CFT system and extend beyond the scope of the AML/CFT Act to other legislative and operational settings across government. The issues and options presented in this RIS largely focus on compliance with the FATF Standards (as necessary for effectiveness and s9(2)(d) [redacted] However, additional non-legislative workstreams outside the scope of this RIS are underway which will further the effectiveness component of the 2028/29 MER.

2022 Statutory Review

12. The Ministry's Statutory Review conducted a broad review of the AML/CFT system that considered the FATF recommendations and whether the Act operates efficiently and effectively. The Statutory Review identified that some requirements in the Act are overly prescriptive and efforts by agencies and businesses are not always being prioritised towards areas of highest risk. This makes it harder and more costly for businesses to comply with the Act, and ultimately undermines efforts from businesses to detect and deter ML/TF.

Our AML/CFT system has matured but needs to keep pace with a challenging environment

13. The AML/CFT system has matured since legislation was enacted in 2009 and the scope of the Act was extended to include "phase two reporting entities" (i.e. the accountancy, legal, real estate and other non-financial sectors) in 2015-2016. Phase two reporting entities are now familiar with their obligations and the controls required to mitigate their risks.

14. At the same time, ML/TF is becoming more sophisticated and harder to detect and deter. The New Zealand National Risk Assessment on Money Laundering, Terrorism Financing and Proliferation Financing 2024[8] (NRA) notes increasing volumes and values of fraud crime as a driver of money laundering, and that the banking sector, money transfer services, and virtual asset service providers (VASPs) remain highly vulnerable to ML/TF.

Steps under way

15. In response to these reviews and to keep pace with the changing environment, Cabinet has agreed to an AML/CFT legislative work programme consisting of three interdependent workstreams (ECO-24-MIN-0220 refers).

- **Workstream 1**: immediate regulatory relief via the Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill (introduced in December 2024).[9]

---

[7] For example, IO5: "Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing and information on their beneficial ownership is available".

[8] https://www.police.govt.nz/about-us/publication/national-risk-assessment-nra

[9] See the associated RIS here: Regulatory-Impact-Statement_-Regulatory-Systems-Justice-Amendment-Bill-package_FINAL.pdf

- **Workstream 2**: structural changes to improve system efficiencies and create a sustainable funding model through the introduction of an industry levy.[10]

- **Workstream 3**: changes to regulatory settings that S9(2)(d) deliver further regulatory relief to New Zealanders.

16. The changes proposed under Workstream 3 are the focus of this regulatory impact statement (RIS).

17. Workstream 2 will establish a single supervisor and introduce an industry levy to provide a sustainable funding mechanism in line with cost recovery principles. A more efficient supervisor and a sustainable funding model is key to the implementation of Workstream 3 initiatives as a number of the options considered in this RIS rely on levy funding or on supervisory support for implementation. A single supervisor also provides economies of scale and consistency which will increase the impact and lower the cost of implementing the proposed initiatives. Cabinet has approved these changes and a Bill is being drafted. The Government intends to introduce a Bill in Quarter Three of 2025.

What is the policy problem or opportunity?

Problem Definition

18. The MER and Statutory Review have identified deficiencies and gaps in the ACT/CFT system that reduce its effectiveness in deterring, detecting and preventing ML/TF. In addition, the Review found that the AML/CFT system is not sufficiently risk based and that some requirements in the Act are overly prescriptive. This approach results in increased regulatory burden and inefficient resource allocation by government and businesses.

19. S9(2)(d)

What objectives are sought in relation to the policy problem?

20. The Government has three overarching objectives for this work:

- Ensuring the AML/CFT system is effective in meeting the purposes of the AML/CFT Act which are to:

    i. Detect and deter money laundering and the financing of terrorism.

[10] The associated RIS and cabinet material can be found here: AMLCFT_Release_Pack_FINAL.pdf. Changes include amendments to the Act to make CDD more risk-based. The CDD proposals in this RIS are aligned with the changes in the Bill.

ii. Maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the FATF.

iii. Contribute to public confidence in the financial system.

- Reducing unnecessary compliance costs for businesses.
- S9(2)(d)

21. There is a potential tension between effectively meeting the purposes of the Act, S9(2)(d) and reducing unnecessary costs for businesses. Some of the options contemplated in the following sections would introduce new or additional costs on reporting entities.

22. S9(2)(d)

Cabinet has agreed to progress five key issues

23. Five key areas for improvement have been identified as providing the most potential to increase the AML/CFT Act's effectiveness, reduce unnecessary compliance costs for businesses S9(2)(d)

- **Customer due diligence (CDD)** – considers options to enable businesses to take a more risk-based approach to CDD obligations, while not compromising the requirement to apply robust AML/CFT controls to high-risk situations.

- **Designated Business Groups (DBGs)** – proposes options to ensure reporting entities can take advantage of the efficiencies of operating in groups while effectively managing associated group risks.

- **Agency Powers** – considers options for improving the effectiveness of Police's Financial Intelligence Unit.

- **Offences and penalties** – seeks to ensure the requirements of the Act (including new interventions contemplated by this work programme) are effective by proposing new or updated offences and penalties.

- **Targeted financial sanctions (TFS) and proliferation financing** – supports access to the international financial system through the establishment of a statutory supervision regime for TFS compliance.

What consultation has been undertaken?

24. The Statutory Review, which informed Cabinet decisions on the legislative work programme and subsequent scope of issues and options, was heavily consulted on with other government agencies and entities such as the Reserve Bank (RBNZ) and Financial

Markets Authority (FMA), and with the private sector. An Industry Advisory Group (IAG) of selected industry stakeholders and peak bodies from across the AML/CFT System was established in 2021[11] and was consulted on the Review's recommendations.

25. We have subsequently consulted with the IAG on the proposed options under each issue through a series of workshops and discussion documents in late 2024-early 2025 which further refined our options and analysis. Feedback from consultation is included in the analysis for each issue below.

26. Agencies consulted on this RIS and its underlying analysis include RBNZ, DIA and FMA (the sector supervisors), Police (including the Financial Intelligence Unit), Office of the Privacy Commissioner (OPC), Ministry of Foreign Affairs and Trade (MFAT), Ministry of Business, Innovation and Employment (MBIE), Inland Revenue (IR), Customs, Public Service Commission (PSC), Department of Prime Minister and Cabinet (DPMC), and the Ministry for Regulation (MfR). Where relevant, agency views have been included in the analysis of each issue below.

27. Some sector specific industry groups beyond the IAG have been engaged on discrete questions. However broader industry or public consultation (e.g. through a public discussion document) has not been undertaken due to time constraints in meeting legislative timelines and objectives.

Section 2: Assessing options to address the policy problem

What criteria will be used to compare options to the status quo?

28. The objectives inform the following criteria. Each of the criteria have various components which are outlined below:

- **Effective**: Does the proposed change enable the AML/CFT Act to meet its purposes? Is the proposal targeting areas of highest ML/TF in New Zealand? Is the proposal risk-based? Does the change align with international best practice? Is the option future proof? Is it flexible?
- **Efficient**: Does the proposal increase the economic efficiency of the AML/CFT regime? Does it increase the efficiency of implementing existing obligations? If it is a new obligation, is this the most efficient way the obligation can be implemented? Is the change likely to lead to regulatory relief or cost savings to business or government (which can then be refocused on highest risk areas)?
- **Feasible**: Can the change be implemented? Easily or at great cost, risk, or disruption (to the government, reporting entities or wider sector)? Are risk-based approaches clear enough to enable the eventual law to be interpreted and applied consistently?

Additional Criteria

29. Additional criteria have been used for issues with specific features below.

[11] Current members of the IAG include banks, financial services, industry representative bodies, and DNFBPs (such as accountancy and law firms).

Agency Powers

- **Constitutionally Appropriate**: Does the option impact on privacy and human rights, and if so, is it proportionate? Does it impact on the rights of the customer (of a reporting entity)?

Offences and Penalties

- **Proportionate:** Does the option allow for penalties that are commensurate to the harm? Does the option make sense within the regime and predicate offences? Does the option support a coherent and consistent approach to similar behaviour?
- **Dissuasive**: Does the option deter offending and/or incentivise compliance?

Table of assessment criteria by issue

Issue	Criteria
CDD	Effective, efficient, and feasible.
DBGs	Effective, efficient, and feasible.
Agency Powers	Effective, feasible and constitutionally appropriate.
Offences and penalties	Effective, proportionate and dissuasive.
TFS	Effective, efficient, and feasible.

What scope will options be considered within?

The conclusions of the Statutory Review provide the broad scope

30. The Statutory Review made 215 recommendations which have formed the basis of the issue identification and subsequent Cabinet decisions on the scope of the work programme. The recommendations have also informed the options in each of the issues.

31. While non-regulatory options have not been excluded from our analysis, most of the recommendations require regulatory amendments to be implemented. The deficiencies identified by FATF also typically relate to legislative issues or gaps.

32. Overseas jurisdictions are also subject to FATF requirements and provide useful experience to draw from. Where applicable the issue sections draw on overseas interventions as options or to inform the likely impacts, costs and benefits of options.

Work on a beneficial ownership register and additional TSOC recommendations is out of scope

33. A workstream on beneficial ownership information was also identified by Cabinet as an area for improvement. Since then, work on transnational, serious and organised crime (TSOC) has been initiated by the Associate Police Minister. This work includes considering reforms to support better identification of beneficial ownership information for trusts and companies. Decisions on the coordination and progressing of these workstreams have yet to be taken and a beneficial ownership register is accordingly out of scope of this RIS.

34. The Ministerial Advisory Group on Transnational, Serious and Organised Crime (TSOC) has recently recommended several changes to the AML/CFT Act to make it more difficult for criminals to exploit cash payments. Officials were not able to fully consider the implications of these recommendations in time for inclusion in the RIS. The Cabinet paper therefore seeks decisions in principle, subject to further policy analysis on the implications of reform and appropriate penalties.

Issue 1 – Customer Due Diligence

What is the context behind the policy problem and how is the status quo expected to develop?

Context: what is CDD?

35. Customer due diligence (CDD) is a cornerstone of the AML/CFT System, and a core component of every reporting entity's AML/CFT compliance programme.[12] CDD is the process through which businesses develop an understanding of their customers, and the ML/TF risks they pose. Knowing who a customer is, verifying any information provided and understanding their risk profile protects businesses from misuse. Understanding why a customer is forming a particular relationship also enables businesses to properly detect unusual or potentially suspicious behaviour.

36. The FATF Recommendations for CDD set out a framework that allows countries to adopt a flexible set of risk based CDD measures.

37. The AML/CFT Act requires businesses to carry out CDD on customers, any "beneficial owner" of a customer and any person acting on behalf of a customer. There are three types of CDD ("simplified", "standard" or "enhanced") specifying the level of information a business must obtain and verify depending on the type and risk of a customer.

Context: AML/CFT compliance programmes

38. New Zealand's AML/CFT System sets a number of measures and safeguards in place to support a risk-based approach to CDD. These include:

    - Requiring all reporting entities to carry out an assessment of the ML/TF risk they may reasonably be expected to face.
    - Based on that risk assessment, creating an AML/CFT compliance programme (AML/CFT programme) that sets out the reporting entity's policies, procedures and controls for detecting, managing and mitigating ML/TF risk (including those needed to meet CDD obligations).
    - Requiring that the risk assessment and AML/CFT programme must be reviewed and kept up to date by the reporting entity, and subject to an independent audit every three years.

39. The options below consider improvements to simplified CDD and enhanced CDD requirements, and the programme auditing process.

What is the policy problem or opportunity?

CDD settings are not sufficiently risk-based and can be overly prescriptive

40. New Zealand's CDD requirements are inefficient and burdensome on reporting entities, particularly in low-risk situations. Reporting entities are not able to apply a sufficiently

[12] Section 56 of the Act states that reporting entities must establish a compliance program that includes internal procedures, policies and controls to detect and manage the risk of ML/TF. Minimum requirements for a compliance program includes complying with CDD requirements.

risk-based approach to their CDD measures. Industry feedback has indicated that this is resulting in:

- Reporting entities undertaking unnecessary, inefficient, and costly CDD.
- New Zealand losing foreign investment opportunities because large international organisations are unwilling to meet onerous CDD requirements for their employees.
- People being excluded from the financial system because they are unable to provide identity information that can be verified.

41. This can also result in some high-risk circumstances (e.g. where enhanced CDD is required) not being appropriately examined and mitigated by reporting entities because, in some cases, they view the prescribed measures alone as sufficient to manage their risk.

Simplified CDD can be improved

42. The Act currently restricts eligibility for simplified CDD to a limited set of low-risk customers (e.g. public service agencies and registered banks).[13] The statutory review and subsequent industry feedback found that that the Act's provisions for simplified CDD are not used as much as they could be.

43. Industry feedback has also indicated that some areas of simplified CDD are overly prescriptive, limiting its usefulness in low-risk situations. Currently:

- Simplified CDD must include the collection and verification of the name, date of birth and – in a case where a person is acting on behalf of a customer (PAOB) – their relationship to the customer (e.g. an employee delegated authority to make transactions on behalf of an organisation).
- A reporting entity must obtain information on the nature and purpose of a business relationship (even when this can be inferred).
- When conducting CDD on a PAOB a reporting entity must obtain and verify the person's full name, date of birth, and their relationship to the customer. A reporting entity must also verify the person's authority to act on behalf of the customer. Feedback from industry has indicated that obtaining and verifying name and date of birth information from large institutional clients with multiple employees authorised to act is resulting in lost business and investment in New Zealand. Increasingly, customers are refusing to provide this information, citing privacy policies, while noting it is not required in other jurisdictions, such as Australia.

Enhanced CDD can create risk of 'tipping off' criminals and is overly prescriptive

44. When a reporting entity is aware of suspicious activity and a Suspicious Activity Report (SAR) is required, it must conduct enhanced CDD as soon as practicable. Implementing this requirement can be very difficult in practice when reporting entities conduct occasional transactions or activities. There is a particular risk that conducting enhanced CDD in these circumstances could inadvertently "tip off" the customer of a pending law

[13] The full list of customers eligible for simplified CDD is specified in section 18(2).

enforcement interest in them which may result in safety risks to employees of the reporting entity.

45. Regulations require reporting entities to differentiate when they will examine the source of wealth or the source of funds (or both), and require them to apply additional measures, if examination of source of wealth or funds is not sufficient to mitigate the risks.

46. Submitters to the Statutory Review 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.

Approved entity provision is unused and can be removed

47. We have also considered the continued appropriateness of the approved entity provision in the Act. This provision was intended to make CDD more efficient for businesses by enabling them to rely on government "approved entities" to undertake CDD on their behalf. There is no clear incentive to become an approved entity and there are known barriers that exist in the form of risks and costs. No organisations have indicated an interest in becoming an approved entity since the provision was introduced in 2017.

There is a lack of clarity around designated non-financial business and profession trust accounts

48. The legal, conveyancing, accounting, trust and company service provider (TCSP) and real estate agent sectors are known as designated non-financial business and professions (DNFBPs). Many DNFBPs have trust accounts and may receive, hold and transfer funds in or out of these accounts for their clients.

49. Under the Act, CDD requirements explicitly apply to a DNFBP's client. This includes when funds are transacted through a trust account on their behalf. However, it is not currently clear, except in the real estate sector, whether a DNFBP has CDD obligations in relation to a non-client (i.e., a counter-party) when funds are held in a trust account. For example, a law firm may represent the vendor of a property but temporarily hold funds of the purchaser in escrow in its trust account until a contractual condition is met.

50. Some DNFBPs have taken a cautious approach and consider all non-clients as their customers and apply the CDD requirements accordingly. Other DNFBPs have interpreted the Act to mean non-clients are not customers and do not apply CDD requirements to them unless the non-client seeks to conduct an occasional transaction or occasional activity. There are various types of prescribed occasional transactions that require CDD on the basis they are of higher ML/TF risk.

The requirement to 'audit' Programmes creates unnecessary costs

51. Reporting entities have reported that they are having difficulty fulfilling the requirement in section 59(2) of the Act to complete an audit of their risk assessment and AML/CFT programme every three years. In the accounting sector, the term 'audit' is perceived as requiring the completion of an audit in line with Chartered Accountants Australia & New Zealand auditing standards. The requirement for specialised auditors to complete this requirement results in a reduced market of qualified professionals, driving up costs, and impacting the ability of reporting entities to complete their auditing requirements every three years.

What options are being considered?

52. We have considered two option sets which would amend CDD settings across three main areas:

- Simplified CDD
    i. eligibility for simplified CDD measures
    ii. Nature and purpose of business
    iii. Persons acting on behalf of customers
- Enhanced CDD
    i. Identity requirements
    ii. Verification
- Tipping off provisions
    i. Enhanced CDD on submission of a SAR

53. There are also three additional complementary options which address issues with the approved entity provision, DNFBP trust accounts and auditing requirements.

Status Quo / Counterfactual

We do not consider the status quo to be viable

54. Under the status quo, the issues identified above would continue and reporting entities would face higher compliance costs than they would under a more risk-based approach. In addition, we consider that the status quo for simplified CDD would not be fully compliant with recent changes to FATF Recommendation 1, which requires countries to allow and encourage simplified CDD in low-risk scenarios, and that measures are proportionate to the level of risk.

Option One: Improved Status Quo

55. This option proposes improving the status quo settings by:

- Expanding the scope and reducing the verification burden of simplified CDD;
- Expanding the measures that reporting entities can apply when carrying out enhanced CDD; and
- Enabling banks to waive enhanced CDD when they intend to submit a SAR.

Simplified CDD

Eligibility for simplified CDD measures and verification

56. Additional categories of customers would be added to the existing list of prescribed customers eligible for simplified CDD. This would not make any changes to the simplified CDD provisions in the Act but would expand the range of customers eligible for simplified CDD through regulation. Risk assessments have identified two additional categories of customers as being low risk for the purposes of simplified CDD:

- any licensed financial provider in New Zealand; and
- any entity subject to public disclosure requirements in New Zealand.

Nature of the business relationship

57. The Act requires that, where a reporting entity is applying simplified CDD measures, they must still obtain information on the nature and purpose of the proposed business relationship.[14] This option would amend the requirements for simplified CDD to allow reporting entities to infer the business relationship, where they deem it is appropriate based on risk. This would be consistent with FATF guidance.

Persons acting on behalf of a customer

58. There are opportunities for more efficient and risk-based application of PAOB requirements where simplified CDD applies. This option would require a reporting entity to obtain a person's name and date of birth, but only verify the date of birth if the level of risk required it.

Enhanced CDD

59. This option would amend the Act to specify additional measures (e.g. enhanced monitoring of a business relationship or obtaining senior management approval for transactions) that can be applied as part of enhanced CDD. This option would also remove the address verification requirement for enhanced CDD.

Tipping Off

60. This option would amend the Act to enable registered banks to submit a SAR without first carrying out enhanced CDD to avoid tipping off the account holder. All other types of reporting entities would still be required to carry out enhanced CDD as required by the Act. This change aligns with the FATF Recommendations.

Option Two: A more risk-based approach (preferred option)

61. Option Two involves amending the Act to provide reporting entities with greater flexibility to apply CDD measures that are appropriate for their business based on the risk assessment they are required to carry out under section 58.

Simplified CDD

62. This option includes the proposed simplified CDD measures from Option One and would also allow a reporting entity to apply simplified CDD where it has determined there is a low risk. Reporting entities would be enabled to determine the circumstances when simplified CDD could be conducted as part of their AML/CFT programme, and what those simplified measures would be, in addition to those circumstances already listed in section 18 of the Act. The types of simplified measures that a reporting entity could apply include not verifying CDD information, reducing or not conducting ongoing monitoring and inferring rather than collecting information on the nature and purpose of a business relationship. Other measures may also be appropriate. In the case of a PAOB, reporting entities would still be required to verify the authority of a person to act for the customer.

[14] Section 21 of the Act

63. The obligation to obtain information on the nature and purpose of the proposed business relationship[15] would also be amended for simplified CDD so that reporting entities could infer this from the type of transactions or business relationship when it is established.

Enhanced CDD

64. In addition to removing the need for address verification (Option One), this option would amend the Act to enable reporting entities to implement enhanced CDD measures as required to mitigate their risks. This option would mean that, where it is not appropriate, enhanced CDD measures do not need to include examination of source of wealth or funds. What is required would depend on the individual business and the circumstances.

65. It is likely that the sector will seek guidance from the Supervisor on when it is appropriate to conduct alternative forms of enhanced CDD. The Supervisor would be expected to maintain oversight of how reporting entities implement these changes and that the approaches taken are appropriate to the level of risk of ML/TF that reporting entities face.

Tipping Off

66. This option would allow for any reporting entity, when it has formed suspicion and identified that a SAR is required, to decide not to conduct or not to complete enhanced CDD if there is a reasonable belief that this may alert the customer a SAR is being submitted. This goes further than Option One which is limited to registered banks.

Additional amendments

67. The following proposals are complementary to the options above.

Approved entities

68. This option would repeal the approved entity settings from the Act.

DNFBP trust accounts

69. This option would prescribe that a non-client is not a customer of a DNFBP when funds are held in a trust account, unless the non-client seeks to conduct an occasional activity or transaction.

Risk assessment and AML/CFT programme audit requirements

70. This option would amend the Act to enable reporting entities to undertake an independent evaluation rather than an 'audit'. This will allow a broader cohort of accounting sector professionals that hold certificates of public practice to conduct their services. This change aligns with the FATF Recommendations.

---

[15] Section 21 of the Act.

How do the options compare to the status quo/counterfactual?

	Option One – Improved Status Quo	Option Two – Risk Based Approach	Approved Entities	DNFBP trust accounts	Audit requirements
Effective	+ Expands simplified CDD but does not fully meet deficiencies raised by the FATF.	++ Enables greater flexibility for reporting entities and addresses deficiencies raised by FATF.	++ Removes an ineffective provision from the Act.	++ Creates a consistent approach to CDD for DNFBP trust accounts.	++ Enables a more flexible approach that is consistent with FATF guidelines.
Efficient	+ Provides efficiencies in some areas by providing additional options when undertaking CDD.	++ Enables reporting entities to reduce unnecessary measures by applying a more risk-based approach.	++ Simplifies the Act by removing redundant provisions.	++ Clarifies requirements for DNFBP trust accounts.	++ Reduces cost while supporting effective compliance monitoring.
Feasible	++ Industry and AML/CFT agencies did not raise any concerns about the feasibility this option.	++ Aligns with FATF recommendations and is industry's preferred option.	++ Removing the provision is a simple amendment.	++ Feasible and can be supported by supervisor guidance.	++ Feasible and aligned with approach of Australia.
Overall assessment	+ Removes some costs, such as address verification requirements for standard customer due diligence. However, there may still be some compliance costs that are disproportionate to risk.	++ In addition to the benefits of Option One, this option establishes a greater risk-based approach to simplified CDD eligibility and verification and supports a risk-based approach to aspects of enhanced CDD. MoJ notes Police's concerns about a 'race to the bottom' in the application of CDD but considers this can be mitigated by the issuance of supervisor guidance and risk-based supervision.	++ Simple and effective measure to clarify reliance settings in the Act.	++ Clarifies CDD requirements and improves reporting entity compliance.	++ Supports greater flexibility for business in meeting AML/CFT compliance obligations, lowering costs.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Option Two delivers the greatest benefits

71. While Option One would reduce compliance costs for reporting entities, Option Two delivers the most significant long-term reduction in reporting entity compliance costs by aligning with FATF recommendations for risk-based approach to CDD. Enabling reporting entities to take a more risk-based approach to CDD will also make the regulatory regime more resilient and dynamic and reduce the costs associated with regulatory stewardship of the AML/CFT regime.

72. Enabling simplified CDD in low-risk situations will also support greater financial inclusion. The Council of Financial Regulators has highlighted that some New Zealanders struggle to access transaction accounts that facilitate everyday banking activities and is working with industry to develop solutions to improve financial inclusion.[16] Transaction accounts are often a person's first interaction with the financial system and can support progression to other financial products and services over time. Research indicates that ID requirements, proof of address, and complexities of paperwork are the top three barriers impeding financial providers from opening transaction accounts. Giving reporting entities the flexibility to conduct simplified CDD for low-risk products, such as transaction accounts with controls, can enable financial providers to offer this type of product to previously excluded customers.

73. RBNZ is supportive of extending simplified CDD provisions, but raised concerns as to the amount of discretion reporting entities should be given and the risk of remediation or rework by reporting entities. Extending simplified CDD too far may also adversely impact New Zealand's next MER.

74. The proposed changes to enhanced CDD are expected to reduce costs for businesses by enabling reporting entities to undertake more effective and efficient enhanced CDD measures based on their risk assessment rather than mandating specific measures that may not be appropriate to every situation. In addition, enabling reporting entities not to conduct or complete enhanced CDD and instead to submit a SAR should reduce the risk to staff that are currently required to interact with customers in those situations. Providing this option will also meet one of the FATF recommendations; that we permit reporting entities to not pursue the CDD process where it may tip off the customer.

75. Both the Police and DIA raised concerns with the introduction of an anti-tipping off provision. There is a risk that reporting entities would take advantage of such a provision as a way of avoiding their compliance obligation to conduct enhanced CDD, which would affect the preventive aspects of the Act. DIA acknowledges that supervision would be key to mitigating this risk and advises that if such a provision is progressed that the restrictions on the circumstances in which enhanced CDD does not have to be conducted are clearly set out. The RBNZ is supportive of the concept of a 'tipping off' provision but considers the drafting needs to be clear as to when enhanced CDD may not need to be conducted.

[16] The World Bank Global Findex 2021 report estimates that approximately 50,000 adult New Zealanders are unbanked, a significant increase from under 20,000 in 2014.

76. Police also raised concerns about the impact that removing the investigation of the source of wealth or source of funds as a mandatory part of enhanced CDD might have. Establishing the source of funds or wealth is an important element of asset recovery, where the defendant needs to prove their funds/assets are not tainted by criminal activity. Police indicates that its preference is that examining the source of wealth or source of funds remains as a mandatory obligation for reporting entities.

77. DIA's view is that in most circumstances, examination of source of funds or wealth is the best way to mitigate ML risk and that its centrality to enhanced CDD should be maintained in any amendment. DIA broadly considers that Option Two does this, noting the required enhanced CDD measure to be taken is the measure that mitigates the ML/TF risk.

The AML/CFT regime is mature enough to support more risk-based

78. The obligations to assess, detect, manage and mitigate risk already provide the AML/CFT system with a strong basis from which to adjust some areas of CDD to be more risk-based, while not compromising the requirement to apply robust AML/CFT controls to high-risk situations. Reporting entities have also had time to become familiar with their obligations and managing their ML/TF risks (with appropriate supervision). As a result, New Zealand's AML/CFT system can support a shift to a more risk-based approach to CDD in some areas where efficiencies can be gained.

One-off costs are mitigated by long term compliance cost reduction

79. We anticipate that there may be initial one-off costs for reporting entities to amend their AML/CFT systems, processes, procedures and controls to reflect the proposed more risk-based approach. The proposed changes to CDD will, however, reduce reporting entities ongoing CDD and account monitoring costs as well as costs associated with customer onboarding. These reduced costs will enable reporting entities to reallocate resource from complying with CDD requirements for low-risk customers and products to focus on mitigating the more significant risks they face. The Supervisor will also need to update Codes of Practice to reflect the proposed new regime to support those reporting entities that will require assistance to establish their risk-based measures.

80. In addition to reducing ongoing costs for reporting entities, some customers will also benefit from reduced transaction costs, particularly those dealing with reporting entities that directly pass on the cost of verifying their customers identities. The proposed changes may also drive the adoption of innovative solutions and new technology to improve the efficiency of reporting entities' CDD measures.

The Supervisor will be key to ensuring risk-based measures are appropriate

81. While the preferred option for a more risk-based approach to CDD meets FAFT requirements, it does introduce a risk that some reporting entities may engage in a "race to the bottom" where they use simplified CDD as a way of reducing costs and/or attracting customers by not verifying customer identity information regardless of the risk posed by a customer. The role of the new Supervisor will be central to maintaining the integrity of the system by carrying out effective monitoring of the quality of reporting entity AML/CFT programmes and monitor the implementation of those programmes. There may be additional costs for the new Supervisor as a more risk-based approach will require enhanced levels of oversight to ensure that reporting entities are meeting their obligations appropriately.

82. The preferred option should reduce the regulatory stewardship costs associated with maintaining a fit-for-purpose AML-CFT regime. The Act already enables the Supervisor to produce Codes of Practice (and guidance) that provide a statement of practice to assist reporting entities to comply with their obligations. These documents can be used to support reporting entities to interpret and appropriately apply legislative settings. They can be amended to reflect changing standards and circumstances within the broad risk-based approach set by the Act.

Industry and AML/CFT supervisors support the transition to a more risk-based approach

83. Implementing the preferred option is not anticipated to create significant risks or disruption. Engagement with industry (through the IAG) indicates that Option Two is their preferred option, and it also conforms with FATF Recommendations for CDD. DIA, as the intended single Supervisor of the AML/CFT regime, has also indicated its comfort with the proposals.

84. We anticipate that the time between any announcement on the proposed approach and Parliament passing legislation will give the new Supervisor and reporting entities sufficient time to prepare. If there is a need, transitional provisions can provide for a phased implementation so that reporting entities can continue to rely on the existing settings until they develop their own risk-based measures.

The approved entity provision can be removed

85. This option recognises that the approved entity provisions do not work and should therefore be removed entirely from the Act without replacement. We considered options for amending the approved entity provisions to improve uptake such as improving the application process or expanding eligibility to non-reporting entities. However, these options were discounted when industry feedback indicated that they were unlikely to result in any change in the use of the approved entity mechanism.

CDD for DNFBP trust accounts can be clarified

86. We propose to prescribe that a non-client is not a customer of a DNFBP when funds are held in a trust account, unless the non-client seeks to conduct an occasional activity or transaction. A DNFBP with a trust account can be required to implement additional procedures, policies and controls in their AML/CFT programme as required to mitigate and manage the associated risks, including relating to funds of non-clients. This would be a broad requirement, placed in regulations and supported by guidance, placing a positive obligation on reporting entities to take steps proportional to their risks (as identified in their risk assessments) to mitigate the risks associated with transactions made through their trust accounts. These changes address recommendations raised in the Statutory Review of the Act.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	One-off cost of developing risk-based measures to implement proposed changes to the AML/CFT regime.	Low	High
Regulators	One-off cost of Codes of Practice and updating other guidance material.	Low	High
Others (eg, wider govt, consumers, etc.)	Potential increased risk of ML/TF activity if more risk-based CDD leads to lower standards. This can be mitigated by risk-based supervision and guidance.	Low	High
Total monetised costs		N/A	N/A
Non-monetised costs	Costs of reform are low and will be predominantly restricted to the initial implementation phase.	Low	High
Additional benefits of the preferred option compared to taking no action			
Regulated groups	Ongoing reduction in verification, ongoing CDD and monitoring costs associated with expansion of simplified CDD.	High Standard and enhanced customer due diligence represented one of the six largest drivers of AML/CFT compliance cost in a 2021 survey of reporting entities.	High
Regulators	An unquantifiable benefit from the improved functioning of the AML/CFT regime as reporting entities will be enabled to focus on their highest risks.	Medium	Medium
Others (eg, wider govt, consumers, etc.)	Improved access to banking products and financial inclusion, reduced costs due to lower cost of verification (average cost per transaction ranges from \$37.76 per transaction for lawyers to \$355.88 for real estate)	Medium	Medium
Total monetised benefits		N/A	N/A
Non-monetised benefits		High	Medium

Issue 2 – Designated Business Groups

What is the context behind the policy problem and how is the status quo expected to develop?

Designated business groups enable the sharing of compliance obligations and support mitigation of group risk

87. Reporting entities are often part of larger business structures such as parent-subsidiary corporate groups, franchises or networks. In recognition of this, section 32 of the Act makes provision for reporting entities to form designated business groups (DBGs) if they meet certain criteria.

88. A DBG is a group of two or more eligible persons that have elected to form a group to enable some obligations under the Act to be met on a shared basis. By taking advantages of efficiencies across a group, DBGs are a key mechanism for reporting entities to reduce their compliance costs. While a reporting entity ultimately remains accountable for compliance with its own AML/CFT obligations, members of a DBG can rely on each other to carry out obligations, such as:

    - Sharing a compliance officer.
    - Customer due diligence (CDD).
    - Submitting annual reports on behalf of another member of the DBG.
    - Risk assessments.
    - Suspicious activity reporting.
    - Prescribed transaction reporting.
    - Parts of an AML/CFT programme (the policies, procedures and controls in a business to detect and mitigate money laundering and terrorism financing) – such as record keeping, account monitoring and ongoing CDD.

89. DBGs also enable reporting entities to address group risks. Reporting entities operating within a group can introduce or share clients with one another but may come to different conclusions as to customer risk, due to different risk appetites or risk information being available, leading to exploitation of differences by criminals. Through their ability to consider these interactions at a group level, DBGs can support better risk mitigation and lower compliance costs.

The FATF Standards require group-wide programmes

90. DBGs are also the primary way that New Zealand's AML/CFT regime addresses Criterion 18.2 and the related Criterion 23.2 of the Financial Action Task Force (FATF) Standards.

91. Criterion 18.2 requires financial groups (including their foreign branches and majority-owned subsidiaries) to implement group-wide programmes against ML/TF.

92. The FATF defines a **financial group** as a group that consists of a parent company or of any other type of legal person exercising control and coordinating functions over the rest of the group, together with branches and/or subsidiaries that are subject to AML/CFT

policies and procedures at the group level. International banks with New Zealand subsidiaries are examples of financial groups within our domestic AML/CFT regime.

93. A **group-wide programme** is a holistic AML/CFT risk assessment and management across a group. This may include group-wide policies and procedures, group risk assessment, the appointment of a group compliance officer and group audit functions. Reporting entities are already required to develop AML/CFT programmes or abide by provisions that address FATF group requirements on an individual entity basis. A group-wide programme would consider how these measures are extended and implemented across the DBG. We are aware that some sectors (e.g. international banks) are already moving to group compliance programmes across their branches and subsidiaries as a matter of best practice or to comply with home jurisdiction requirements.

94. Criterion 23.2 extends the requirements of 18.2 to groups of **designated non-financial businesses and professions (DNFBPs).** In New Zealand, DNFBPs include the legal, conveyancing, accounting, trust and company service provider (TCSP) and real estate agent sectors. A **DNFBP group** operates under the same structures as a financial group (i.e., parent/subsidiary-branch structure).

95. The requirement for group-wide programmes is dependent on there being some connection between entities in a structure, which makes it possible to set a programme, monitor its implementation, and enforce compliance. In the case of a financial or DNFBP group, this connection is through the parent company or head office.

96. The FATF also asks countries to determine when the requirements for group-wide programmes should apply to **'other DNFBP structures'**. These include DNFBP groups that operate differently to traditional vertical corporate structure, but share elements of common ownership, management or compliance control. Real estate franchises are a common example of other DNFBP structures in New Zealand.

What is the policy problem or opportunity?

97. While the Act allows for the formation of DBGs and the sharing of compliance functions, it does not require group-wide programmes. The FATF identified this lack of a requirement as a deficiency. As a result, New Zealand was rated partially compliant on Recommendation 18, and the related Recommendation 23,[17] in its 2021 MER. S9(2)(d)

98. The status quo also poses challenges for the supervisor in ensuring both group and individual level risks are being managed. One supervisor identified the lack of a designated lead entity responsible for oversight of the group programme makes it difficult for supervisors to engage with large DBGs and ensure they have appropriate policies for sharing and protecting personal information. In addition, a lack of oversight within a group can allow for inconsistent ML/TF risk mitigation and AML/CFT compliance practices within groups or blanket approaches to risk that don't consider the differing contexts of individual members.

[17] Recommendation 23 was amended to largely compliant in the 2024 Follow up Report due to our remedying of other unrelated deficiencies.

99. In addition, criterion 26.4 and criterion 17.3 (and 22.5 for DNFBPs) of the FATF standards essentially require the AML/CFT supervision for financial groups to be conducted at a group level. This is significantly more difficult without a lead entity that has oversight of the activities of the group.

What options are being considered?

100. We have considered options for the scope of a group-wide programme requirement as well as two sub-options for how a preferred option would be implemented.

Status Quo

101. DBGs are voluntary and may choose to share aspects of a group programme among other compliance obligations. While each reporting entity remains responsible for implementing its own AML/CFT programme, as there is no requirement to consider risks across the group it is possible that DBGs are not taking a holistic approach to group risk. The status quo is non-compliant with FATF Recommendations.

Option One: Require DBGs to have a group-wide programme

102. DBGs would remain voluntary but once formed would be required to implement group-wide compliance programmes. This would result in widespread uptake of group-wide programmes as most business groups operate as DBGs given the benefits of being able to share compliance obligations.

Option Two: Group-wide programmes are mandatory for financial and DNFBP groups

103. This option would require reporting entities that meet the definitions of a financial or DNFPB group to implement a group-wide programme. For reporting entities outside these definitions (i.e. 'other financial or DNFBP structures') group-wide programmes would remain voluntary.

104. This option recognises that the FATF Recommendations apply mandatory group-wide programmes to those business groups with traditional corporate structures (i.e. those structures with clear mechanisms for implementing and enforcing compliance with a group-wide programme) but for other corporate structures only asks countries to consider whether ML/TF risks could be better mitigated by requiring group-wide programmes.

Option Three: Group-wide programmes are mandatory for all business groups

105. This option would extend the requirement for group wide programmes to all business groups (financial groups, DNFBP groups and other DNFBP structures).

106. In practice financial groups and DNFBP groups inherently have common ownership and control through the parent-subsidiary relationship. "Other DNFBP structures" can also have shared ownership, control, or management, e.g. a real estate franchise where the franchisor holds compliance functions for all franchisees.

Sub-options for implementing Options 2 and 3

Sub-option A: Mandatory DBGs (preferred)

107. This option would require the formation of DBGs for those groups subject to the requirement under the FATF standards to have a group-wide programme. This is a similar

approach to the one taken by Australia in its recent AML/CFT reforms which requires the formation of "reporting groups" to implement group-wide programmes. Retaining the concept of DBGs would allow groups to continue to share compliance obligations and lower their costs within the known framework of a DBG. It also means that a smaller number of reporting entities are subject to changes to group settings, as those group structures not required to implement group-wide programmes (under Option Two) would be unaffected.

Sub-option B: Prescribing group-wide programmes

108. In this approach, the DBG provisions in the Act would be replaced by prescribed requirements depending on the category of business group. Groups would be automatically formed where they meet a prescribed definition (based on the FATF definitions) and required to implement group-wide programmes. This is the approach taken by the UK and Canadian AML/CFT regimes. While this would achieve similar effect on uptake as making some DBGs mandatory, we consider that removing the concept of DBGs would be more disruptive for established DBGs and impose costs on a wider range of businesses (to implement changes to programmes and sharing of compliance obligations).

Other considerations

Requiring a lead entity

109. This option would require DBGs to have a lead entity to provide oversight of the group programme (if required) and shared compliance activities. This requirement would apply to all DBGs – whether mandatory or voluntary.

How do the options compare to the status quo/counterfactual?

Group-wide programme requirement

	Option One: Require DBGs to have group-wide programmes	Option Two: Group-wide programmes are mandatory for financial and DNFBP groups	Option Three: Group-wide programmes are mandatory for all groups
Effective	0 Ensures DBGs are alive to group-level risks but does not significantly improve FATF compliance over the status quo.	++ Ensures financial and DNFBP groups are alive to group-level risks. Other business groups retain flexibility over forming DBGs. Consistent with FATF Standards.	+ Ensures all business groups are alive to group-level risks. Consistent with, but potentially exceeds the FATF Recommendations by including all 'other DNFBP structures'.
Efficient	-- Disincentivises DBG formation in cases where group-wide programmes would outweigh the benefits of reliance across the group which would worsen ML/TF risk mitigations and increasing compliance costs.	+ A subset of groups will face additional costs to implement group-wide programmes but the option retains flexibility for 'other financial and DNFBP structures' which are more likely to have complex/novel structures.	- A significant number of other DNFBP structures (and some financial and DNFBP groups) would incur additional costs. There is a risk of capturing groups with structures that make implementing group-wide programmes impractical.
Feasible	++ Consistent approach that is relatively simple to implement. DBG settings remain unchanged.	+ Applies existing FATF definitions in the New Zealand context. Requirements would be supported by guidance from the single supervisor.	- Captures a high number of groups with minimal, or no, common ownership, control or management – making it costly and difficult for those groups.
Overall assessment	- Marginally improve compliance practice across DBGs but would fail to meet the objective of FATF compliance.	++ Balances meeting the FATF Recommendations while retaining the benefits and flexibility of the current voluntary DBG settings.	+ Ensures FATF compliance but introduce unnecessary costs on reporting entities operating in non-traditional structures.

Implementing a group-wide programme requirement

	Sub-option A: Mandatory DBGs	Sub-option B: Repeal DBG provisions and prescribe group-wide programmes
Effective	++ Ensures high-uptake of group-wide programmes.	++ Ensures high-uptake of group-wide programmes.
Efficient	+ Amends existing DBG concept, minimising disruption to reporting entities.	- Disruptive to existing DBGs, including those not required to implement group-wide programmes (under Option Two).
Feasible	+ Able to use existing definitions in the Act as the basis for the requirement.	- More technically difficult to implement.
Overall assessment	++ Provides a mechanism for requiring group wide programmes while minimising disruption to existing DBGs.	0 Enable a group-wide programme requirement but is less efficient and more complicated to implement.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

110. **Option Two** and **Sub-option A** are together the preferred option. Under these options, Financial and DNFPB groups must form DBGs and implement group-wide programmes. Groups that are outside of these definitions (e.g. other financial and DNFBP structures) may continue to form DBGs and implement group-wide programmes on a voluntary basis.

111. This approach seeks to preserve the flexibility of DBGs and their ability to lower costs while improving group risk mitigation and FATF compliance. Most submitters to the Statutory Review and IAG participants agreed that groups of businesses should be required to have group-wide programmes, ensuring a common approach to risks across the group. Those opposed were concerned that this requirement could make it more difficult for international businesses to operate in New Zealand, increase compliance costs, and result in businesses being required to manage risks to which they are not exposed.

112. These concerns are mitigated in the following ways:

- Retaining voluntary DBGs for other DNFBP and financial structures preserves flexibility for those groups of reporting entities that are more likely to have difficulty in implementing group-wide programmes. However, they will still be able to form DBGs and share parts of their AML/CFT programmes where appropriate and they wish to do so.
- Ministerial exemptions to DBG provisions can be considered (including with appropriate conditions) for financial or DNFBP groups, where forming a DBG

according to the definition would impose undue compliance costs due to aspects of their operations or structure.

- A group-wide programme will not necessarily mean a 'one-size-fits-all' approach. Rather, DBGs will need to consider at a group level only those AML/CFT compliance obligations (e.g. CDD, including account monitoring on customers, CDD reliance, information sharing safeguards) that cross over different members of a group. As members of a DBG may have differing functions, product offerings and risk profiles, the FATF notes that financial and DNFBP group-wide programmes should be appropriate to the business of the branches and majority-owned subsidiaries.
- Detailed supervisory guidance on group-wide programmes will be developed to support businesses and DBGs to be aware of their obligations and to apply appropriate risk-based programmes. We also anticipate education and outreach to industry regarding the changes to DBGs (and other statutory reform proposals) will help lower compliance costs.
- Group-wide programmes are consistent with the direction of international practice. We are aware that some sectors (e.g. international banks) are already moving to group-wide compliance programmes across their branches and subsidiaries as a matter of best practice or to comply with overseas jurisdiction requirements.

113. Options One and Three have significant drawbacks:

- As DBGs remain voluntary under Option One, it would be possible for eligible groups to not form a DBG (or to disestablish an existing DBG) if they determined the costs of implementing a group-wide programme outweighed the benefits of reliance/sharing within the group. This would reduce both the effectiveness and efficiency of the Act and as group wide programmes ultimately remain voluntary, would not meet the FATF requirements.
- Costs on reporting entities are likely to be higher for Option Three over Option Two given the inclusion of 'other DNFBP structures' which are less likely to already implement group-wide programmes. When consulted, the real estate sector (where franchises are a large proportion of DBGs considered 'other DNFPB structures' in New Zealand) opposed implementing a group-wide programme requirement on 'other DNFBP structures' due to the costs associated with compliance for franchises.

Other considerations

Requiring a lead entity

114. In addition to the preferred option described above we consider DBGs being required to have a lead entity to be an important control to mitigate the risks associated with group reliance and would enable the supervisor to direct its group supervision more efficiently. Australia, in its recent reforms of its AML/CFT regime, has introduced a requirement for reporting groups to have a 'lead entity', to develop and maintain an AML/CTF program that identifies, assesses, mitigates and manages ML/TF risk and ensures AML/CTF compliance across the group.

115. Many DBGs already have a functional lead entity due to the structure of the group (typically the parent company in a financial or DNFBP group) and the benefits of consolidating compliance functions. However, it is likely that there would be additional costs involved for franchise or network structures that do not have a natural organising or controlling function. We consider that any additional cost to such groups is warranted

(with regard to voluntary DBGs) as structures without natural oversight of group activities are more vulnerable to risk and therefore a lead entity is a more important control.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

116. Yes.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups			
Financial and DNFBP groups	Costs associated with developing a required group programme. Costs associated with establishing and/or supporting a lead entity. *We are confident in the degree of impact however, there is some uncertainty in its scope – we lack information on the proportion of DBGs that would be defined as financial or DNFBP groups and the number of reporting entities within those DBGs. Assumptions are based on supervisor and targeted industry feedback but detailed analysis has not been undertaken due to time constraints.*	**Low** for most groups (some groups likely already compliant). **Medium** for subset of groups with structures or operations that are highly independent or complex but where costs are not disproportionate and so do not warrant an exemption.	**Medium**
Other DNFBP structures	Costs associated with establishing and supporting a lead entity. *(Above constraints apply).*	**Low** for most groups (some groups likely already compliant). **Medium** for subset of groups with structures or operations that are highly independent or complex but where costs are not disproportionate and so do not warrant an exemption	**Medium**

Regulators	One off costs associated with production of guidance material to support requirements. There may be some additional DBGs formed as a result of the requirement (and therefore requiring group supervision) however any additional administrative cost is likely offset by efficiencies gained through the requirement for a lead entity.	**Low**	**High**
Others (eg, wider govt, consumers, etc.)	None	N/A	N/A
Total monetised costs		N/A	N/A
Non-monetised costs		Low-Medium	Medium
Additional benefits of the preferred option compared to taking no action			
Regulated groups			
Financial and DNFBP groups	No changes to existing benefits stemming from sharing of compliance obligations within DBGs.	N/A	N/A
Other DNFBP structures	No changes to existing benefits stemming from sharing of compliance obligations within DBGs.	N/A	N/A
Regulators	Efficiency gains from lead entity and group-level supervision of DBGs. Small cost reduction due to automatic formation of some groups (which do not require supervisory oversight to set up).	Medium	High
Others (eg, wider govt, consumers, etc.)	s9(2)(d) [redacted] Improved compliance practice across AML/CFT system as a result of group-wide programme and lead entity requirements – corresponding to improved ability to detect/deter/prevent ML/TF activity.	High	High
Total monetised benefits		N/A	N/A
Non-monetised benefits		*High*	*High*

Issue 3 – Agency Powers

What is the context behind the policy problem and how is the status quo expected to develop?

FIU intelligence gathering powers are essential to detecting and investigating money laundering and financing of terrorism

117. The Financial Intelligence Unit (FIU) is a business unit in the New Zealand Police that is mandated to assist with the detection and investigation of money laundering, terrorism financing and other offences.

118. The FIU collects and analyses reporting received under the Act from reporting entities and external parties. This can range from business-as-usual reporting to reporting on suspicious activity. As such, the FIU is a key part of New Zealand's AML/CFT system as they detect, and gather intelligence on, financial crime that initiates or informs investigations. This helps the Government fulfil its obligations to the FATF, alongside the Government's organised crime strategy, and the overall approach to the prevention and detection of crime.

The statutory review identified areas of improvement for FIU's powers based on New Zealand's last mutual evaluation

119. It is a FATF requirement for FIUs to be able to obtain additional information from reporting entities and have timely access to the information it requires to undertake its functions properly (Recommendation 29).

120. The Statutory Review identified that improvements were needed to enable the FIU to:

- Gather intelligence from non-reporting entities.
- Order ongoing information relevant to high-risk individuals (monitoring orders).
- Establish freezing powers.

121. The recommendations reflect feedback from submitters and are consistent with gaps in the FIU's powers based on comparison with the powers of foreign FIUs. Addressing these recommendations will support law enforcement to detect and deter organised crime.

What is the policy problem or opportunity?

Amendments to the Act are needed to improve FATF compliance and enhance detection and responses to AML/CFT

122. The proposals in this section are intended to enable the FIU to generate a more fulsome picture from suspicious activity reporting and stop preventable harm or crime from occurring. We have analysed the proposals to assess their effectiveness, feasibility and constitutional appropriateness.

Intelligence from non-reporting entities

123. Section 143(1)(a) of the Act enables the FIU to order information from any reporting entities relevant to analysing information received under the Act. While information obtained from reporting entities will provide the FIU with some additional information to understand an intelligence picture, non-reporting entities (such as telecommunications

companies and travel agents) can hold information the FIU cannot access (and is not available under any other power) that is relevant to analysing other intelligence held. Information collected from reporting entities under the current section 143 powers does not always provide all the information needed to determine if a law enforcement investigation should be initiated.

124. In the absence of a power to order information from non-reporting entities, the FIU either relies on incomplete information or must seek non-reporting entity information through production orders. Obtaining a production order can delay the commencement of investigations as, depending on the information needed from non-reporting entities, a number of separate orders may be needed, and orders must also be approved by an issuing officer (outlined in sections 3 and 108 of the Search and Surveillance Act 2012). The time it takes for an order to be approved can vary depending on availability of an issuing officer and time of day and year. The Ministry considers this process could be made simpler and streamlined by expanding the current section 143 powers available to the FIU to include non-reporting entities. FATF has also commented on the need to make greater use of the FIU's intelligence and to initiate more investigations from FIU intelligence alone. This was noted in New Zealand's 2021 MER as an area for improvement.

125. While New Zealand is technically compliant with FATF requirements in this respect, including non-reporting entities in the FIU's information gathering powers would significantly improve their ability to analyse the reporting they receive. Expanding FIU powers to include non-reporting entities will also address FATF comments on the system's need to make greater use of the FIU's financial intelligence and to initiate more investigations from FIU intelligence alone.

Monitoring orders

126. The current section 143(1)(a) powers enable the FIU to obtain details of financial activities once an activity has occurred or financial intelligence reporting has been received. The FIU can order more information from a reporting entity following receipt of information under the Act. However, it cannot order information from reporting entities on an ongoing basis to monitor individuals or situations identified as high risk or time sensitive. For example, where an individual is suspected to be involved in online child exploitation, or where someone is suspected to be fundraising for terrorist activities. The delay between the identification of suspicious activity and obtaining retrospective information risks illicit funds being shifted to avoid detection, or preventable criminal harm occurring before law enforcement intervention.

Freezing powers

127. The FIU is notified by reporting entities of suspicious financial activity that indicates impending harm (e.g. where a scam or fraud has occurred and funds are likely to move offshore, or terrorism financing).

128. The Act does not allow the FIU to direct a reporting entity to block a transaction or freeze an account, for an investigation or to reduce harm. Freezing transactions and/or accounts can be an effective tool to prevent criminal acts and/or to prevent proceeds of crime being moved beyond the reach of law enforcement. The FIU must rely on other powers (such as court processes or disclosing the risk to the reporting entity of facilitating the transaction

or activity) which can be slow and allow illicit funds to move beyond the reach of law enforcement.

129. The next round of FATF evaluations will include a requirement for the FIU, or another competent authority, to be able to take immediate action to freeze a transaction related to money laundering, predicate offences, or terrorist financing, in response to a request from a foreign counterpart (Recommendation 38). New Zealand does not currently meet this requirement whereas several FATF member countries have powers to freeze accounts or stop transactions and some FIUs can freeze accounts as well as transactions.

What options are being considered?

Intelligence from non-reporting entities

Status Quo

130. The FIU can gather intelligence from reporting entities only. Maintaining the status quo does not allow the FIU to fully assess the financial intelligence it receives from reporting entities, nor does it reflect modern business practices where businesses may outsource their compliance functions to non-reporting entities.

Option One – FIU discretion (Minister preferred)

131. This option would provide the FIU with discretion to request information, following the receipt of a suspicious activity report (SAR), from any non-reporting entity business that has an existing business relationship to the person of interest.

132. Option One would provide the FIU with discretion as to which businesses it can obtain further information from. This is similar to the power AUSTRAC (Australia's FIU equivalent) has. This option provides less certainty to non-reporting entities on what their obligations might be under the Act. It would be the costliest to implement as it would require a wide-reaching communications plan to notify a wide range of businesses that they are likely to have obligations under the Act. It would also have the largest impacts on privacy and human rights for the individuals affected.

133. In targeted engagement with agencies, the FIU and the IAG, there was broad support for Option One. However, there were concerns about the power being too broad, providing little certainty to non-reporting entities, and having privacy impacts. It was agreed that having a high threshold for any use of this power would mitigate some of the concerns expressed regarding privacy and feasibility for businesses.

Option Two - Prescribed list in regulations (Ministry preferred)

134. This option would define the non-reporting entities through a list prescribed in regulations. This would restrict and clarify the business sectors included and therefore narrow the scope of information that can be requested by the FIU. This would lower implementation costs and provide more certainty to businesses on their obligations, making it more feasible than Option One. Additionally, by prescribing a limited set of identified business types there would be less impact on individual privacy and human rights than from power with wider scope.

135. While this would help balance feasibility, privacy and human rights concerns, Option Two means the FIU may be unable to access necessary information from entities not

anticipated at the time the list was defined. This may also incentivise the exploitation of businesses not listed.

136. We have considered that the list might be prescribed in legislation rather than regulations. However, this would provide less flexibility when the risk environment changes. Prescribing the list in regulations will achieve the same level of effectiveness and allow for easier amendment. We have therefore discounted this option.

137. While agencies, the FIU and the IAG generally preferred Option One, Option Two would best mitigate privacy impacts and costs while still providing for some flexibility if amendments are needed.

Non-reporting entities - How do the options compare to the status quo/counterfactual?

	Option One – FIU discretion (Minister Preferred)	Option Two - List defined in regulations (Ministry preferred)
Effective	++ Provides the FIU with the greatest ability to gather information.	+ Provides the FIU with the ability to gather information from prescribed non-reporting entities.
Feasible	- Places an obligation on all businesses. Costly to implement and to educate businesses.	+ Scope of the obligation is narrower and easier to implement. Regulations can be amended to account for changing risk environment.
Constitutionally appropriate	- Increases uncertainty for businesses. Larger impact on privacy.	+ Provides certainty for businesses about their obligations. Less impacts on privacy.
Overall assessment	**0** While effective, this option is difficult to implement and may have significant privacy impacts on businesses.	++ This option is preferred as it achieves the best balance between criteria while empowering the FIU to gather the necessary information.

Non-reporting entities – What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

138. Option Two – enable the FIU to order information from a prescribed list of non-reporting entities, defined in regulations – is our preferred option. Although stakeholders preferred Option One, Option Two provides clarity for businesses affected while addressing law enforcement needs, meets the purpose of the Act, and provides more safeguards for privacy and human rights. Additionally, it provides some flexibility to respond to a changing risk environment.

139. The impacts of this intervention are primarily focussed on non-reporting entities who do not currently have any obligations under the Act. There are some general impacts to be managed with reporting entities which includes risks of customers being tipped off and

confidentiality concerns being raised. There are also general privacy and human rights impacts associated with powers like these to consider.

140. An underlying assumption in the analysis for expanding and establishing new FIU powers is the extent to which they will be used. Between 2019 – 2025, the FIU issued 190 requests for information under section 143, approximately 31 requests per year. This reflects the current resourcing of the FIU and that requests for information have been steadily used. Once a decision has been made on which businesses will be affected by this power, those businesses can be engaged to work through the impacts on them.

141. The Ministry considers that, based on the qualitative evidence provided by Police and the FIU, the benefits of expanding the current section 143 powers to include non-reporting entities, outweigh the costs.

Monitoring orders

142. These options explore how the monitoring power might work and be implemented.

Status quo

143. The FIU obtains details of financial activities retrospectively. The delay between the identification of suspicious activity and obtaining information risks illicit funds being shifted to avoid detection, or preventable criminal harm occurring before law enforcement intervention.

Option One – Direct access

144. This option would allow the FIU to directly access information from reporting entities in real time. This option would involve significant investment in a technology solution and have significant privacy implications. As such Option One was regarded not feasible and the least preferred option by stakeholders.

Option Two – Intervals defined by FIU (Ministry preferred)

145. This option would require reporting entities to provide ongoing relevant information at intervals defined by the FIU, rather than at the initiation of a reporting entity report. Option Two provides the FIU with flexibility to respond to an evolving risk environment. While this will involve some increased compliance burden for smaller reporting entities, all reporting entities are currently required to be able to respond to similar requests. It is more likely to be the frequency of these requests that are burdensome for reporting entities as opposed to the process of responding to them itself.

Option Three – Mirror a production order (Minister preferred)

146. Option Three would enable the FIU (following the receipt of information) to apply to the Court for approval to order reporting entities to provide ongoing relevant information. This would be a similar process to getting a production order approved by the Court. Under this process the FIU can apply for an order under the Search and Surveillance Act 2012 (section 71) through the Courts if they are able to satisfy the Courts that they have met the outlined conditions. We consider this option would have a low impact on judiciary time and resources. Based on the current number cases requiring FIU information orders, the number of applications for court orders is likely to be fewer than one per month, and the orders would be relatively simple if aligned with the existing section 143(1) production order regime.

Monitoring order conditions

147. To have appropriate balances on this power, we also need to outline the conditions where the FIU might request an ongoing monitoring order and how this would be authorised. We have identified three options for the conditions where it would be appropriate for the FIU to request an ongoing monitoring order.

Option One – Authorising person to use discretion (Ministry preferred)

148. This option would enable the person authorising the order to exercise discretion as to whether the circumstances are high risk and monitoring is justified (under the direct access or intervals defined by the FIU options). While the discretion would be informed by guidance such as the National Risk Assessment (NRA), this option provides less safeguards for individual privacy and human rights.

Option Two – Circumstances listed in regulations

149. This option would prescribe the circumstances of a monitoring order in regulations (under the direct access or intervals defined by the FIU options). This could include specific offences and other factors such as the likelihood of capital flight.

Option Three - Conditions for application mirror those of production orders (Minister preferred)

150. This option mirrors the conditions for application set out in the Search and Surveillance Act for production orders. This option would outline in the Act that to apply for a monitoring order the FIU must satisfy the Courts that they suspect an offence is, has or will be committed.

151. This option has been added to support the Minister's preferred option of requiring the FIU to apply to the Courts for monitoring orders. The Ministry's preferred option is for the FIU to be able to authorise the use of this power, however if Court approval is required, the Ministry considers mirroring the conditions outlined above is likely to best enable the FIU to operationalise this power.

How do the options compare to the status quo/counterfactual?

Monitoring orders

	Option One – Direct access	Option Two – Intervals defined by FIU (Ministry preferred)	Option Three – Mirror extended production order (Minister preferred)
Effective	+ Effective for the FIU.	++ Effective and allows for bespoke intervals set by FIU.	**0** Would not enable the FIU to respond to a dynamic situation in a timely manner.
Feasible	- Requires significant investment in technological solution.	+ Supported by industry. Increased compliance burden from frequency of request, not the power itself.	- May allow for less flexibility in how reporting entities respond.
Constitutionally appropriate	-	+	++

	Most intrusive and least preferred by stakeholders.	Similar to existing powers to request information.	Judicial authorisation provides stronger safeguards for privacy and individual rights
Overall assessment	- Does not meet feasibility and appropriateness criteria.	++ Effective and feasible for industry with minimal additional privacy impacts.	+ Does not meet effectiveness criteria, but is feasible and constitutionally appropriate.

Monitoring order conditions

	Option One – Authoriser uses discretion (Ministry preferred)	**Option Two – Circumstances outlined in regulations**	**Option Three – Conditions mirror production order (Minister preferred)**
Effective	++ Most effective as it empowers the FIU to be flexible in application of the power.	+ Effective but less flexible.	+ Effective but risks delays to Police investigations.
Feasible	++ Simplest to implement and easily adapted to changing environment.	+ Feasible but slower to adapt to changing environment.	- May allow for less flexibility in how reporting entities respond.
Constitutionally appropriate	**0** Less safeguards for privacy and individual rights.	**0** Greater certainty and safeguards regarding privacy and individual rights.	+ Greatest safeguards for privacy and individual rights.
Overall assessment	++ Provides the most effectiveness while being easy to implement.	+ Suitably effective but less adaptable to changing environment.	+ Least effective given timeliness impacts on Police investigations. Greatest safeguards.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Monitoring orders

152. We recommend Option Two - amending the Act to include a new section enabling the FIU (following the receipt of information) to require reporting entities to provide ongoing information relevant to the order, at intervals defined by the FIU. In targeted engagement with relevant agencies and the IAG, there was broad support for Option Two, and similarities were drawn to the existing Financial Crime Prevention Network (FCPN) process between the FIU and the major banks which is not legislatively supported.

153. Allowing the FIU to monitor high risk individuals or situations through the ongoing provision of information by reporting entities will minimise the risk of illicit funds being shifted to avoid detection, or preventable criminal harm occurring before law enforcement intervention. This power would be restricted to transactions related to high-

risk individuals or situations, relevant to information received by the FIU under the Act. The information requested would largely be restricted to financial transactions, thereby reducing the privacy implications of the power.

154. Situations where a monitoring power could be used include:

- monitoring financial activity of individuals suspected to be engaged in terrorist activity to detect preparation of an attack or travel overseas,
- monitoring financial activity of individuals suspected to be engaged in online exploitation to detect transactions indicative of active abuse i.e. transactions for children's clothes, transactions for payment of abuse material, and
- monitoring financial activity of individuals suspected to be engaged in the illicit drug trade to detect transactions related to shipment or storage of drugs.

155. While Option Three provides more safeguards for privacy as the Court needs to consider that the law enforcement benefits of the monitoring order outweigh any privacy concerns, it may have timeliness impacts on the FIU and Police investigations. Applying to the Court may create time delays that do not enable timely monitoring. This could risk preventable harm or crime from occurring. The Ministry considers this is not effective as it is too prescriptive and would not enable the FIU to respond to a dynamic situation in a timely manner. Additionally, the FIU note that having to meet the threshold for production orders in all cases will mean there will be occasions where there is a justified reason for the FIU to obtain further information (e.g. due to information obtained through a suspicious activity report) but where there is insufficient information to obtain a production order.

156. While this option may be feasible for reporting entities, in consultation the IAG did not consider this option as being any more beneficial than the status quo.

157. The Office of the Privacy Commissioner (OPC) supports this option. They note that due to the privacy intrusion these proposals introduce, their preference is that the power to monitor best sits with the judiciary.

Monitoring order conditions

158. In issuing a monitoring order, our preferred option is for an authorised person to be able to use discretion as to whether there are reasonable grounds to suspect that a crime has been committed, is being committed or will be committed and monitoring is justified to assess this risk (Option One).

159. This will provide enough flexibility for use as the risk environment evolves and enables the FIU to act as suspicious activity arises, whilst still restricting the use of the power to reasonable circumstances, providing for protections on privacy and human rights.

160. The IAG was also generally supportive of this option and shared the FIU's concern that prescribed lists would not future proof the AML/CFT system against shifts in the risk landscape over time and may influence criminal methods.

161. Section 143(1)(a) allows the FIU to make repeated requests for information from reporting entities as a means of monitoring high risk individuals. An ongoing monitoring order would in some cases reduce the compliance burden on reporting entities. One of

the reasons the IAG supported the creation of a power to order ongoing information was because it could reduce the number and frequency of information requests from the FIU.

Other considerations

162. Monitoring orders would be used similarly to powers outlined in section 143(1)(a) of the AML/CFT Act[18] and we consider it appropriate to align the decision-making authority. The power would therefore be an administrative power of the Commissioner, which can then be delegated to a Commissioned Officer, or equivalently senior Police employee. To support the proportionate use of the monitoring power, the requirement for all delegated use of the administrative production order to be reported to the Commissioner should be mirrored. This was supported in stakeholder engagement.

163. To provide additional safeguards we consider a 90-day maximum an appropriate timeframe to further mitigate the risk of unnecessary use of monitoring orders. Legislation would specify that the FIU should request the order be ceased as soon as possible after identifying there is no longer reasonable grounds to suspect illicit activity, or the order is no longer justified based on a reassessment or changes to the risk. To support this, the FIU would develop internal processes around frequent monitoring or assessments of the risk. This was supported in stakeholder engagement.

Freezing powers

Status Quo

164. The FIU is currently not able to direct a reporting entity to freeze a transaction or account.

Option One – Authorising person to use discretion (preferred)

165. The person authorising the order would exercise discretion as to whether the circumstances are high risk and freezing is justified. This discretion should be informed by guidance such as the NRA.

Option Two - Circumstances listed in regulations

166. The circumstances for freezing an account or transaction would be listed in regulations. This could include specific offences and other examples such as the likelihood of capital flight.

Option Three – The Judiciary to approve use of freezing power (Minister preferred)

167. Under this option the power would sit with the Judiciary. This would mean the FIU would be required to apply for an account or transaction freeze with the Judiciary, who would then have to determine whether the request meets the threshold (to be confirmed) and would then approve or decline the request.

[18] Section 143(1)(a): The Commissioner may order production of or access to all records, documents, or information from any reporting entity that is relevant to analysing information received by the Commissioner under this Act, with or without a court order.

How do the options compare to the status quo/counterfactual?

	Option One – FIU discretion (Ministry preferred)	Option Two – circumstances prescribed in regulations	Option Three – Judiciary to approve (Minister preferred)
Effective	++ FIU is able to respond to widest variety of circumstances.	+ Effective, but for a limited set of circumstances prescribed in regulations.	+ Not bound by prescribed circumstances but requires court approval.
Feasible	+ Most flexible option and easiest to implement.	- Less flexible to changing environment.	-- Not sufficiently responsive given time delays in seeking court approval.
Constitutionally appropriate	+ Authorisation, oversight and time period requirements help protect privacy and individual rights.	+ Provides additional certainty to business by prescribing list. authorisation, oversight and time period requirements help protect privacy and individual rights.	++ Court approval provides the greatest protection for privacy and individual rights.
Overall assessment	++ Most effective option.	+ An effective option with minor limitations due to circumstances where the power can be used being prescribed and the feasibility of amending the list	- Timeliness impacts make this power unworkable in time sensitive situations.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

168. Our preferred option is Option One - amend the Act to introduce a new power for the FIU and Police to have discretion to order to freeze one or all accounts belonging to a person of interest in two circumstances:

- when the person authorising the freezing order considers the circumstances are high risk (e.g. terrorism financing, online child exploitation, movement of proceeds of crime offshore), and freezing is justified; or
- when an international FIU requests the FIU freeze a transaction/account.

169. The decision to issue an order would be informed by guidance such as the NRA. This option provides the most flexibility for the FIU to use the power and will most effectively support Police and the FIU to take immediate action to freeze a transaction, meeting the updated FATF requirements and law enforcement objectives. This was the preferred option in engagement with IAG and agencies.

170. Option Two would provide certainty over when the freezing power could be used, however it was discounted as it provides less flexibility for use as the risk environment or FATF guidance changes, and the circumstances prescribed become less relevant.

171. The OPC noted the potential human rights impacts associated with the preferred option and recommend that this power sit with the judiciary instead. They consider human rights impacts are somewhat mitigated by the proposed exemptions for human rights transactions (e.g. food and housing), but that clear operational procedures and safeguards will need to be in place to ensure the power is used correctly. They support the proposed mandatory judicial review of the power.

172. The FIU and the Ministry strongly consider that application to the Court is likely to make the power unworkable as judges are very rarely available out of hours and so may be unable to review a request in time. As this power is intended to be used in emergency or high-risk circumstances, delaying freezing accounts or transactions until the judiciary can approve on the use of the power risks preventable harm or law evasion occurring. This issue could be partially mitigated by expanding authorisation to the broader category of "issuing officers" (as in the Search and Surveillance Act 2012) which would allow for more availability and responsiveness.

173. The Ministry considers that the establishment of a freezing power is reasonable and proportionate to the risk of harm caused by high-risk criminal activity such as terrorism, child exploitation and drug trafficking. We note the concerns raised around human rights impacts, and (with IAG and agency support) anticipate several limitations on the use of freezing powers, in addition to the allowance of human rights exemptions. We consider these requirements will ensure the freezing power does not infringe on New Zealander's right to be secure against unreasonable search and seizure.

Other considerations

174. We consider the following requirements will ensure the freezing power does not infringe on New Zealander's right to be secure against unreasonable search and seizure:

- **Authorisation**: Legislation will specify the Commissioner of Police is authorised to carry out the power and that the Commissioner may delegate the power to the FIU and other relevant parts of Police (e.g. Asset Recovery Unit), at the level of inspector to ensure 24/7 capability to respond to high-risk circumstances (including SARs and other intelligence).
- **Oversight**: We consider that any exercise of this power should be reviewed by the Courts within a legislated period of time. This is expected to have a low impact on court time and resources, due to this being a power reserved for high-risk and immediate situations.
- **Maximum time period**: We consider a freezing order should be for a maximum of three working days. If additional time is required, The FIU and Police could apply to the Courts to extend the freeze for a further 30 days. This aligns with similar powers used overseas.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

175. The Minister's preferred options differ for all proposed amendments. For gathering intelligence from non-reporting entities, the Ministry prefers Option Two: List of prescribed entities, the Minister prefers Option One: FIU discretion. For monitoring order conditions, the Ministry prefers Option One: authoriser uses discretion while the Minister prefers Option Three: mirroring a production order. Lastly, for freezing powers, the Ministry prefers Option One: FIU discretion while the Minister prefers Option Three: Judicial approval. We have reflected the Minister's preferred option in the marginal costs and benefits analysis below.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
	Additional costs of the preferred option compared to taking no action		
Regulated groups *(non-reporting entities)*	***Intelligence from non-reporting entities.*** These groups (i.e. all non-reporting entities) have not been engaged on this issue. It is likely some businesses will have time and resourcing costs incurred by information requests under this power. These costs are likely to be low given the very low numbers of orders issued to reporting entities and subsequently the low numbers of expected orders for non-reporting entities. A prescribed list will also minimise the number of businesses affected and provide those prescribed with certainty around their obligations. ***Minister preferred option*** *This option will impact a higher number of businesses and as a result provides less certainty to businesses around their obligations under the Act.*	Low *Low*	Medium *Medium*
(reporting entities)	***Intelligence from non-reporting entities.*** While reporting entities will be largely unaffected by this proposal, some reporting entities have raised concerns about the proposal raising confidentiality concerns from customers and increasing risks of tipping off.	Low	Low
	Monitoring orders. *Time and resourcing:* There will be some cost to reporting entities – particularly banks. While this information is currently provided to the FIU, it is provided retrospectively. Supplying it in an ongoing manner may require additional time and resourcing to be able to do so depending on the frequency of reporting required by the FIU. Most of the large banks have existing processes for ongoing monitoring as part of their enhanced customer due diligence procedures. ***Minister preferred option*** *A court order may not allow for the same flexibility to consider smaller reporting entities capacity to respond to information requests when compared with FIU authorisation of the information request and the intervals at which the information must be provided.*	Medium	Low

	Freezing Powers *Time and resourcing***:** There will be some cost to reporting entities but as this is supplementary to existing processes between the FIU and banks, the impact is likely to be minimal. Reporting entities have indicated they will need to provide additional guidance to staff to avoid tipping off and manage staff safety. The impacts may vary depending on the type of reporting entities and further work will be needed with the FIU and banks to determine how to implement this power with minimal impact.	Medium	Low
New Zealand Police/the Financial Intelligence Unit	***Intelligence from non-reporting entities***. *Implementation costs:* Training associated with educating staff internally on updated powers, developing up with guidance material, for non-reporting entities subject to the power	Low	Low
	Monitoring orders *Implementation costs:* Training associated with educating staff internally on updated powers, developing with guidance material ***Minister preferred option*** *Mirroring a production order will have impacts on the FIU and Police investigations, by creating time delays that may not enable responsive monitoring. This could risk preventable harm or crime from occurring.*	Low *Medium*	Low *Medium*
	Freezing powers *Implementation costs:* Training and guidance material associated with educating staff internally on updated powers. There may also be additional guidance required for the banks in relation to tipping off.	Low	Medium
Wider govt	***Intelligence from non-reporting entities***. *Implementation costs:* There will be costs associated with communications to notify businesses of their new obligations under the Act. ***Minister preferred option*** *Not clearly defining which businesses are affected by these changes to the Act will require larger communications efforts to support businesses is understanding their new obligations under the Act.*	Low *Medium*	Medium *Medium*
	Monitoring orders ***Minister preferred option***	*Medium*	*Medium*

	This option will have impacts on District Court workloads and may add to the current backlogs and court timeliness issues Courts are currently facing.		
	Freezing powers ***Minister preferred option*** *This option will have some minor impacts on District Court workloads though the low number of expected freezing orders will mitigate any contribution to court timeliness issues.*	*Low*	*Medium*
The public	***Freezing powers*** *Financial loss/inconvenience:* having accounts frozen may mean financial loss for persons of interest. The short timeframe for freezing as well as having exemptions is a mitigation for this. There many need to be a protection from civil litigation from a customer if the freezing power was used in good faith. ***Minister preferred option*** *Judicial approval of a freezing order may affect how quickly the FIU are able to respond to financial crime being committed. A delay in response may result in preventable harm occurring.*	Medium *Medium*	Low *Medium*
Total monetised costs		N/A	N/A
Non-monetised costs		Medium	Low
Additional benefits of the preferred option compared to taking no action			
The public	***Intelligence from non-reporting entities***. It is a benefit to the public for the FIU to have the effective powers to identify criminal behaviour. This will increase public trust in our economic system.	Medium	Medium
	Monitoring orders It is a benefit to the public for the FIU to have the effective powers to identify and monitor criminal behaviour. This will increase public trust in our economic system and in some instances, prevent crime or harm from occurring. ***Monitoring orders (Minister preferred option)***	Medium	Medium

	This option would have stronger protections for privacy and individual rights than the Ministry preferred option.		
	Freezing powers It is a benefit for the public for the FIU to have the effective powers to identify criminal behaviour. This will increase public trust in our economic system and in some instances, prevent crime or harm from occurring. S9(2)(d)	High	High
Reporting entities	***Freezing powers*** Creating more certainty for reporting entities in transacting with customers who are involved in illicit financial activity	Medium	Low
New Zealand Police/the Financial Intelligence Unit	***Intelligence from non-reporting entities.*** *Improved insights*: Creating more efficient systems for use in dynamic situations that provide context/additional intelligence to the FIU on a SAR. *Time*: Timely and accurate intelligence will support to decision makers on whether to progress an investigation.	High	High
	Monitoring orders *Time*: Creating more efficient systems for use in dynamic situations. Will save the FIU time in filing to back capture information and will allow them to pick up suspicious activity more quickly.	High	High
	Freezing Powers *Time*: Creating more efficient systems for use in dynamic situations. Will mean criminals cannot move illicit funds before Police are able to get a restraint placed on their accounts	High	Medium
Total monetised benefits		N/A	N/A
Non-monetised benefits		High	High

Issue 4 – Offences and Penalties

What is the context behind the policy problem and how is the status quo expected to develop?

Civil liability acts and enforcement tools

176. Section 78 of the Act provides that a civil liability act occurs when a reporting entity fails to comply with any AML/CFT requirement. There are a range of enforcement tools available to the supervisor in response to a civil liability act, alongside 'softer-touch' remediation plans and education. These include:

Section	Enforcement Tool	What is it?
80	Formal warning (public or private)	Issued by a supervisor that has reasonable grounds to believe a civil liability act has been engaged in.
81	Enforceable undertaking	May be accepted and enforced by a supervisor in connection with compliance with the AML/CFT Act or regulations. This requires agreement by a reporting entity.
85	Performance injunction	Granted by the High Court (on application of the supervisor) if a person has, is, or is proposing to refuse or fail to do an act or thing where it constitutes a civil liability act.
87	Restraining injunction	Granted by High Court (on application by the supervisor) to restrain a person from engaging in conduct that constitutes, or would constitute, a contravention of the Act.
90	Pecuniary penalty	May be ordered by the High Court (on application of a supervisor) if the court is satisfied that a person has engaged in a civil liability act.

177. Two-tiered pecuniary penalties depend on which provision the reporting entity fails to comply with (e.g. non-compliance with CDD and record keeping requirement can be subject to higher fines: maximum \$200,000 for individual or \$2 million for body corporate/partnership).

178. AML/CFT supervisors and law enforcement agencies use the full range of sanctions and penalties available in the Act to address non-compliance. However, public or private formal warnings are more commonly used. This is partly due to significant amendments in 2017 that extended AMLCFT obligations to DNFBPs, resulting in many small businesses becoming subject to the Act's provisions. As the regime matures, offence and penalty

settings need to support a shift in enforcement approach that recognises education has been ineffective for some reporting entities.

Criminal offences and penalties

179. The Act contains a range of offences reserved for the more serious instances of non-compliance. Businesses which knowingly or recklessly engage in civil liability acts can be held criminally liable. Other criminal liability arises from conduct relating to suspicious activity reports, prescribed transaction reports, structuring of transactions, failure to report certain matters and obstruction of investigations or a supervisors' performance of their functions. Criminal offences contain both imprisonment and financial penalties.

180. Maximum penalties range from three months to two years' imprisonment for individuals and fines from $50,000 to $5 million for bodies corporate or partnerships. Offences can be committed by reporting entities or by individuals or bodies corporate/partnerships, depending on the particular provision.

181. Offences include:

Section	Offence
91	Engaging in a civil liability act knowingly or recklessly
92	Failing to report suspicious activity
93	Providing false or misleading information in connection with suspicious activity reports (SARs) or prescribed transaction reports (PTRs)
94	Unlawful disclosure of SARs or PTRs
95	Failure to keep or retain adequate records relating to suspicious activities or prescribed transactions
96	Obstruction of investigation relating to SARs or PTRs
97	Contravention of s 47(1), which relates to disclosure of information contained in a SAR in judicial proceedings) or s48A(1), which relates to the reporting of prescribed transactions to the Commissioner
101	Structuring a transaction to avoid the application of any AML/CFT requirement
102	Obstructing a supervisor
103	Providing false or misleading information to a supervisor
106	Failure to report cash $10,000 or over moved into or out of New Zealand
107	Failure to report cash $10,000 or over received by a person in New Zealand from overseas

108	Structuring cross-border transportation of cash to avoid the application of AML/CFT requirements
110	Providing false or misleading information in connection with a cash report
111	Obstructing or not answering questions from a Customs officer

182. Section 243 of the Crimes Act 1961 (the Crimes Act) also makes it an offence to:

- Engage in a money laundering transaction, knowing or believing, or being reckless as to whether the property is the proceeds of an offence, with a maximum penalty of 7 years imprisonment; and
- Obtain or possess any property with intent to engage in money laundering, and knowing or believing, or being reckless as to whether, the property is the proceeds of an offence, with a maximum penalty of 5 years imprisonment.

Enforcement approach

183. Enforcement by the supervisors aims to be proportionate to the nature and severity of any non-compliance on a case-by-case basis, and decisions on enforcement actions are made in accordance with a variety of guiding principles, including:

- A risk-based approach to ensure actions taken are targeted and informed, as well as cost effective;
- Fostering compliance by assisting reporting entities to understand their obligations, with accessible information and advice;
- Proportionate responses relative to the AML/CFT risk or potential impact involved;
- Apply high standards consistently and fairly in similar circumstances, with robust and consistent supervision.

184. DIA applies a risk-based and responsive regulatory approach that promotes compliance through a mix of strategies, initiatives and tools that aim to:

- make it easy for reporting entities who want to comply;
- help reporting entities who are trying to comply; and
- use the law against those that refuse to comply.

International context

185. In New Zealand's 2021 MER, the FATF considered the penalty framework in the Act is not sufficiently comprehensive in that it does not enable proportionate, effective, and dissuasive penalties in every instance. The statutory review recommended several changes relating to offences and penalties in the AML/CFT regime.

What is the policy problem or opportunity?

186. We have identified (through the MER and Statutory Review) five problem areas with current offence and penalty settings:

- **New offences and penalties** are needed to respond to some forms of concerning conduct. Conduct considered includes:
    i. Offences against the FIU
    ii. Structuring non-transaction-based obligations
    iii. Structuring legal persons or legal arrangements.
- The Act does not sufficiently allow for **intermediary enforcement options**.
- The Act does not allow for proportionate, dissuasive, and effective **penalties at the top end of seriousness**.
- The current **limitation period** risks some conduct going unpunished because too much time has elapsed as a consequence of how offending is identified.
- In addition to the above issues, aspects of the **wider AML/CFT reforms require offences and penalties** to ensure changes are effective.

187. Financial penalties have not been recently adjusted to account for inflation. Some penalties do not align with comparable domestic legislation, such as those addressing financial crime.

International context

188. s9(2)(d) [redacted]

189. s9(2)(d) [redacted]

There are no offences and penalties available to respond to some forms of concerning conduct

190. There are certain types of concerning conduct that the Act currently does not cover:

- There are currently no consequences if a reporting entity generally obstructs the FIU, or fails to provide or provides false or misleading information to the FIU following a request under s143 for further information. Comparable offences exist in relation to the AML/CFT supervisors under section 102 and 103. The statutory review identified these do not cover the FIU, but should.[20]
- It is an offence for a person to structure a transaction to avoid AML/CFT requirements. However, the Act does not capture those who structure non-transaction-based obligations (such as using a false identity or other document to defeat customer due diligence requirements) to avoid AML/CFT requirements. By structuring non-

[19] See page 87 of FATF Methodology 22 Feb 2013.pdf.coredownload.pdf

[20] The Cathy Hua case is an example of this type of activity. Police reported Hua's reporting was low quality, and she would fail to resubmit with the required information. Police reported her reporting was highly selective to give the appearance of compliance while the actual criminals using her services were not the subject of reports. Cathy Hua is the recipient of the longest prison term for money laundering ever handed down by a New Zealand court.

transaction-based requirements a person may inaccurately present themselves as low risk to a reporting entity[21] to hide the involvement of a politically exposed person or connection to crime. The statutory review recommended the Act should be able to respond to, and hold to account, those who evade all forms of AML/CFT obligations.

- Accurate beneficial ownership information is essential for law enforcement to identify the natural person responsible for the underlying activity of concern by legal persons/arrangements. It is currently not an offence to deliberately structure a legal person[22] or a legal arrangement[23] in a way that obscures who the beneficial owner[24] of that legal person or legal arrangement is, for example, by creating unnecessary layers[25], including in jurisdictions without transparency of legal persons or arrangements. An offence is needed to combat persons knowingly taking steps to obstruct the beneficial owner being identified by a law enforcement agency or reporting entity.

The Act does not sufficiently allow for intermediary enforcement options

191. The Act does not currently provide the ability for AML/CFT supervisors to respond to low/moderate-serious non-compliance efficiently and appropriately, i.e. conduct that requires more than an informal response (e.g. through education or remediation plans) or a formal warning, but not serious enough to warrant an injunction or pecuniary penalty.

192. In these instances, supervisors could undertake civil proceedings against the party in question, however there are significant barriers to civil proceedings. These include:

- Costly and prolonged court proceedings.
- Most of the approximate 6000 entities captured by the Act are small business, so many are unable to pay court-imposed penalties if they are significant.
- Legal fees for taking proceedings can be upwards of $70,000 even for straightforward proceedings.

193. The lack of available, graduated enforcement interventions makes it difficult to encourage compliance without using disproportionate enforcement tools. DIA notes it must issue frequent and repeated warnings to little effect, ask reporting entities to sign an enforceable undertaking (which they do not have to do) or spend tens of thousands of dollars on time consuming civil proceedings, often with little prospect of any resulting penalty ever being paid.

---

21 The establishment of shell companies is an example of structuring non-transaction-based obligations. A director may travel to New Zealand for the express purpose of establishing companies and obtaining bank accounts. That director may then leave New Zealand and have no further involvement in either the company or bank accounts. In that sense "false" identity documents have not been used, but the activity is nonetheless fraudulent in that the intent is to provide newly established companies and bank accounts to other persons engaged in money laundering and/or "underground" remittance operations.

22 Any entities, other than natural persons, that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, and partnerships.

23 A relationship established pursuant to a contract between two or more parties that does not result in the emergence of a legal person. A trust is an example of a type of legal arrangement.

24 Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

25 Layering is when successive layers of legitimacy are added to the initially placed funds, until the source of the gains is adequately hidden from authorities to be undetected as ever having been illegal.

The Act does not allow for proportionate, dissuasive, and effective penalties at the top end of seriousness

194. The Act provides for civil pecuniary penalties and criminal penalties. The MER and Review identified that sanctions may be insufficiently proportionate and dissuasive for larger reporting entities (including for branches of multinational companies) and serious non-compliance. The Review identified current penalties are unlikely to exceed the cost of compliance for some businesses and are not always in line with comparable domestic regimes and offences nor likeminded international jurisdictions. Penalties have not been recently updated for inflation. Current penalties, including imprisonment terms, are not sufficiently dissuasive to discourage non-compliance in all circumstances. These findings are in line with shortcomings identified by the FATF.

195. The current penalty levels are largely sufficient and dissuasive for small and medium-sized businesses, but not for large businesses. Some penalties are not sufficient or proportionate to the potential or actual harm caused by the offending. Evolving and increasing organised crime threatens to further reduce the effectiveness of penalties and the options available to the courts.

196. Like-minded jurisdictions, including Australia,[26] Canada[27] and the UK[28] allow the implementation of significantly larger penalties. For example, in 2024 Australia imposed an AUD $67 million penalty on SkyCity Adelaide, whereas DIA was only able to obtain an NZD $4.16 million penalty to SkyCity in New Zealand[29] for similar non-compliance. Current penalty levels risk New Zealand being seen as a weaker link in the international community. A contributing factor to comparative disproportionality is that in New Zealand the maximum penalty is per civil liability act, whereas in most other countries the maximum penalty is per instance of civil liability act.

The current limitation period is too short to address complex AML/CFT offending

197. Limitation periods balance an individual's right to a fair hearing, the need for legal certainty in business and private life, entitlements to compensation, and the public interest in seeing unlawful or otherwise wrongful conduct addressed.

198. The current limitation period of three years risks some conduct going unpunished because too much time has elapsed due to how offending is identified. There can be significant delays between the AML/CFT offence occurring and being detected by the supervisor, often due to the complex nature of AML/CFT non-compliance and the fact that non-compliance is often detected through examining historical records and at monitoring visits or desk-based reviews (which may only happen every few years). Criminal AML/CFT non-compliance may only emerge after a Police ML investigation, which may make the 3-year statute of limitations very hard to meet (and criminal AML/CFT non-compliance

---

26 Civil penalties are up to A$6.6m for individuals, and A$33m for corporations.

27 Canada are undergoing substantial reform with significant increases to penalties planned. They are also able to apply penalties per instance of offending. Proposed penalties include a 40-fold increase and fines of up to C$20m or 3% of annual worldwide gross revenue. For individuals, the maximum penalty is proposed to be the greater of C$4m or 3% of annual worldwide gross revenue. Proposed increases to fines for criminal offences are 10-fold, with potential for increased prison terms.

28 Non-compliance can result in a range of penalties, including financial fines, regulatory actions, and imprisonment. The fines can be substantial, and the FCA has the power to impose unlimited fines for breaches of AML/CFT requirements.

29 SkyCity Casino Management Limited.

unpunished). This also limits the range of enforcement actions that supervisors can take to address AML/CFT non-compliance.

CDD reform requires offences and penalties to ensure changes are effective

199. As a result of broader AML/CFT reform, a new explicit offence would provide clarity.

200. The preferred options for reforming CDD settings in the Act will move to a more risk-based approach to CDD in which reporting entities have greater discretion to determine when to apply simplified CDD and how to conduct enhanced CDD. This creates a risk that reporting entities may implement ineffective CDD measures, and doing so will need an associated offence to appropriately respond where an educational, or other, approach is inappropriate.

The money laundering offences in the Crimes Act

201. The New Zealand Court of Appeal has held that individuals who launder money for drug dealers are nearly as culpable in the eyes of the law as those who participate directly in drug distribution [*R v Wallace* CA415/98]. Despite this, money laundering penalties are lower than for many predicate offences.[30] For example, dealing with controlled drugs involves a maximum potential term of imprisonment for life, and the maximum term for trafficking in persons is 20 years imprisonment.

202. The social harm caused by crime enabled by money laundering is significant. The 2024 National Risk Assessment estimates profit from drug crime to be conservatively in the range of $500–$600 million annually, and is estimated to have caused $1.5 billion in social harm last year. The 2024 Crime and Victims Survey also identified that 10 percent of New Zealanders have experienced fraud in the last 12 months. Large money-laundering schemes are often punished with less serious penalties such as home detention. A recent case involving $123 million of illicit deposits, which facilitated drug dealing, illicit cigarette trafficking and fraud, resulted in a nine-month home detention sentence.

203. The penalties available for money laundering are disproportionate to the harm caused and do not account for the profits that could be gained from illegal conduct. This is particularly the case for offenders involved in criminal business enterprises or providing third party money laundering as a criminal service who may see a low penalty as a cost of doing business.

204. s9(2)(g)(i) [redacted]

What options are being considered?

New offences and penalties

205. Analysis for scoping which new offences are needed are not included in this document as we have focused on whether to implement the identified viable options. Analysis here is therefore binary. Options are not mutually exclusive and can be progressed together.

[30] Predicate offences are the underlying criminal activities that generate the illicit funds that are then laundered.

Agencies would have discretion whether to use a sanction or respond alternatively in lower-serious instances.

Status Quo

206. Concerning behaviours such as misleading the FIU, structuring of non-transaction-based obligations, and structuring legal persons and arrangements would continue without direct ability to apply appropriate offences and penalties. This would facilitate ML/TF activity and S9(2)(d)

Option One – Offences relating to the FIU

207. This option will introduce three offences to respond to concerning conduct related to the functions of the FIU:

- Wilful obstruction of the FIU in the exercise of its powers under the Act.
- Failing to provide the FIU with information following a request under s143 of the Act.
- Knowingly or recklessly providing the FIU with false or misleading information following a request under section 143 of the Act.

208. There are existing penalties for comparable conduct already under the Act. As the conduct, mens rea elements and harm is alike, penalties for these offences would compare to those set out in section 105 of the Act.[31] The Act provides a similar offence if a person wilfully obstructs any supervisor or provides false or misleading material to them.[32] These offences contain identical mens rea elements to those proposed. We consider the penalty should align with existing comparable provisions given similar harm is caused.[33]

209. These offences will still enable the FIU (as it does for the supervisors and existing offences) to take alternative actions such as education, but they enable more serious action to be discretionarily taken where appropriate (e.g. where education was ineffective).

210. The agency powers section of this RIS proposes extending section 143(1)(a) to also cover non-reporting entities. We consider the new offences should also apply to non-reporting entities as well as reporting entities, with the expectation that the FIU and Police would take an education first approach where appropriate, particularly for non-reporting entities to acknowledge the difference in expected AML/CFT understanding. Lower penalties would be able to be sought to account for such factors.

Option Two – Structuring offences

Structuring non-transaction-based obligations

211. This option will make it an offence for any person to structure non-transaction-based obligations to avoid AML/CFT requirements in addition to the existing offence to structure transaction-based obligations.

---

31 Later options include increasing section 105 penalties.

32 Sections 102 – 103, and section 105, of the Act. To be found guilty of an offence under s103 the conduct must have been done without a reasonable excuse.

33 Section 105 of the Act sets out comparable penalties that this would match. Any increases to section 105 penalties would be reflected in the penalties for this offence.

212. An offence is needed to deter those seeking to get around the AML/CFT obligations by setting up illegitimate structures to mislead reporting entities. Comparable wording in the structuring transaction-based-obligations offence is strict liability but requires proof that the action was taken to avoid the application of AML/CFT requirements.

213. As recommended in the Statutory Review and to align with existing requirements in the Act, this option would expand the existing strict liability offence to cover any person who structures non-transaction-based obligations. This will ensure those who evade AML/CFT obligations (e.g. a person, such as a customer, circumventing a reporting entity's AML/CFT controls) via structuring are able to be held to account. This option would capture a situation where a person is presenting as lower risk when there is potential criminality. This offence could apply to all kinds of non-transaction structuring, such as providing false information regarding "nature and purpose", "source of funds", or a false document. This could also include structuring of CDD information to conceal who a beneficial owner is.

214. We considered whether a non-exhaustive list of captured obligations would promote clarity for reporting entities but consider a general catch-all offence provides desirable flexibility and sufficient clarity.

Structuring legal persons or legal arrangements

215. This option would introduce an offence to structure legal persons or legal arrangements in a way that obscures or obstructs who the beneficial owner of that legal person or legal arrangement is for criminal reasons.

216. A legal person or legal arrangement may apply to a reporting entity for a captured activity and do so in a way that the reporting entity cannot, or finds it difficult to, identify beneficial ownership. Similarly, were a law enforcement agency to investigate, the same challenges would apply. Examples include creating unnecessary layers of legal persons or arrangements, including in jurisdictions without transparency of legal persons or legal arrangements.

217. This would apply to any person, not just reporting entities. The offence could involve defining how a structure would 'avoid or obstruct' transparency to assist reporting entities understand what this behaviour looks like. Penalties would be in line with existing structuring offences[34]. Application could be restricted to target only those who do so for criminal purposes.

218. There is a need to prevent inappropriate retrospective application of this new offence. In line with any changes in the beneficial ownership workstream, this option would include a warning system preceding sanctions and an education-first approach where appropriate. This would mean legal arrangements, including existing arrangements, can be told they need to change their structure to meet a certain standard within a certain timeframe to avoid liability. This is aimed at assisting the many already existing trusts to understand when they may be in breach without unreasonably holding them to account. This is in line with existing, graduated enforcement approaches.

[34] Under section 101 of the Act.

Option Three – New offences to support CDD reform

219. This option will explicitly include, in the section 78 list of civil liability acts, the act of implementing ineffective CDD measures following proposed CDD reform. Where it is engaged in knowingly or recklessly, it will be a criminal offence under section 91. Section 78 makes it a civil liability act for failing to comply with any AML/CFT requirement, and includes a non-exhaustive list of acts. Failure to comply with new AML/CFT CDD obligations following reform would be captured by nature of being an AML/CFT requirement, however this option would make it explicit and provide extra clarity and certainty for reporting entities.

220. Penalties will be in line with comparable penalties that already exist under the Act. Section 90(2) and s90(3) provide penalties for civil liability acts, and section 100 for criminal penalties.

How do the options compare to the status quo/counterfactual?

221. Options can be progressed together and are not mutually exclusive.

New offences

	Option One – New offences relating to the FIU	**Option Two – New structuring offences**	**Option Three – Offences to support broader reform**
Proportionate	+ Comparable offences and penalties for similar conduct exist and alternatives, like an educational approach, can still be taken.	+ Comparable offences and penalties for similar conduct exist and alternatives, like an educational approach, can still be taken.	+ Comparable offences and penalties for similar conduct exist and alternatives, like an educational approach, can still be taken.
Dissuasive	++ Enables response to concerning conduct, which has a dissuasive effect.	++ Enables response to concerning conduct, which has a dissuasive effect.	++ Enables response to concerning conduct, which has a dissuasive effect.
Effective	++ New offences fill current gaps.	++ New offences fill current gaps.	++ New offenses ensure non-compliance with new obligations can be effectively responded to.
Overall assessment	++	++	++

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Increasing the range of sanctions

222. All options are preferred to enable proportionate, dissuasive, and effective responses to concerning conduct where there are no current corresponding offences or penalties under the Act. Without new or amended offences, such conduct would go unpunished and expose the regime to bad actors.

223. We also recommend explicitly including implementing ineffective CDD measures in the non-exhaustive list of civil liability acts to ensure the consequences of non-compliance under the new CDD settings are as clear as possible.

224. Non-reporting entities should be captured by the new offence relating to the FIU to align with agency powers reform.

Strict liability offences are justified for structuring offences

225. Strict liability offences are used to enforce requirements of regulatory regimes, such as regulating an occupation or commercial activity. As strict liability offences do not take mens rea into account they can have human rights implications around principles of fairness and proportionality. The Ministry considers strict liability offenses justified for the structuring offence relating to non-transaction-based obligations given the need to provide an incentive for business to adopt appropriate precautions to prevent breaches facilitating money laundering and terrorism financing.

Intermediary enforcement options

226. The statutory review recommended two broad directions for how the Act could be amended to increase the range of intermediary enforcement options, which are not mutually exclusive:

- Create and infringement offence regime; and
- Allow for the restriction, suspension, or cancellation of a licence or registration.

227. We have identified options relating to each of these recommended directions.

Infringement notices and administrative penalties

Status Quo

245. There are limited effective and dissuasive sanctions options if the non-compliance threshold of a formal warning is exceeded.

Option One – Infringement offence scheme

228. This option would allow supervisors (and other appropriate agencies) to issue infringement notices (flat fees) for non-compliance in appropriate circumstances, such as where they are straightforward to identify and where a “one size fits all” approach can be taken. An infringement offence scheme would fill the middle ground between formal warnings and civil proceedings, as a graduated and proportionate response to the level of non-compliance.

229. Infringement notices would be issued for administrative matters (e.g., where businesses do not submit annual reports on time), or straightforward but nonetheless minor to moderately serious non-compliance. Supervisors would have discretion whether to apply

a formal warning, infringement notice, or civil proceedings depending on the circumstances of offending.

230. New Zealand law contains many infringement provisions that impose penalties in excess of $1,000, which are exceptions to the general principles in chapter 25 of the Legislation Design and Advisory Committee's (LDAC) guidelines. This option would introduce infringement fees that could range from up to $20,000 to align with the Financial Markets Conduct Regulations 2014. These are higher than the $1000 maximum recommended in LDAC guidelines, however these have been discussed with the Ministry's Offense and Penalty Vetting (OPV) team which advised higher penalties can be justified in such cases of financial crime where a dissuasive effect is needed and a cost of doing business is a material factor. The infringement fee levels should be set to correspond with similar offences and behaviour captured in other Acts, such as the Financial Markets Conduct Regulations Schedule 22 (where infringement fees go up to $20,000). This is a comparable example of a schedule of infringement fees, both in terms of penalty values and type and seriousness of captured conduct.

231. The fee collected from infringements would be payable to the Crown Bank Account rather than to the enforcement body.

232. This option involves a transfer of a traditional judicial function to the executive branch of government, and it is important that any individual can request that the Court review or reduce the penalty. The criminal courts will generally become involved only if the infringement fee is not paid or if the recipient of the infringement notice challenges it. This option would include the ability to judicially review the infringement.

233. This option would involve creating empowering provisions within the Act to establish the infringement offence scheme, the maximum penalty provisions, identify who can issue infringement notices; and the entitlements to revenue that prosecuting agencies receive from infringement fees.

234. A flat fee would be administratively efficient to apply and easier to understand, compared to a tiered fee option. This provides certainty about the infringement fee amount, without the complexity of considering additional factors in a tiered approach, such as the size or sector.

235. A decision to prosecute may be taken if an infringement offence and fee is insufficient for the seriousness of the offending behaviour through the graduated approach taken by enforcement agencies.

236. Examples of the type of conduct that could be infringement offences are listed below. Exact offences and corresponding penalties would be set through regulations and vetted by the Ministry's OPV team to ensure appropriateness:

THEME	STRICT LIABILITY OFFENCE
Compliance with AML/CFT requirements	• Section 56 – reporting entity must have an AML/CFT programme • Section 56 – reporting entity must have an AML/CFT compliance officer

	• Section 57 – failing to have a procedure, policy or control for a requirement of s57 as required • Section 58 – reporting entity must undertake a risk assessment • Section 59 – review and audit of risk assessment and AML/CFT programmes
Customer due diligence	• Section 11/14 – Must conduct customer due diligence • Section 15/19/23 Must obtain information (as part of CDD) • Section 22 – Must conduct enhanced CDD in certain prescribed circumstances. • Section 37 – must not establish, or must terminate a business relationship or not conduct an occasional activity or transaction (if CDD is not conducted)
Reporting requirements	• Section 60 – annual AML/CFT report • Section 48A – requirement to report prescribed transactions • Section 40 – requirement to report suspicious activity (note: this risks a subjective assessment and could incentivise 'defensive reporting', which could lead to poorer quality SARs being reported which wastes Police resources) • Failure to register for levy • Failure to respond to notice issued by supervisor under s132(2)(a) of the Act
Record-keeping	• Section 49, and Reg.15N (R&C) Regulations – obligation to keep prescribed records • Section 49A – obligation to keep reports of suspicious activities • Section 50 – obligation to keep identity and verification records • Section 51 – obligation to keep other records

237. The Act would be amended to create a regulation-making power that would allow the prescribing of acts of non-compliance that would be eligible for infringement notices.

238. This infringement notice option broadly aligns with Australia's approach, who has the power to issue infringement notices (which can be public) for breaching specific parts of the AML/CFT Act regarding know your customer procedures, reporting, enrolment, registration, providing information, and record-keeping. Infringement notices can be made public in Australia.

Option Two – Administrative offence regime

239. Administrative penalties are financial penalties that are imposed directly by a regulator and do not result in a conviction. This option would establish a new tiered administrative penalty system that will enable AML/CFT supervisors to determine what penalty is appropriate depending on the contravening behaviour.

240. Under this approach, breaches of the law are adjudicated (including seriousness and state of mind) and penalised by the agency that regulates and monitors that area of the law. This is different from the normal process in the civil and criminal law where breaches of the law are adjudicated, and penalties are issued, by a court.

241. This option will provide AML/CFT supervisors with additional enforcement tools to address low or moderate level offences that are not serious enough to require an injunction without the need for prosecution, enhancing supervisors' ability to incentivise compliance with the Act according to the harm of the behaviour.

242. Administrative penalties are often used as they often occupy an administrative/discretionary middle ground. The conduct being captured by AML/CFT supervisors may be too serious for the maximum penalties recommended for infringement offences, but not serious enough to justify the regulator taking the issue to court. They are also used in instances where expert knowledge may be required to regulate a particular regime – which in this case would be best known by the supervisor what behaviour has been contravened.

AML/CFT non-compliance and licensing

Status Quo

243. The DIA can share information with licensing bodies when they have taken enforcement action. s9(2)(g)(i) [redacted]. If a licensing body sought more detail (i.e. a customer or transaction details that underpin the assessment of non-compliance), the supervisor would need to consider whether that was within the provisions of the Privacy Act, likely on a case-by-case basis. There may be the option of redacting identifying information. s9(2)(g)(i) [redacted]

244. While supervisors may currently share information with licencing bodies in limited circumstances under sections 48 and 139 of the Act, there will continue to be limited intermediary enforcement actions without increasing the range of responses to non-compliance via enabling supervisors to restrict, suspend or cancel a licence or registration, or request a licencing body to do so.

Option One – Supervisory power to impact license of reporting entity

245. This option will provide the AML/CFT supervisor with the power to restrict, suspend, or cancel a reporting entity's prudential licence or registration following AML/CFT non-compliance.

246. The option recommended in the statutory review recommended this power extend to AML/CFT specific licensing and registration. In lieu of any development of AML/CFT specific licensing and registration systems, this option would extend only to prudential licenses.

247. Licensing bodies include RBNZ, FMA, New Zealand Law Society (NZLS), Real Estate Authority (REA), and Chartered Accountants Australia and New Zealand (CAANZ). While licensing bodies could be consulted, the decision of whether to restrict, suspend, or cancel a prudential licence would sit with the AML/CFT supervisor and be based on

findings of AML/CFT non-compliance. Controls would ensure appropriate use of this power.

Option Two – Referral of AML/CFT non-compliance to licensing body

248. This option would formalise the current ability to share information relating to non-compliance with appropriate licensing bodies. This would increase the range of options that a supervisor would have to respond to non-compliance.

249. This option involves an explicit sanction or response to AML/CFT non-compliance, where the AML/CFT supervisor can make a referral to applicable licensing bodies to consider whether there is a case to review eligibility to hold a license or take any other appropriate action. The licensing body would then be able to receive and consider this information as appropriate under their licensing responsibilities.

250. This would involve provisions, or other means, to make sure DIA are doing due diligence first. Taking this action outside of existing information sharing settings (i.e. ss 48, 139) (i.e. as an explicit response to non-compliance) could be possible when non-compliance is proven to the standard required to take other action (such as formal warnings) where the supervisor has "reasonable grounds to believe" non-compliance has occurred.

251. Similar to sharing information relating to a formal warning, the type of information shared would be a summary of findings of non-compliance. This would be possible without sharing personal information of underlying customers. If a licensing body wanted more detail, this could be considered against the Privacy Act on a case-by-case basis.

How do the options compare to the status quo/counterfactual?

Intermediary options - Infringement and administrative regime

	Option One – Infringement penalty regime	Option Two – Administrative penalty regime
Proportionate	+ Ensures proportionate responses are available for lower-level offending and small-medium reporting entities.	++ Tiered penalty system accounts for a variety of factors to ensure proportionality.
Dissuasive	+ Provides additional easy-to-implement tools for supervisors to act against offending but may not deter large businesses or have strong reputational effects.	++ The penalty can be determined by the revenue which is more dissuasive to large entities.
Effective	++ Supervisors can respond to straight-forward issues of non-compliance more effectively.	+ Linking revenue and size to the penalty increases effectiveness but administrative penalties combine regulatory, adjudication and enforcement functions which the Ministry generally considers inappropriate.
Overall assessment	+	+

Intermediary options - Licensing

	Option One – Supervisory power to impact licence	**Option Two – Referral of non-compliance to licensing bodies**
Proportionate	+ Expands range of tools available to the supervisor to respond to non-compliance in a manner deemed most proportionate.	+ Encourages licensing bodies to consider whether a reporting entity remains eligible to hold a licence or to take other appropriate, proportionate action.
Dissuasive	++ The potential impact that AML/CFT non-compliance may have on licensing decisions provides dissuasive effect.	+ The ability for a reporting entity to share information on non-compliance exists already under the Act. Formalising this ability as a sanction would place extra weight behind this action.
Effective	- Inappropriate for licensing decisions to be made by DIA for reporting entities that are regulated by RBNZ and FMA, nor for DNFBPs licensing by professional bodies.	+ Information is already able to be shared in limited circumstances, but formalising this as a response to non-compliance would place extra weight behind this action.
Overall assessment	**0**	+

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Intermediary enforcement options – Infringement or administrative penalties

252. Option One, an infringement regime, is preferred. An infringement regime fills the current gap that exists between formal warnings (whether public or private) and civil pecuniary penalties (which are costly, take time, and involve the courts so are not appropriate for lower-level offending). While enforceable undertakings and injunctions are available, they are rarely used because enforceable undertakings must be agreed to by a reporting entity, and injunctions involve the courts and can be costly. An infringement regime incentivises compliance by ensuring a proportionate course of action can be taken. This would improve the status quo as supervisors would be more able and willing to act against all types of offending, which provides a greater incentive to comply. This approach aligns with Australia's infringement approach and addresses a recommended action in New Zealand's MER, improving our compliance with FATF Standards.

253. Set infringement fees may lead to disproportionately low penalties for larger businesses. As there are a range of sizes of stakeholders impacted, a $5k penalty for a small business could be large while it is a very minor cost of doing business for a big entity. In addition, infringement penalties may not have a reputational impact as they are typically resolved outside of the courts and do not result in a conviction, though they can be made public. To address this, a decision to prosecute can be taken if an infringement notice is insufficient for the seriousness of the offending behaviour, such as multiple offences or large-scale offending.

254. Administrative penalties are flexible and enable a discretionary middle-ground and would allow for higher penalties than an infringement regime, however we consider they inappropriately blur the line between regulator and adjudicator. Establishing new adjudication and appeals functions to support an administrative penalty regime would also involve additional costs that would be borne by levied reporting entities.

255. As with the structuring of non-transaction-based obligation offence, The Ministry considers strict liability appropriate for the infringement regime. Infringement offences should concern conduct that involves straightforward issues of fact that can be easily identified. The addition of mental elements would incentive challenging the matter in court which runs counter to the purpose of an infringement regime which is to keep minor infringements of criminal law out of courts. The Ministry considers this will also minimise the impact on court timeliness.

Intermediary enforcement options – Licensing and AML/CFT non-compliance

256. Option Two is preferred. Formalising the ability to share non-compliance information with licensing bodies via an explicit response to non-compliance expands the range of options a supervisor can take in response to non-compliance and provides extra weight behind the action. This achieves the purpose of ensuring supervisors can provide proportionate, dissuasive and effective sanctions, improve international compliance (although not as far as explicitly required by the FATF, which requires the supervisor be able to directly impact licences) and increase the range of sanctions as identified by the statutory review.

257. With DIA becoming the single supervisor, Option Two is preferred over Option One to avoid DIA making licensing decisions when they are not the appropriate body. We anticipate non-compliance will be appropriately considered in any licensing decisions by the responsible licensing body given the importance of compliance with the Act and the impact non-compliance has on the integrity of our financial system. We consider leaving action to the expertise of the applicable licensing body most appropriate.

Penalties at the top end of seriousness

258. We have identified several options to ensure that proportionate penalties can be applied in all instances. Reform is needed to enable more proportionate outcomes at higher ends of the scale that can influence decision-making within those businesses.

Status quo

259. Retaining the status quo would mean existing maximum penalties will remain unchanged, of which some are considered in our Statutory Review, and by the FATF, to be disproportionate and not dissuasive. Some penalties are out of line with comparable domestic legislation, such as the Commerce Act 1986 and the Financial Markets Conduct Act 2013. Most penalties are lower than those in like-minded international jurisdictions.

Option One – Raising maximum penalties where needed

260. This option will raise maximum penalties for offences that need a higher ceiling, such as civil pecuniary penalties and some criminal penalties. This will raise maximum penalties where they need to be more proportionate, dissuasive, and effective, and where needed to bring them into line with comparable domestic regimes[35] and like-minded international jurisdictions. If progressed alone, this option would keep the structure of the offences and

---

[35] Such as those dealing with financial crime.

penalties regime in the AML/CFT Act the same. This would be done by an absolute increase for appropriate penalties, such as section 90 for civil liability acts under section 78, and imprisonment where appropriate.

Option Two - Introduce a penalty unit system

261. This will introduce a penalty unit system, which would use penalty units to calculate the maximum fines and pecuniary penalties for breaking New Zealand laws. Maximum penalties would be calculated by multiplying the value of one penalty unit by the number of units that an offence carries, but judges would retain discretion concerning the ultimate fine imposed.

262. A similar system is used in Australia by AUSTRAC whereby penalty units are used to calculate fines. For example, if a penalty unit is worth $100, and the penalty for an offence is set at 10 penalty units, the penalty will be $1000 (100 x 10).

263. The penalty unit can be updated/amended through a separate process (via regulations) so can be easily inflation-adjusted as the value of a single penalty unit would be set in regulations. The number of units that can be applied to each offence would be set in legislation.

Option Three - Tie penalties to another factor

264. This option would allow a penalty to be determined by factors other than a prescribed figure. We considered whether the penalty to another factor such as a percentage of the money laundered / profits of the reporting entity during the period of non-compliance (or annual turnover), sector type, the size of the business, or other material factors that could contribute to whether an applied penalty is circumstantially proportionate and dissuasive. These sub-options are described below.

Sub options for Option Three – Potential factors

265. **Status quo**. Penalties are assigned a maximum penalty and discretion applied in individual circumstances. Penalties can be applied as appropriate below that maximum, with most serious breaches resulting in the maximum.

266. **Sub-Option One – Linked to sector, size and/or nature of business.** Link penalties to sector, size and/or nature of business or the risk of the sector, role of the sector within the financial system, and footprint of the sector on the New Zealand economy. Penalties would be set out via a schedule factoring in some of, or all of, these characteristics.

267. **Sub-Option Two – Enable penalties to be applied per instance of offending.** Allow monetary penalties under the Act to be applied per instance of non-compliance, rather than on a representative or aggregate basis. This option would enable the overall penalty to be proportionate to the duration, severity and repeated or systemic nature of the non-compliance.

268. This sub-option would enable penalties per instance for both civil pecuniary penalties and criminal penalties otherwise a per instance approach could cause supervisors choose civil proceedings over criminal (if there is evidence of criminal non-compliance) because the ultimate penalty would be higher. An upper limit would provide a ceiling and avoid disproportionate maximums.

269. **Sub-Option Three – Proportionate to turnover and/or commercial gain.** Allow for maximum available penalties to be the greater of a prescribed penalty, a multiple of commercial gain, or a percentage of annual turnover in appropriate civil and criminal instances where needed to better align with comparable regimes.

270. Under this option, legislation would enable the additional factors (multiple of commercial gain and percentage of turnover) to be considered where they are greater than the maximum prescribed penalty by enabling the 'greater of' the potential figures to be considered. The courts would still have discretion to apply a penalty at the level they deem proportionate and appropriate, but this option would allow those factors to potentially set a higher maximum penalty / ceiling for larger reporting entities or more serious non-compliance. Under this option there will always be the absolute discretion for the courts, and the parties can make submissions as to the appropriate methodology.

271. Where commercial gain is not ascertainable, the penalty can still be linked to turnover or be the prescribed penalty. In civil instances, even when ascertainable, it would be for the parties to make submissions as to which limb is most appropriate as the greater available may not be the most appropriate. This provides flexibility without restricting and risking disproportionate outcomes.

272. This option in based in part on the Commerce Act's system whereby fines can be directly linked to either the benefit gained from illegal activity or to the turnover of the entity. It aligns with the approaches taken in comparable domestic regimes such as the Financial Markets Conduct Act 2013 and the Commerce Act 1986.

273. This option would also somewhat account for the size and nature of the business, but not through a schedule as per Sub-Option One.

274. This option would retains court discretion by setting the greater of figures penalty to ensure proportionality such as at lower ends of offending. The courts are likely only involved at higher end instances already, given agency discretion.

How do the options compare to the status quo/counterfactual?

	Option One – Increase prescribed penalty	Option Two – Penalty unit system	Option Three –Tying the penalty to other factors
Proportionate	+ More proportionate penalties at upper end of seriousness though requires updating over time.	+ Ensures long-term proportionality as unit figure can be adjusted for inflation.	++ Flexibility to consider other factors promotes proportionality and a risk-based approach.
Dissuasive	+ More dissuasive for larger reporting entities. Greater imprisonment terms provide dissuasive effect.	+ Dissuasive effect lasts through inflation and changing AML/CFT environment.	+ Allowing penalties to account for specific factors associated with a reporting entity, such as the size, compliance costs, and of the business,

		Up-to-date penalties incentivises compliance.	May complicate application of penalties.
Effective	++ Improves FATF compliance and ensures proportionate and dissuasive penalties are applied.	**0** A significant shift from New Zealand's typical approach and unfamiliar to judiciary Easy to adjust over time.	++ More adaptable than the status quo and Option One. Aligns with comparable regimes and familiar to the courts.
Overall assessment	++	+	++

Sub-options to Option Three – Potential factors

	Sub-Option One – Link to sector, or size, or nature of business	Sub-Option Two – Allow penalties to be applied per instance of offending	Sub-Option Three – Proportion of profits, turnover or commercial gain
Proportionate	- Does not account for range of reporting entities and size of reporting entities within sectors – variance could result in disproportionate outcomes.	+ Would scale with size of entity (large businesses engage in orders of magnitude more activity). May risk disproportionate outcomes in extremes, though court discretion remains.	++ Proportionate to financial impact/severity and accounts for inflation.
Dissuasive	+ Specificity to sector/risk provides additional dissuasion for high turnover/high-risk sectors. Does not account for reporting entities with low residual risk in high-risk sectors.	++ Disincentivises intentional and ongoing breaches. Incentivises businesses to promptly identify and address instances of non-compliance.	++ Ensures penalties cannot be seen as a cost of doing business.
Effective	- Difficult to define sector type, size of reporting entity, and nature of business. Size / nature of business will already be considered by courts.	+ Repeated breaches contribute to overall seriousness of the offending. Improves FATF compliance.	+ Existing precedent in domestic legislation and improves FATF compliance. Commercial gain may not be readily ascertainable and would benefit from being combined with other options.

Overall assessment	+	+	++

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

275. The preferred option combines several options. **Option One and Three are preferred**. Increasing the maximum penalties, both civil and criminal (including imprisonment terms) where needed, will ensure they are proportionate, dissuasive, and effective, are in line with comparable domestic regimes, and better align with like-minded international jurisdictions and international standards. Alongside flat increases to maximum penalties, we also consider the maximum available penalty should be influenced by other factors:

- **Sub-option Three is preferred**. Incorporating a multiple of commercial gain and percentage of turnover will allow fines to be directly linked to either the benefit an entity gets from illegal activity or to the turnover of the entity. This is based in-part on comparable domestic legislation such as the Commerce Act and Financial Markets Conduct Act.
- **Sub-option Two is preferred**. By enabling penalties to be applied per instance of offending, repeated and systemic breaches can be better accounted for, and we will bring our system closer into alignment with like-minded jurisdictions by enabling higher penalties in appropriate circumstances.

276. This combination of options will allow responses proportionate to the level of harm that could be caused by a contravention or the gain made, provide a stronger deterrent effect against potential contraventions, ensure penalties are proportionate and dissuasive against entities of all sizes, better accounts for the cost of compliance, while maintaining proportionate responses at lower ends of offending. It would also avoid the need to regularly review a fixed penalty amount by ensuring it can be set at an appropriate level as turnover and compliance costs change. It would align more closely with comparable regimes and align New Zealand better with the approach and penalties available in likeminded jurisdictions. It would also better meet the purposes of the Act, namely deterring ML/TF, maintaining and enhancing New Zealand's international reputation by where appropriate adopting FATF recommendations, and contributing to public confidence in the financial system.

277. Our preferred combination of options would prioritise compliance and education first, and ensure a graduated approach can respond to non-compliance with appropriate actions accounting for a variety of seriousness of offending and reporting entities. Reserving the top end of penalties for the most serious of offending that requires a punitive effect, this combination of options would see the maximum range of pecuniary penalties, and criminal penalties, increased to bring them in line with comparable domestic. It would maintain the ability for supervisors use discretion as to what enforcement action is taken. This would be more proportionate and dissuasive for larger businesses and more serious offending through a multiple of commercial gain or a percentage of turnover. This option also will allow for the duration, severity and repeated or systemic nature of the non-compliance to be considered. Providing a range of options better ensures proportionality in all instances, and accounts for factors such as growth industries and where there is plenty of funding

(e.g. funding of underlying beneficial owners of that company) which is not showing in turnover.

278. The size and nature of the business can be considered where appropriate through a graduated enforcement approach.

279. The maximum penalty that can be awarded from civil proceedings is significantly lower than in most other comparable countries with AML/CFT regimes. A large part of this is due to the maximum penalty in New Zealand is per civil liability act, whereas in most other countries the maximum penalty is per instance of civil liability act. Canada takes this approach, which enables considerably larger penalties despite the maximum penalty for a single instance of offending currently[36] being lower. This change would capture repeated non-compliance but enable consideration of factors such as whether a technical error occurred resulting in multiple instances of non-compliance.

Allowing for penalties at the top end of seriousness – Crimes Act

Status Quo

280. Current penalties for money laundering in section 243 of the Crimes Act will remain unchanged. Money laundering will remain punishable by a maximum term of imprisonment of 7 years.

Option One – Increase maximum penalties in line with predicate offences

281. This option would involve increasing the maximum term of imprisonment for the money laundering offence under section 243(2) of the Crimes Act to 14 years. The maximum penalty for obtaining or possessing property with the intent to engage in money laundering under section 243(3) would be increased to 10 years imprisonment.

282. This is in line with predicate offending for dealing in class B drugs, and human trafficking. These penalties reflect the mid-point for equivalent offending in partner jurisdictions.[37]

283. This option will also raise the current maximum penalties for the offences for money laundering set out in the Crimes Act. This will ensure money laundering penalties can be proportionate to the underlying predicate offences in all instances.

How do the options compare to the status quo/counterfactual?

	Status Quo	Option One – increasing penalties in line with predicate offending
Proportionate	**0** Under the status quo the penalties are not proportionate to the most serious kinds of predicate offending.	+ Brings offences into line with more serious predicate offending (e.g. some forms of drug trafficking).
Dissuasive	**0** Under the status quo, large money-laundering schemes are often	++ When imposing sentences the courts have regard to the maximum penalty available, so increasing offences will

[36] Canada is undergoing significant reform, including 40x increases for some penalties.

[37] The maximum term of imprisonment for money laundering is 10 years in Canada, 14 years in the United Kingdom and 20 years in Australia.

	punished with less serious penalties such as home detention.	result in more appropriate sentencing for serious money-laundering.
Effective	**0** Police have argued that the low anticipated penalty discourages prosecutors from pursuing prosecution of money laundering charges. The FATF has previously identified that money laundering is not pursued enough in New Zealand.	++ Higher penalties will incentivise the pursuit of money laundering offences.
Overall assessment	**0**	++

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

284. Option One is preferred over the status quo. Increasing maximum penalties for money laundering allows the Courts to apply proportionate penalties in line with the most serious predicate offending. This will ensure money laundering penalties can be proportionate to the underlying predicate offences in all instances. It will also better service the public interest by incentivising the pursuit of money laundering prosecutions.

Time limit for prosecuting

Status Quo

285. The limitation period for prosecuting offences relating to non-compliance with requirements under the Act is 3 years from the date the offence was committed.

Option One – Five years

286. This option would extend the limitation period for prosecuting an offence under the Act to five years, which aligns with record-keeping obligations.

How do the options compare to the status quo/counterfactual?

	Option One – Five years
Proportionate	+ Supervisors will have more time to escalate their response to a breach, including prosecuting an entity where appropriate. 5 years is a proportionate period when considering harm and nature of non-compliance and identification.
Dissuasive	++ Greater chance of non-compliance being identified and actionable within 5 years. Certainty of being caught provides a dissuasive effect.
Effective	++ Aligns with current record-keeping timeframes and ensures effective responses to a breach of the Act, including prosecuting business where appropriate.
Overall assessment	++

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

287. Option One is preferred over the status quo. Extending the time limit for prosecuting offences to align with record keeping requirements better accounts for the inherent way that AML/CFT non-compliance is identified and better ensures the public good can be achieved by prosecuting non-compliance in a wider range of appropriate circumstances. This option further disincentivises non-compliance as there would be greater certainty that a bad actor will be caught when the ability to hold non-compliance accountable does not expire due to impractical timeframes. It will increase the ability of the Police and supervisors to bring enforcement action against non-compliance.

288. Non-compliance is often detected through examining historical records at a monitoring visit or desk-based review. Such reviews may only happen years after a potential offence has occurred. Criminal AML/CFT non-compliance may also only emerge after a Police money laundering investigation, which can make the 3-year limitation period very hard to meet. The nature of AML/CFT offending, and subsequent detection, means that a 5-year limitation period is needed. The Ministry's 2022 statutory review noted most submitters supported changing the timeframe, noting it should align with other obligations such as record keeping obligations (5 years) or tax legislation.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

289. Yes.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	Largest reporting entities subject to higher penalties. Infringement offence scheme may result in more financial penalties for reporting entities.	Medium	High
Regulators	Minor administrative cost for infringement regime.	Low	High
Others (eg, wider govt, consumers, etc.) *For fiscal costs, both increased costs and loss of revenue could be relevant*	Larger penalties may be passed on to consumers. Additional/new offences may require small additional investigative resource. Additional costs to court due to better and wider capture of non-compliance (e.g. due to aligning limitation period with record keeping requirements).	Low	Medium
Total monetised costs	N/A	N/A	N/A
Non-monetised costs		Low	Low
Additional benefits of the preferred option compared to taking no action			
Regulated groups	Court costs often saved when issued infringement notices.	Low	Medium
Regulators	Alternative action out of courts will save court costs - reduced cost of bringing court proceedings or of proving the elements of the offence.	Low	Medium
Others (eg, wider govt, consumers, etc.)	Increased range of offences will enable alternative action to keep non-compliance out of the courts. The fee collected from infringements would be payable to the Crown Bank Account rather than to the enforcement body. Ensures offences are proportionate and dissuasive in light with international standards.	Low	Medium
Total monetised benefits	N/A	N/A	N/A
Non-monetised benefits		Low	Medium

Issue 5 – Targeted Financial Sanctions

What is the context behind the policy problem and how is the status quo expected to develop?

What are targeted financial sanctions (TFS) and proliferation financing (PF)?

290. TFS are a specific type of financial sanction with a stated objective, including the prevention of terrorism financing and proliferation financing. TFS require people to freeze the assets of designated persons and entities and prohibit them from providing funds or services to those designated persons or entities. The Ministry of Foreign Affairs and Trade (MFAT) is responsible for sanctions policy in New Zealand.

291. Proliferation financing is the act of providing funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons, their means of delivery and related materials. It includes trade in technologies and dual-use items - goods that have both civilian and military uses relating to weapons of mass destruction and their means of delivery.

292. Within this context, TFS for proliferation financing and terrorism financing share key similarities. While the types of activities that sanctions are designed to deter and prevent are distinct, there is strong overlap between the actual financing activities that these sanctions apply to, especially given the same obligations apply to all persons in New Zealand under each set of sanctions. Noting that sanctions apply to all persons in New Zealand, and not just reporting entities.

293. Globally, many individuals are associated with terrorist entities. However, country-specific proliferation financing-related TFS by the United Nations Security Council (UNSC) currently emanate entirely from two countries (Iran and the Democratic People's Republic of Korea (DPRK)).

294. For the first time, the 2024 NRA has included a proliferation financing risk assessment. New Zealand has a well-developed AML/CFT regime and is therefore not likely to be attractive for proliferation financing. Vulnerabilities for proliferation financing are likely to be similar (but broader) to those for money laundering or terrorism financing as the proliferation financing risk could occur through the transfer of funds or goods out of New Zealand, or through the provision of assistance to a proliferating state (potentially without funds ever moving into or out of New Zealand).

295. Because there has been limited identification of proliferation financing-related TFS breaches, the 2024 NRA found that New Zealand faces a low risk of proliferation financing. However, the NRA represents a point-in-time assessment, S9(2)(g)(i) [redacted]

What is the existing statutory framework for sanctions in New Zealand?

296. The United Nations Act 1946 (UNA) and the Terrorism Suppression Act 2002 (the TSA) require all New Zealanders to implement TFS imposed by the UNSC. Non-compliance is a criminal offence. The Russia Sanctions Act 2022 (RSA) also imposes sanctions responding to Russia's invasion of Ukraine. These are not mandated by the UNSC. Positive obligations

within these statutes (e.g. PPCs that would provide assurance that TFS are not being breached) are limited and relate primarily to reporting suspicions of sanctions evasion for sanctions under the TSA and RSA.[38]

MFAT's role in the implementation of sanctions

297. MFAT is responsible for sanctions policy in New Zealand, and administers sanctions legislation, including the TSA, the UNA and the RSA.

298. In 2022, MFAT established a Sanctions Unit, with an explicit operational role to implement the RSA. The Sanctions Unit also has administrative responsibility for UN sanctions. The Sanctions Unit provides core policy, legal, education and outreach on sanctions. It also provides a governance role for the compliance and enforcement of sanctions, including supporting information sharing with relevant agencies across the sanction's environment.

299. However, other than it being an offence not to report a suspicious activity under the TSA, or to breach a sanction, the Sanctions Unit has no legal authority to set TFS compliance standards. Furthermore, MFAT undertakes no activities to proactively supervise the effectiveness of reporting entity processes for implementing TFS. S9(2)(g)(i) [redacted]

300. MFAT also house the Export Control Unit. The purpose of New Zealand's Export Controls regime is to regulate the export of goods which may be intended for use that could, directly or indirectly, be to the detriment of New Zealand's security or national interests, or contribute to human rights abuse or the contravention of international humanitarian law. These comprise strategic goods, dual use goods, such as some drones, night vision technology, thermal imaging and also certain other goods intended for export to military and police end-users.

What are the FATF TFS Recommendations?

301. The FATF includes two specific recommendations relating to the effective implementation of TFS relating to the prevention, suppression, and disruption of terrorism financing (Recommendation 6) and proliferation financing (Recommendation 7). The recommendations require countries to freeze without delay the funds or assets of any person or entity designated by the UNSC, and to ensure that no funds or assets are made available to them.[39]

302. TFS requirements are rules-based rather than risk-based. Therefore, the fact that New Zealand is at low risk to terrorism and proliferation financing is not relevant to the assessment of our compliance with FATF Recommendations 6 and 7.

303. The FATF has also recently (in 2020) amended Recommendation 1 (Assessing risks and applying a risk-based approach). The updated recommendation requires countries and

---

[38] There is only an obligation to report suspicious activity, or, under the Terrorism Suppression Act, an obligation to freeze the known assets of a designated entity and submit suspicious property reports.

[39] Recommendation 6 is applicable to all designated entities listed in UNSC resolutions 1267 and its successor resolutions, and UNSC resolution 1373. Recommendation 7 is applicable to all current and future UNSC resolutions applying targeted financial sanctions relating to the financing of proliferation of weapons of mass destruction.

their reporting entities to identify, assess and effectively mitigate the risk of non-implementation or evasion of the proliferation financing-related TFS obligations. Without reform, New Zealand is at risk of being downgraded to non/partially-compliant on Recommendation 1.

304. Finally, FATF Recommendations 26 and 28 require that countries ensure that financial institutions and designated non-financial businesses and professions (DNFBPs) are subject to adequate regulation and supervision. This includes the supervision for the effective and proportionate implementation of reporting entities' TFS obligations.

305. The FATF's MER process also assesses the effectiveness of the operational implementation of policy through its immediate outcomes (IO's). There are several IO's relevant to TFS, including IO1 (Identification of risk), IO3 and IO4 (Preventive measures and supervision for financial institutions and DNFBPs), IO10 (Implementation of terrorism financing TFS) and IO11 (Implementation of proliferation financing TFS).

306. Effectiveness of TFS implementation depends on a range of activities, including:

- how well a supervisor promotes understanding of risk amongst reporting entities, and whether proportionate, risk-based measures are implemented,
- whether a supervisor is effectively monitoring compliance,
- whether a supervisor understands the level and nature of risk across the sector,
- how well reporting entities understand their obligations,
- how effectively supervisors communicate change,
- procedures for ensuring relevant information is collected, and
- whether funds for persons designated in TFS are identified and prevented from being moved through New Zealand-based reporting entities.

How is TFS/PF approached in other jurisdictions?

307. In the UK, TFS and PF are part of the AML/CFT system (rather than introducing new legislation), and AML supervision also includes PF and TFS. In line with the UK's higher sanctions risk environment, the supervisory model is very comprehensive. Reporting entities are required to undertake formal assessments for terrorism financing and proliferation financing related-TFS risk.

308. The Government of Canada has been attempting to update its sanctions regime by targeting sanctions evasion through changes to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and the Criminal Code. Reporting entities must report every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a sanction's evasion offence. The Financial Transactions and Reports Analysis Centre of Canada has advised that reporting entities must include policies and procedures that are developed and applied to assess their money laundering, terrorist activity financing and sanctions evasion risks.

309. Australia is further ahead than New Zealand in implementing a TFS compliance regime. Whilst Australia has not changed the objectives of its AML/CFT Act, its new ML/TF risk assessment requirements state a reporting entity is required to identify and assess the risk of ML, FT, and PF that the reporting entity may face. Reporting entities are also required to monitor for unusual transactions and behaviours that may give rise to a suspicious matter reporting obligation, including in relation to sanctions offences (not just targeted financial sanctions, but all sanctions offences).

310. In the United States, The Office of Foreign Assets Control (OFAC) within the US Department of the Treasury administers and enforces these sanctions, as well as the United States' autonomous sanctions regime. Formal assessments of TFS risks are not a requirement under the US regime. The US regime includes significant penalties for wilful sanctions violations (up to 20 years in prison). A separate Treasury Department bureau, the Financial Crimes Enforcement Network, is responsible for countering AML/CFT.

What is the policy problem or opportunity?

Why is New Zealand concerned about TFS?

311. TFS imposed by the UN establish rules-based obligations that all countries must abide by. International financial institutions, although not exclusively, are subject to these rules and assess the risk of doing business with foreign partners in order to have confidence that they will not breach their own stringent obligations to their home jurisdictions.

312. The expectations of these international banks and financial institutions are a major driver of the current practice of New Zealand businesses. Larger New Zealand financial institutions generally already assess and mitigate their sanctions risks in order to meet these expectations. However, the FATF has identified that there is a wide variation in the understanding of how to effectively implement TFS by New Zealand businesses. Poor understanding of obligations could result in additional costs and unnecessary disputes between reporting entities, and their partners and customers.

313. Members of the IAG who commented on these proposals generally supported the establishment of a statutory supervision regime for TFS-compliance, provided the supervisor had the necessary sanctions expertise to set clear regulatory expectations and provide guidance and education. For this reason, submitters in the banking sector generally supported the establishment of a supervisor within MFAT, or within a new dedicated sanctions agency. This, would empower industry to meet their international obligations, thereby supporting access to the international financial system.

The FATF has identified several deficiencies with New Zealand's TFS regime

314. In the absence of a dedicated supervisor to set clear expectations and support implementation of TFS, the FATF has identified a number of deficiencies in New Zealand's TFS regime. At the last FATF MER, New Zealand was found to be partially compliant with Recommendations 7, 26 and 28.

315. In the FATF's 2021 MER of New Zealand identified the following deficiencies:

- Up-to-date lists of designated persons or entities are not easily accessible, including in consolidated form.

- This information, and timely notice of changes to it, is not proactively provided to reporting entities.
- A significant number of reporting entities are not registered (nor are they obligated to be registered) to directly receive such information through channels (i.e. goAML[40]) which could be used to proactively provide the information.
- Insufficient guidance and outreach is provided to help reporting entities understand and action their TFS obligations, including where reporting should be directed.
- Due diligence undertaken by reporting entities to identify sanctioned persons is insufficient, either in terms of sophistication or timeliness.

316. Administrative, operational, and potentially some low-cost resourcing improvements by regulatory agencies can help address some of the deficiencies identified by the FATF. These include the provision of up-to-date and accessible information about designated entities, the content and quality of guidance and the proactive education and engagement of those with obligations.

317. However, without reform to address some of the higher-level deficiencies around supervision, it is likely that New Zealand will again be found partially or non-compliant recommendations 7, 26 and 28.

318. Furthermore, the amendment to FATF Recommendation 1 to require the incorporation of PF sanctions into risk assessments will be a hard requirement for compliance with FATF Recommendation 1 in the next MER. Without amendments to achieve this, we will be at significant risk of being found non-compliant with Recommendation 1, which will have a cascading effect through the rest of New Zealand's assessment. This particular obligation will create a greater imposition and cost on captured businesses.

319. In IO 10 (preventative measures and financial sanctions for terrorism financing)) and IO 11 (implementation of proliferation financing sanctions), the FATF noted shortcomings reflected the absence of meaningful supervision of either set of targeted financial sanctions. All three sections repeated the recommendation that, to address the above deficiencies, an appropriate agency or agencies should be given clear powers and mandate to supervise and enforce both types of TFS.

320. Some of the identified FATF deficiencies (e.g. the provision of guidance, the provision of up-to-date lists of designated entities) could be addressed through improved operational practice. Additionally, there are a range of informal supervisory interventions that MFAT and DIA could undertake that may enhance compliance with FATF recommendations (e.g. supervising the effective reporting of suspicious activities relating to terrorism financing TFS).

Without effective supervision of TFS implementation, reporting entities will struggle to meet international expectations

321. TFS deficiencies identified by the FATF have not been addressed, and New Zealand still has no legally mandated authority to set standards and assess compliance with TFS. This

[40] The goAML application is a fully integrated software solution developed specifically for use by FIU's and is one of United Nations Office on Drugs and Crime's strategic responses to financial crime, including ML/TF.

results in businesses being left to determine what is needed to meet the requirements of international partners by themselves.

322. Additionally, establishing an effective compliance and supervision regime (above the current compliance through the UN sanctions mechanism) will support compliance with FATF technical recommendations and IO's. Without reform, it is likely New Zealand will be found partially/non-compliant or downgraded for TFS related recommendations at our next MER. S9(2)(d) [redacted]

What consultation has been undertaken?

323. Consultation beyond the AML/CFT supervisors, Police, the FIU and IAG has included:

- Engagement with the MFAT New Zealand Sanction Unit
- Direct engagement with key banks due to their higher risk in the TFS environment
- Engagement with AUSTRAC and His Majesty's Treasury on the approach to supervising TFS in Australia and the United Kingdom.

What options are being considered?

324. We have explored a range of options to establish an AML/CFT compliance and supervision regime. These included establishing a requirement for risk assessment, mitigation and supervision of proliferation financing more generally (not just proliferation financing related-TFS). The following three options were progressed based on the fact that they most effectively address identified statutory FATF deficiencies and involve the smallest impact on reporting entity obligations and costs:

- Option One: amend the Act to establish a TFS compliance and supervision function within the AML/CFT supervisor (DIA);
- Option Two: establish compliance and supervision functions for TFS within a separate legislative vehicle (e.g. the UN act and regulations) with MFAT as the supervisor; and
- Option Three: establish a new dedicated agency for AML/CFT and TFS supervision and compliance through a new legislative vehicle.

Status quo

325. Without reform, there will continue to be a lack of proactive assurance through supervision. As a result, it is likely that varying degrees of understanding of obligations and the approach to implement TFS by businesses in New Zealand will remain. This lack of proactive assurance supervision will also contribute to at the risk of being found non-compliant with FATF recommendations.

Option One – TFS with DIA

326. New Zealand's maturing AML/CFT regime provides an existing framework that can be used to establish a compliance and supervision regime for the implementation of TFS. Specifically:

- all reporting entities must carry out an assessment of the ML/TF risk that they may reasonably expect to face. Based on that risk assessment, the reporting entity must create an AML/CFT compliance programme (Programme);
- the Programme (among other things) sets out the reporting entity's policies, procedures and controls (PPCs) to detect, manage and mitigate the risk of ML/TF; and
- the risk assessment and Programme must be reviewed and kept up to date by the reporting entity and reported annually to their AML/CFT supervisor.

327. By amending the purpose of the Act, it would be possible to incorporate TFS within the Act. This approach is broadly in line with that taken by Australia and the United Kingdom. In addition to amending the purpose of the Act, there would need to be several amendments to the AML/CFT Act to support this approach:

- reporting entities would explicitly need to consider their TFS obligations when undertaking their risk assessment (section 58) and developing their AML/CFT programme (section 56) and associated AML/CFT PPCs,
- the supervisor's functions (section 131) would need to be amended to include the supervision of reporting entity TFS obligations,
- enable the supervisor to issue guidance and offer support to reporting entities as they implement their TFS obligations to ensure that the obligations placed on reporting entities are commensurate with their risk profile,
- establish a regulation-making power to enable specific TFS measures to be imposed by regulation; and
- additional consequential amendments to reflect the expanded purpose of the Act and to support the supervisor to carry out its new functions (e.g. amending the scope of the power to grant exemptions and make regulations to include proliferation financing, amending the obligation to report suspicious activities relevant to TFS to include proliferation financing TFS).

328. This would not oblige reporting entities to undertake separate risk assessments for TFS but would enable these to be incorporated as part of existing obligations. If a reporting entity does identify any risks, they would be required to show how they would implement their proliferation financing related TFS obligations through their AML/CFT Programme.

Option Two – TFS with MFAT

329. This option would establish MFAT as the supervisor for TFS and wider sanctions (e.g. trade sanctions), with a legal compliance and supervision mandate established within a separate legislative vehicle. s9(2)(g)(i) [redacted]

330. In order to address the lack of uniformity in the approach of businesses to TFS obligations and support compliance with the FATF Recommendations, the RSA would need to be amended to establish:

- the functions of MFAT as the supervisor for sanctions implementation,
- the power for MFAT to supervise sanctions implementation, including the power to:

i. require the production of information and conduct interviews relevant to the assessment of compliance with sanctions obligations,

ii. conduct on-site inspections of businesses with sanctions obligations,

- a requirement for duty holders to assess and mitigate their sanctions risk,
- an amendment to the definition of a duty holder (currently based on the definition of a reporting entity) to incorporate wider businesses and at-risk organisations; and
- the application of the Act's supervision provisions to wider sanctions, including TFS issued by the UNSC.

331. MFAT, as part of its overarching responsibility for the sanctions regime, would take on specific responsibility for TFS. Operationally, responsibility for the supervision of TFS would likely sit within the existing MFAT Sanctions Unit coupled with the MFAT responsibility for Export Control.

332. Establishing TFS responsibilities within MFAT would maintain banking industry preferred separation of sanctions and AML/CFT.

Option Three – TFS within a new dedicated departmental agency

333. Option Three would establish a single agency with authority to implement and supervise sanctions. This option would likely ensure compliance with FATF recommendations. However, it would require substantive revisions to both the Act and sanctions legislation that would not be feasible in the timeframe before the next MER.

How do the options compare to the status quo/counterfactual?

	Option One – TFS with DIA (Preferred)	Option Two – TFS with MFAT	Option Three – New Sanctions agency
Effective	+ FATF compliant and leverages existing supervisor capabilities. Restricts scope to only reporting entities.	++ FATF compliant and leverages MFAT's sanctions expertise. Creates a wider supervision scheme, and potentially supports its application to a wider range of sanctions.	+ + FATF compliant and establishes a dedicated agency for sanctions compliance and financial intelligence. Creates a wider supervision scheme.
Efficient	+ Uses a single, consolidated statute and aligns with partner jurisdictions. Opposed by majority of banking sector submitters.	+ Establishes a single home for sanctions policy, administration and supervision but requires the establishment of a separate supervision process. Supported by majority of banking sector submitters.	**0** Establishes a dedicated agency for sanctions administration and supervision but requires the establishment of a separate supervision process.
Feasible	+ Leverages existing risk assessment and	- - No existing legal framework to give MFAT a legal mandate to supervise TFS.	- - A new agency, while preferred by industry,

	supervision framework but will require the supervisor to build new TFS supervision capacity.	MFAT would need to build supervisory capability.	would involve substantial costs and revisions to both the Act and sanctions legislation.
Overall assessment	+ Establishes an effective and FATF compliant supervision model that can be feasibly implemented.	**0** An effective option but not feasible given MFATs lack of legal mandate and operational role.	- Establishes an effective model, but requires substantive revisions to legislation that are not feasible prior to the next MER.

What option is likely to best address the problem, meet the policy objectives, and deliver the highest net benefits?

Option One is the preferred option

334. Amending the Act to include supporting the implementation of proliferation financing and terrorism financing-related TFS (Option One) is the preferred option. This option represents an effective approach to addressing the fundamental deficiency with our TFS system, by establishing a dedicated TFS supervisor, and requiring reporting entities to assess and take steps to mitigate their TFS risk.

335. From a feasibility perspective, Option One also has several advantages. It allows the TFS supervisor to leverage existing functions within the AML/CFT supervisor, including intelligence and risk analysis, and on-site inspection powers. It also avoids the duplication of risk assessment and on-site supervision processes at two different agencies.

336. Comprehensive guidance and outreach will be pivotal for the effective risk-based implementation of PPCs (as required) to comply with TFS. This guidance will need to be kept up to date and leverage both MFAT and FIU's experience and role in the implementation of TFS. Uncertainty about the Supervisor's mandate to assess TFS compliance could be addressed by establishing in legislation the ability of the supervisor to provide guidance. This would be a new area of DIA responsibility with corresponding need for resourcing and skills. The cost of establishing the new function could be funded from within existing AML/CFT baselines and the industry levy established through the AML/CFT (Supervisor and Levy) Amendment Bill.

337. The Act only regulates reporting entities, while TFS apply to all New Zealanders. This difference risks creating fairness issues, as some low risk reporting entities could be required to undertake risk assessments, while other high-risk non-reporting entities (e.g. import and export companies) are not. Option One provides the potential to expand the TFS supervision scheme to non-reporting entities such as import and export service providers via Regulations. The consideration of regulations would require engagement with MFAT, Customs and other agencies.

Industry and impacted agencies have been consulted on the options

338. Non-bank IAG members were not opposed to the AML/CFT supervisor taking a role in TFS supervision, though they noted that the supervisor's role would need to be defined clearly to avoid unintended consequences.

339. One banking sector representative also supported Option One, noting the criticality of New Zealand achieving compliance with FATF recommendations. They considered that the impact of incorporating TFS into the Act would have a minimal impact on compliance obligations, provided the supervisor takes a pragmatic approach to minimising disruption. However, the majority of banking sector representatives were opposed citing the differences between the strict liability nature of TFS and the risk-based nature of the AML/CFT system; the increased costs associated with TFS risk-assessment; potential ambiguity about who (MFAT or DIA) has responsibility for TFS implementation; and the non-application of AML/CFT laws to potential high TFS-risk entities (e.g. import and export companies).

340. The preferred option of most banking sector submitters was Option Two: establishing TFS supervision within MFAT. Option Two is likely to be as effective as Option One establishing a TFS supervision scheme. However, Option Two is not viable as it would require amending an existing legislative vehicle (e.g. the RSA) to give MFAT a legal mandate to supervise TFS implementation. This would require substantive reforms to the purpose and scope of the legislation that are not feasible in the time before the next MER.

341. In addition, S9(2)(g)(i) [redacted]. It would require establishing an entirely new operational function and the related support services. This would require additional Crown funding, as the levy was established to only fund AML/CFT activities undertaken by the supervisor, the FIU and the Ministry of Justice.

342. Option Three would also require substantive revisions to both the Act and sanctions legislation. Following analysis, it became clear that Option Three, while favoured by IAG during consultation, was not feasible in the current budget, time and legislative constraints.

Additional compliance burden of TFS for most reporting entities will be low

343. Banking sector representatives of the IAG considered that there will be increased costs associated with TFS risk-assessment and mitigation requirements for reporting entities, many of whom will be low-risk. We consider there are mechanisms to mitigate this concern.

344. Establishing new requirements to assess and mitigate risk for TFS will incur additional compliance costs. The amount of burden will depend on the level of risk a reporting entity faces and the amount of current work that is done to assess and mitigate those risks. High risk entities include banks, money or value transfer services (e.g. remitters), VASPs and trust and company service providers.

345. For larger institutions (such as banks) with established sanctions risk assessment functions, these costs would relate primarily to ensuring that existing TFS procedures and assessments are included or linked to the AML/CFT programme. However, smaller

reporting entities could be more exposed to cost increases as TFS controls require different skillsets and/or processes to current AML/CFT requirements.

346. However, the additional costs of establishing risk assessment requirements (a FATF requirement) will be incurred regardless of where the supervisor is established. Further, the FATF's Guidance on Proliferation Financing Risk Assessment and Mitigation notes that low risk, small reporting entities serving predominantly locally based and low-risk customers are not expected to devote significant time and resources to risk mitigation.

347. We consider that in most cases the additional compliance burden of these requirements is expected to be quite low. For many low-risk reporting entities it may amount to no more than establishing their awareness of the sanctions regime, their potential vulnerabilities and noting that they do not expect to be exposed to TFS risks. This approach is considered best practice by the United Kingdom's Financial Conduct Authority for small firms.

348. Additionally, it will also be possible for exemptions to be issued for classes of reporting entities from proliferation financing-TFS obligations, where risk is low (as determined by the National Risk Assessment and Sector Risk Assessments). The FATF recommendations state that where there is an assessed low risk of proliferation financing relating to reporting entities, countries may decide to exempt them from risk assessment, management and mitigation requirements. Providing exemptions would ensure that the compliance burden is targeted at the highest risk rather than across all reporting entities.

Is the Minister's preferred option in the Cabinet paper the same as the agency's preferred option in the RIS?

349. Yes.

What are the marginal costs and benefits of the preferred option in the Cabinet paper?

Affected groups	Comment.	Impact	Evidence Certainty
Additional costs of the preferred option compared to taking no action			
Regulated groups	Expand risk assessment. Expand compliance programme. Ongoing TFS measures in line with existing AML/CFT requirements. Some initial cost and some cost for ongoing measures (e.g. screening, transaction monitoring). Larger financial institutions are likely to be undertaking these activities already and so will face limited additional cost.	*Low to medium –* depending on risk profile and existing sanctions capability.	*High*
Regulators	Would require the establishment of dedicated TFS resource within the single supervisor. Supervisor responsibilities would include: • Production of guidance material including sector risk assessments and TFS focused material. • Engagement and outreach with industry • Upskilling of supervisory staff in TFS. • TFS related supervision, Some initial costs for guidance production and training. Also ongoing costs to maintain skill set, keep material up to date, undertake TFS supervision, develop intelligence and engage with industry. s9(2)(g)(i) [redacted] A scaled option s9(2)(f)(iv) [redacted] to lead the development of guidance and upskill the rest of the Supervisor. Justice officials consider this could achieve desired outcomes. s9(2)(g)(i) [redacted]	*Medium*	*High*
Others (eg, wider govt, consumers, etc.) *For fiscal costs, both increased costs and loss of revenue could be relevant*	FIU (and police) to upskill on TFS, including additional resourcing to analyse intelligence and produce guidance material. TFS related intelligence and investigative actions. Additional capacity at FIU and Police will be required if the establishment of a supervision regime results in an increase in suspicious activity reports relating to TFS. Some initial costs for guidance production and training. Also ongoing costs to maintain skill set and keep material – e.g NRA and alerts - up to date. TFS related information gathering, intelligence production and investigations will need resourcing. TFS matters are complex and international in nature. FIU has suggested a provisional estimate of 4 additional FTE may be required, while Police have stated that to investigate the breach of sanctions will	*Medium*	*High*

	also require an additional 4FTE that will need to be funded from a Crown allocation.		
Total monetised costs		NA	NA
Non-monetised costs		*Medium*	*High*
Additional benefits of the preferred option compared to taking no action			
Regulated groups	Businesses provided with education and support on how to comply with their TFS obligations. Benefits to reporting entities in terms of improved access to international capital s9(2)(d) [redacted]	*High*	*High*
Regulators	Supervision of AML/CFT will lead to more uniform understanding of sanctions obligations, and a better understanding of New Zealand's TFS risk environment.	*Medium*	*High*
Others (eg, wider govt, consumers, etc.)	FIU will have a better intel picture of TFS. MFAT will have improved sanctions oversight (via NCC/SGG). Police will be better positioned to investigate sanctions related cases. NZ will meet FATF requirements around TFS recommendations and immediate outcomes. s9(2)(d) [redacted] Greater confidence in the NZ financial systems. Alignment with like-minded countries on TFS. Easier to do business internationally.	*High*	*High*
Total monetised benefits		NA	NA
Non-monetised benefits		*Medium-High*	*High*

Section 3: Delivering the options

How will the proposals be implemented?

We plan to introduce legislation in Q2 2026 to be ready for the 2028/29 MER

350. To contribute towards FATF compliance proposals must be in effect by the beginning of New Zealand's next MER which is scheduled to begin in late 2028. To achieve this, we intend to introduce legislation giving effect to the proposals in Q2 2026.

351. This allows one year for passing the Bill (Q2 2027) and an additional one-year transition period (Q2 2027 – Q2 2028) for reporting entities to become familiar with the changes to the Act. If the Supervisor considers additional implementation time is required for businesses, they will be able to take an "assisted compliance" approach for a period for a time or for specific issues as appropriate. A communications plan will be developed to educate and inform stakeholders of the amendments to the Act and support them through the transition period.

Levy funding will support implementation

352. The funding model proposed in Workstream 2 (Single Supervisor and Levy) will see the industry regulation component of the system partially funded by the levy, while enforcement and public good aspects remain Crown funded. The levy is anticipated to begin collection in mid-2027 in time to support the implementation of Workstream 3 proposals and the transition period.

The single supervisor and FIU are key to the implementation of the proposed settings

353. The single supervisor proposed by Workstream 2 will be the central regulatory agency in the AML/CFT system. As such it will be key to the implementation of the new arrangements for CDD and DBGs. DIA (the proposed single supervisor) has been consulted on the development of the options and supports the proposals including the ability of the single supervisor to implement the proposals once in effect.

354. Supervisory guidance and updated or new codes of practice will be key tools for ensuring reporting entities know and understand their obligations. Clarity around the changes to the Act, particularly what is now required under a more risk-based approach to CDD, will help ensure businesses are taking advantage of the improved approach and are minimising transition costs. DIA, supported by RBNZ and FMA, has already begun work to identify and plan for the necessary guidance to enable the transition to a single supervisor,[41] which can be extended to the implementation of the Workstream 3 proposals.

355. The FIU expects it will require additional resource to fulfil its intelligence functions in relation to TFS and PF. Introducing TFS into the AML/CFT system will increase the indicators of potential PF or sanctions evasions, which will enable more criminal investigations to occur. Additionally, increased guidance from the supervisor to entities

[41] The establishment of a single supervisor and introduction of an industry levy are being progressed through Workstream Two. These changes have been agreed by Cabinet and are currently in the legislative drafting stage. We intend to introduce a Bill in Quarter Three of 2025.

will result in an uptick in reporting, which will increase the requirement on FIU to fulfil its intelligence functions and on Police for related investigations.

356. Key, as with other aspects of reform, will be managing expectations, engaging with reporting entities early and producing high quality timely guidance material. Outreach and education will be important, especially regarding the proposed ‘light touch’ TFS supervisory model. As with the introduction of the AML/CFT Act, other potential initiatives to make things easier for reporting entities could be a grace period to become compliant with TFS, class exemptions and the creation of regulatory safe harbours which provide certainty to reporting entities.

357. The proposals also include additional powers for the FIU. Police was closely involved in the design of these powers and have been consulted on their effectiveness in providing the information needed to carry out the FIU’s functions and meet international obligations.

How will the proposal be monitored, evaluated, and reviewed?

358. New Zealand will undergo a MER in 2028/29 which will comprehensively evaluate our AML/CFT system for both effectiveness and technical compliance with the Recommendations. The MER, and our subsequent rating by the FATF, will be an early indication of the impact of these proposals and where there might still be gaps or improvements.

359. The changes to the supervisor, introduction of an industry levy and legislative reform will also be supported by an AML/CFT National Strategy (Strategy) developed in partnership with industry. The Strategy will build on the foundation of legislative reform, to provide a clear pathway to maximise system infrastructure and ensure it operates effectively and efficiently to deliver the best outcomes by identifying the key actions, responsible parties, and timeframes needed to support the realisation of system goals. Industry participation in the development implementation of the Strategy will ensure transparency and enable meaningful consultation on how levy payers’ contributions are used. This will provide a further mechanism to monitor and evaluate the effectiveness of the regulatory settings changes proposed in this RIS.

360. The effectiveness and functioning of the system will also be monitored and reported on through the National Coordination Committee (NCC) comprising the key AML/CFT agencies.

S9(2)(d)