Internal Affairs
Te Tari Taiwhenua

New Zealand Government
Te Kāwanatanga o Aotearoa

Sector Risk Assessment

Accounting

September 2026

AML ONLINE

Risk Assessment Requirements:

The DIA has produced this sector risk assessment (SRA 2026) for accounting practices under section 132(2) of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act).

The Department of Internal Affairs (DIA) is the supervisor of businesses that are accounting practices with obligations under the AML/CFT Act. The term 'accounting practice' in the SRA 2026 means an 'accounting practice' that is a reporting entity under the AML/CFT Act. This includes an accountant in public practice on their own account in sole practice, a partnership or an incorporated accounting practice.

Under section 131 of the AML/CFT Act, one of the functions of an AML/CFT supervisor is to assess the level of money laundering and terrorism financing risk across all the reporting entities that it supervises. This Sector Risk Assessment (SRA 2026) has been produced as part of this function.

For the purposes of section 131 of the AML/CFT Act, the DIA assesses the following accounting practice services as the most vulnerable to money laundering or terrorism financing. These services are identified as having **relevant risks** (as at the date of publication of the SRA 2026). An accounting practice that carries out one or more of the following services **must** incorporate assessment of the risks associated with the service in its risk assessment.

Money laundering:

- Trust and company services
- Trust accounts
- Insolvency practice
- Other management of client funds, accounts, securities or assets

Terrorism financing:

- Trust and company services

Note: An accounting practice must also have regard to the SRA 2026 when conducting or updating its risk assessment in relation to its other services.

Accounting: Sector Risk Assessment 2026

Inherent Vulnerability Rating:

- Money Laundering: **Medium**
- Terrorism Financing: **Low** (except for trust and company services rated **Medium-High**)
- Proliferation Financing: Low (except for trust and company services rated **Medium-High**)

Strength of AML/CFT Controls Rating: Moderate

Residual Sector Risk Rating:

- Money Laundering: **Low-Medium**
- Terrorism Financing: **Low**
- Proliferation Financing: **Low**

Contents

Executive summary

1. Accounting practices are often referred to as **gatekeepers**. This is because they provide specialist services that facilitate the entry and movement of funds in the financial system. These services can be misused by criminals.
2. This Sector Risk Assessment for accounting practices (SRA 2026) follows the National Risk Assessment conducted by the New Zealand Police Financial Intelligence Unit (FIU) in 2024 (NRA 2024). The SRA 2026 considers supervisory findings and data and includes an assessment of the effectiveness of the sector's overall AML/CFT controls.
3. The inherent vulnerability and residual risk ratings assessed in the SRA 2026 reflect the accounting sector **as a whole**. Not all accounting practices will have the same level of risk.
4. The SRA 2026 assists accounting practices to understand their money laundering (ML) and terrorism financing (TF) risks and implement an AML/CFT programme to mitigate those risks.[1]

Money laundering

5. Money laundering is the process that criminals use to "clean" the money or assets generated from crime. Money laundering involves converting the money or assets from one form to another, disguising the ownership of it, or otherwise taking steps to conceal its origin.
6. The **Money Laundering Threat** to New Zealand is significant. The three highest risk crime threats for Money Laundering in New Zealand are **fraud**, **drug crime,** and **transnational laundering** from foreign predicate crimes (by which funds are laundered through New Zealand's financial system). More than $1.6 billion is generated annually for laundering in New Zealand just from fraud and drug crime.[2] The volume of funds laundered through the New Zealand financial system from crimes committed overseas is unknown.
7. Other significant crime threats in New Zealand are **tax non-compliance** and **property crime** (including retail crime, burglary, and vehicle theft).

Accounting sector

8. There are 1,444 known accounting practices that are reporting entities under the AML/CFT Act. The sector is disparate in nature, with varying levels of regulatory oversight, professional standards and types of practitioners. Broadly, the sector comprises chartered accountants, other qualified statutory accountants, insolvency practitioners, bookkeepers, tax agents and PAYE intermediaries.

[1] The SRA 2026 also considers proliferation financing (PF) risks.
[2] New Zealand Police **New Zealand National Risk Assessment 2024** (March 2025) at 24 and 28.

9. The money laundering risk faced by an accounting practice may be:
    - **Direct** - the accounting practice is directly responsible for transacting the proceeds of crime (including involving funds transacted through a trust account or other bank account on which it has authority).
    - **Indirect** - the accounting practice's services (for example trust and company services) are enablers of money laundering. These services allow the proceeds of crime to be converted, disguised or concealed, even though the accounting practice does not directly conduct any financial transactions.
    - In some circumstances, an accounting practice's risk is both **direct** and **indirect**.

Sector vulnerability to money laundering

10. The services provided by accounting practices that have higher inherent vulnerability to money laundering are **trust and company services**, **trust accounts**, **insolvency practice** and other **managing of client funds, accounts, securities or assets**.

Services	ML Vulnerability Rating
1. Trust and company services	**Medium-High**

Trust and company services include forming legal persons or legal arrangements and acting (or arranging for a person to act) as a nominee director or nominee shareholder or trustee. Companies, limited partnerships, or trusts (and other legal structures) can be misused for money laundering, or for the commission of underlying criminal activity such as tax evasion. This includes through setting up fake businesses, such as consulting, investment, or import/export, including obtaining banking facilities.

The money laundering vulnerability primarily relates to the ability to conceal or obscure ultimate beneficial ownership or effective control of the legal person or arrangement. This enables the ownership or transfer of funds or assets to be disguised, and for underlying parties to be hidden. Furthermore, the involvement of an accountant as a nominee or trustee provides an impression of respectability so that financial or other activity appears legitimate. This assists to avoid detection.

Services	ML Vulnerability Rating
2. Managing client funds – trust accounts	**Medium-High**

When an accounting practice operates a trust account, the money laundering risk is at its most direct. Once funds are in a trust account, access to the wider banking and financial system is facilitated and at the same time, the origin of the money is obscured to onwards recipients.

Services	ML Vulnerability Rating
3. Insolvency practice	**Medium**

The nature of insolvency practice means that the money laundering vulnerability manifests differently. At the point of liquidation, receivership or administration, it is the insolvency practitioner in control of the client, i.e. the insolvent entity and/or its assets, depending on the nature of the appointment.

The money laundering vulnerability arises from criminals seeking to exploit the insolvency process. This allows audit trails to be masked and could involve collusion between persons associated with the insolvent entity and its creditor(s). Additionally, there may have been underlying criminal activity associated with the insolvent party.

Services	ML Vulnerability Rating
4. Other managing client funds, accounts, securities, or assets	**Medium**

It is common for an accounting practice to manage client funds, accounts, securities, or other assets (other than as part of a trust and company service).

In these circumstances, funds or assets are usually held directly in the name of the owner with the accounting practice authorised to act as a representative on their behalf. For example, as an authorised signatory on a bank account, for other business activity or in relation to investments. The ability to conceal or disguise beneficial ownership is therefore harder. However, the involvement of an accounting practice still provides an impression of respectability and legitimacy to financial transactions that may be attractive to criminals.

Other services

11. Other services provided by accounting practices have lower inherent vulnerability to money laundering but could also be exploited. These are:

Services	ML Vulnerability Rating
5. Bookkeeping	**Low-Medium**
6. Tax transfers	**Low**
7. PAYE intermediary	**Low**
8. Providing registered office or other address	**Low**
9. Other accounting services subject to the AML/CFT Act	**Low**

Overall sector ML vulnerability

12. The overall inherent sector vulnerability rating to money laundering of the accounting sector is assessed as **Medium**.

Strength of Controls

13. DIA's AML/CFT supervision of accounting practices assesses controls at the sector level as **moderately** effective in managing and mitigating the sector's vulnerability to money laundering. In particular:
    - ✓ Nearly all accounting practices known to the DIA have appointed a compliance officer and have a written risk assessment and AML/CFT programme.
    - ✓ Most accounting practices conduct standard customer due diligence on their clients, keep records, and are enrolled to report prescribed transactions and suspicious activity to the New Zealand Police Financial Intelligence Unit (FIU) via goAML.
    - ✓ Some accounting practices, including most larger practices, have implemented strong governance and compliance frameworks to detect and respond to money laundering risks.
    - ✓ Some accounting practices are reporting suspicious activity and prescribed transaction reports. From 1 October 2018 to 31 December 2025, there were:
        - 111 suspicious activity reports, with approximately 6% of accounting practices having submitted a report.
        - 9,601 prescribed transaction reports (covering 13,444 transactions).
14. Notwithstanding the above, the DIA identifies three factors impacting the effectiveness of AML/CFT controls at a sector level:
    - There is no requirement that accounting practices register with DIA as the AML/CFT supervisor. This means DIA must proactively identify those accounting practices that are reporting entities and do not make themselves known to DIA. Noting the disparate nature of the sector, it is likely that not all accounting practices are known to the DIA or subject to active AML/CFT supervision.
    - There are common deficiencies across the sector relating to requirements to monitor, examine and keep written findings for high-risk clients, activities, or transactions, and to conduct enhanced customer due diligence in all situations where the level of risk requires it.
    - The number of suspicious activity reports from accounting practices is consistently low. Noting the deficiency above relating to monitoring, examination and enhanced customer due diligence, it is possible that not all suspicious activity is being identified or reported to the FIU.

Overall sector risk rating – Money Laundering

15. While the accounting sector has a medium inherent money laundering vulnerability rating, the implementation of AML/CFT controls reduces the risk of the sector being targeted by criminals seeking to launder illicit funds. Accordingly, the residual risk rating of the accounting sector after the implementation of AML/CFT controls is assessed as **Low-Medium**.

Inherent ML Vulnerability Rating	Strength of Controls Rating	Residual ML Risk Rating
Medium	**Moderate**	**Low-Medium**

Terrorism financing

16. While money laundering is the process of concealing the illicit origin of proceeds of crime, terrorism financing is the process by which terrorist acts, or ongoing operations to perform terrorist acts, are funded.

17. The overall **Terrorism Financing threat** to New Zealand is assessed as **Low**. However, and while not specific to accounting practices, the NRA 2024 determines there is a possibility that New Zealand companies have or will at some future time be misused for terrorism financing.

18. The inherent vulnerability to terrorism financing rating of the accounting sector as a whole is therefore assessed as **Low**. However, accounting practices providing trust and company services have an elevated inherent vulnerability assessed as **Medium-High**.
19. Many accounting practices do not need to implement any specific measures to mitigate terrorism financing risk. To the extent there is risk, this can be mitigated by well-implemented AML controls across customer due diligence, monitoring for unusual and higher-risk activities or transactions, and suspicious activity reporting. These controls are assessed as **moderately** effective at a sector level.
20. However, accounting practices should ensure they understand their terrorism financing risks. Those most exposed are:
    - Accounting practices that provide trust and company services involving clients, activities, or transactions internationally.
    - Any accounting practice that provides services to charities or other non-profit organisations operating in, or providing humanitarian support to, conflict zones or to countries with terrorist groups.
21. The overall accounting residual sector risk rating for terrorism financing after the implementation of AML/CFT controls is assessed as **Low**.

Overall sector risk rating – Terrorism Financing

Inherent TF Vulnerability Rating	Strength of Controls Rating	Residual TF Risk Rating
Low	Moderate	Low

Proliferation financing

22. Proliferation financing is the act of raising or providing funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of weapons of mass destruction (whether nuclear, chemical, or biological). New Zealand's proliferation financing threat largely emanates from transactions or activities with links to North Korea or Iran.

23. The overall **Proliferation Financing threat** to New Zealand is assessed as **Low**. However, and while not specific to accounting practices, the NRA 2024 identifies that the misuse of New Zealand's corporate structures and legal arrangements is (along with cyber-attacks) our most significant proliferation financing risk.

24. The inherent vulnerability to proliferation financing rating of the accounting sector as a whole is therefore assessed as **Low**. However, accounting practices that provide trust and company services have an elevated inherent vulnerability assessed as **Medium-High**.
25. Many accounting practices do not need to implement any specific measures to mitigate proliferation financing risk. To the extent there is risk, this can be mitigated by well-implemented AML controls across customer due diligence, monitoring for unusual and higher-risk activities or transactions, and suspicious activity reporting. These controls are assessed as **moderately** effective at a sector level.
26. However, accounting practices should remain vigilant and aware of proliferation financing risks. Those most exposed are:
    - Accounting practices that provide trust and company services involving clients, activities, or transactions internationally. This is particularly so if involving jurisdictions with links to North Korea or Iran, or if involving North Korea or Iran themselves.
27. The overall accounting residual sector risk rating for proliferation financing after the implementation of AML/CFT controls is assessed as **Low**.

Overall sector risk rating – Proliferation Financing

Inherent PF Vulnerability Rating	Strength of Controls Rating	Residual PF Risk Rating
Low	Moderate	Low

Introduction

28. The AML/CFT Act is New Zealand's response to financial crime risk, including through imposing obligations on certain business sectors that are vulnerable to being misused for money laundering or terrorism financing.
29. Under section 131 of the AML/CFT Act, one of the functions of an AML/CFT supervisor is to assess the level of money laundering and terrorism financing risk across the sectors that it supervises. This Sector Risk Assessment (SRA 2026) has been produced as part of this function.
30. The SRA 2026 contains four parts:
    - Part 1 of the SRA 2026 considers the criminal threat environment in which accounting practices in New Zealand operate. Money laundering, terrorism financing and proliferation financing are considered in turn.
    - Part 2 assesses the accounting sector risks to money laundering. The analysis:
        - considers the size, nature and complexity of the sector and the services provided by accounting practices.
        - assesses the inherent sector vulnerability to money laundering.
        - assesses the overall strength of sector-wide AML/CFT controls implemented by accounting practices.
        - determines the overall residual risk rating of the accounting sector to money laundering.
        - Key high-risk indicators (known as "red flags") are also identified.
    - Part 3 assesses the accounting sector's vulnerability to terrorism financing and proliferation financing and determines the overall residual risk rating.
    - Part 4 considers other factors that increase or decrease risk for individual accounting practices.
    - The Appendix contains a summary of key requirements under the AML/CFT Act that an accounting practice must comply with.

Purpose of the Accounting Sector Risk Assessment

31. Accounting practices need to be aware of the ways in which criminals[3] can misuse their services to launder money or finance terrorism or proliferation. Identifying and understanding the risks is the first step towards combatting these activities.
32. The DIA has produced the SRA 2026 to:
    - Provide an updated sector-level understanding of money laundering, terrorism financing and proliferation financing risks[4] across New Zealand's accounting sector, reflecting changes in the operating and criminal threat environment since 2019.

[3] In the SRA 2026, the word 'criminal' is used to denote a person engaging in criminal activity.

[4] Requirements relating to proliferation financing (other than suspicious activity reporting) are not currently explicitly required under the AML/CFT Act. However, upcoming regulatory reforms are expected to expand the requirements of the AML/CFT Act to include proliferation financing.

- Assist accounting practices to identify, assess and understand the money laundering, terrorism financing and proliferation financing risks relevant to their sector to inform their own risk assessment.
- Promote a shared and consistent understanding of accounting practice risks across the DIA, the New Zealand Police Financial Intelligence Unit (FIU) and other agency partners, aligned with the National Risk Assessment 2024 (NRA 2024).

33. The SRA 2026 draws upon DIA's supervisory experience of accounting practices since 2018. It supersedes the Designated Non-Financial Businesses and Professions Sector Risk (DNFBP) Assessment of 2019 for accounting practices.
34. Figures cited in the SRA 2026 are based on Annual AML/CFT Reports submitted by accounting practices for the financial year 2024-2025 (unless specified otherwise). Annual reports contain self-reported data. Transaction values and other statistics in the SRA 2026 should be considered an estimate rather than exact figures for the sector.

Methodology

35. New Zealand's understanding of money laundering, terrorism financing and proliferation financing risk is informed by national, sector and entity-level risk assessments. The NRA 2024 provides a law enforcement led assessment of risk, supported by other FIU products such as typology reports. SRAs build on this national view by assessing risks at a sector level, drawing on supervisory experience, reporting entity information and international guidance.
36. Risk is assessed through the interaction of threat and vulnerability. Threat refers to the nature and scale of criminal activity relevant to the sector, including exposure to predicate offending and known typologies. Vulnerabilities are characteristics of a sector or its products and services that can be exploited by a criminal threat or may support or facilitate its activities.
37. Risk is assessed at two levels:
    - Inherent vulnerability (sometimes referred to as "inherent risk") – reflects the level of risk in the absence of AML/CFT controls.
    - Residual risk – reflects the level of risk remaining after considering the effectiveness of implementation of AML/CFT controls at a sector level.
38. The SRA 2026 utilises inherent vulnerability and residual risk ratings of "High", "Medium-High", "Medium", "Low-Medium" and "Low". "Strength of Controls" at a sector level utilises ratings of "Substantial", "Moderate" and "Partial".
39. The inherent vulnerability and residual risk ratings assessed in the SRA 2026 reflect the accounting sector **as a whole**. Not all accounting practices will have the same level of risk.

How accounting practices should use the SRA 2026

40. The SRA 2026 should be used by an accounting practice when conducting or updating its risk assessment to:
    - review and consider the criminal threat environment in which it operates (as set out in Part 1).
    - understand the vulnerabilities associated with its products and services that could be exploited for money laundering, terrorism financing and proliferation financing (as set out in Parts 2 and 3).
    - consider the other factors that will increase or decrease an accounting practice's risks (as set out in Part 4). This will enable an accounting practice to identify the risks it faces in the course of its business, and to enable it to determine the level of risk in relation to relevant AML/CFT obligations.
41. In turn, the types of clients, activities, and transactions where the risks are higher is where accounting practices must apply the most AML/CFT scrutiny. This should be clearly documented in an accounting practice's AML/CFT programme.

42. **Note**: The strength of an accounting practice's AML/CFT controls will then impact on its residual level of risk. Accounting practices may consider it useful and decide to incorporate an assessment of residual risk into their risk assessment. However, this is not a requirement of the AML/CFT Act and not mandatory. For further information on risk assessment obligations, please refer to the DIA's **ML/TF Risk Assessment Guidance**.

Part 1: Criminal Threat Environment

43. Accounting practices are often referred to as **gatekeepers**. This is because they provide specialist services that facilitate the entry and movement of funds in the financial system. These services can be misused by criminals.

Money Laundering

44. Money laundering[5] is the process that criminals use to “clean” the money or assets generated from criminal activity. In the context of the relationship to money laundering, these crimes are known as “predicate offences”. Money laundering involves converting the money or assets from one form to another, disguising the ownership of it, or otherwise taking steps to conceal its origin.
45. The sectors identified in the NRA 2024 as most vulnerable to money laundering are banks, money remitters, and virtual asset service providers. However, **accounting practices** are a sector also identified as being misused by criminals. Other sectors identified to be misused by criminals are real estate agents, trust and company service providers, law and conveyancing firms, dealers in high value goods and casinos.
46. In addition, it is important to note that the money laundering threat faced by an accounting practice may be:
    - **Direct** - the accounting practice is directly responsible for transacting the proceeds of crime (including involving funds transacted through a trust account or other bank account on which it has authority).
    - **Indirect** - the accounting practice’s services (for example trust and company services) are enablers of money laundering. These services allow the proceeds of crime to be converted, disguised or concealed, even though the accounting practice does not directly conduct any financial transactions.
    - In some circumstances, an accounting practice’s risk is both **direct** and **indirect**.

[5] Money laundering is an offence under s 243 of the Crimes Act 1961.

47. Money laundering, in so far as it relates to money, is often conceived to be a three-step process: **placement**, **layering** and **integration**:

Type	Summary
Placement	This involves introducing criminally derived funds into the financial system. For some predicate offences, including drug offending, the criminally derived funds are likely held and placed into the financial system in cash. For other offences, such as fraud or tax evasion, placement may occur electronically. Placement may occur through large transactions deposited directly into an account, or by breaking up large amounts into smaller sums. It could be deposited by an account holder or a third party, in cash or through electronic payments. It may occur via other mechanisms such as purchasing shares or loading credit cards.
Layering	Funds are moved or converted into other property to distance or disguise them from the criminal derived source. This may involve breaking the funds up or moving them around in a series of transactions, such as between bank accounts. Funds might be channelled through the purchase and sale of investment instruments or high-value goods or be wired through various accounts across the world. In some instances, a launderer might disguise the transfers as payments for goods or services, giving them an appearance of legitimacy.
Integration	The funds then emerge from the financial system in a form that appears legitimate. This is the ultimate objective of laundering, the funds can then be used for further criminal activity, for legitimate business or enjoyed as property, such as real estate or high-value assets.

48. While understanding this three-step process is useful, it is also important to note that:
    - Money laundering takes many forms and has many typologies, some simple and others complex and they are constantly evolving.
    - For the offence of money laundering to occur, it does not require all three steps to be completed. One is often enough.
    - The three steps are not always discrete; they can often overlap or be concurrent. Furthermore, in some circumstances (such as electronic payments made as part of frauds, scams and cyber-crimes), the placement stage of money laundering is often inherent to the predicate offending.
    - Money laundering does not just occur in relation to money; any property that is the proceeds of crime can be laundered. However, the three-step model is more relevant to money than to other property that is the proceeds of crime.

Self-laundering or through professional launderer or network

49. Money may be self-laundered (by the person who committed the predicate offence), through a close or trusted associate or through a professional money launderer or network.
50. Some money laundering networks are extremely sophisticated and operate internationally. They are able to launder larger volumes of funds through complex typologies, often involving multiple countries, including:
    - use/abuse of legal persons or legal arrangements to conceal the origin and destination of funds, while presenting legitimate business activity.
    - movement of funds through multiple financial institutions, other gatekeeper professions, businesses, and assets.
    - trade-based money laundering techniques and typologies.

Trade-based money laundering

51. Trade-based money laundering (TBML) is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins. This could involve the falsification of price, quantity and quality of goods, or the falsification of invoices or supporting shipment documents. Techniques used include:
    - Over-invoicing or under-invoicing the price of the goods or services.
    - Misstating the quality or type of good to justify value differences.
    - Issuing multiple invoices for the same transaction to justify multiple payments for the same shipment of goods or delivery of services.
    - Fictitious trading (sometimes referred to as “ghost” or “phantom” shipping), by which invoices are issued and paid but ultimately no goods are actually traded.

52. Accounting practices that manage funds and/or are involved in processing payments internationally for clients are well placed to identify and detect false or manipulated trade related invoices or other documents.

Exposure to predicate offences

53. The NRA 2024 identifies the three highest risk predicate crime threats to New Zealand as **fraud**, **drug crime,** and **transnational money laundering** from foreign predicate crimes (by which funds are laundered through New Zealand's financial system). Other notable crimes identified by the NRA 2024 are **tax non-compliance** and **property crime** (including retail crime, burglary, and vehicle theft). Accounting practices are exposed to these predicate crime threats.

Fraud

NRA 2024:

54. An estimated **$700M to $1B** is generated annually from fraud and scams. This comprises fraud against individuals, businesses, including banks, and the Government (including MSD, ACC, and Inland Revenue). This includes both general and cyber-enabled fraud, with volumes and values anticipated to rise. Cyber-fraud (including phishing, smishing, identity theft, romance and business scams and business email compromise) often operate from overseas.
55. Proceeds generated from fraud and scams, which is less likely to be cash, is typically transferred through the banking system, although use of cryptocurrency is also increasing.[6]

56. Accounting practices have limited exposure to the direct **placement** of the proceeds of fraud. More likely, an accounting practice's exposure to placement activity relating to fraud is indirect. This primarily applies to accounting practices providing trust and company services, on the basis that legal persons in particular are often used to commit fraud.
57. Accounting practices have significant exposure to potential **layering** and **integration** activity relating to the proceeds of fraud. The most direct risk relates to funds transacted through trust or other bank accounts over which the accounting practice has authority (after the proceeds of fraud are already in the financial system), including through international payments. Alternatively, accounting services, particularly trust and company services, can be used to assist conceal or disguise criminal proceeds, even in the absence of directly transacting funds.

[6] NRA 2024 at 28.

Drug crime

NRA 2024:

58. An estimated upwards of **$500M to $600M** is generated annually from drug crime. The majority of this relates to methamphetamine, followed by cannabis, cocaine, and MDMA. Proceeds generated from drug crime is typically in cash.[7]

59. Accounting practices have limited exposure to **placement** activity associated with drug crime as they do not normally deal in cash.[8] However, and similarly to fraud, accounting practices have significant exposure to **layering** and **integration** activity relating to the proceeds of drug crime. This may include funds transacted through their trust or other bank accounts over which the accounting practice has authority (after the cash has been placed into the financial system elsewhere). In addition, trust and company services and other involvement in managing client funds or assets can be used to disguise or move the proceeds of crime.

Transnational laundering of foreign predicate crimes

NRA 2024:

60. The amount of proceeds generated annually from foreign predicate crimes that is laundered through the New Zealand system (including using NZ legal persons or arrangements) is unknown. However, it is estimated to be significant. It typically involves high value transactions but with less frequency, seeking to control New Zealand assets (real estate) and/or settle trusts in New Zealand.
61. Proceeds generated from foreign predicate crimes, which have included corruption and fraud, are typically transferred through the banking system.[9]

62. Accounting practices with international clients, activities, or transactions have significant exposure to transnational laundering of foreign predicate crime. As with fraud and drug crime, the most exposure will be the **layering** or **integration** stages of money laundering, noting that activities and transactions are likely to be of large amounts or value. As with fraud and drug crime above, exposure to transnational laundering may be direct (if funds are directly transacted) or indirect (if accounting services are used to assist conceal or disguise criminal proceeds, even in the absence of directly transacting funds).

[7] NRA 2024 at 24.
[8] Large cash payments or cash deposits to a bank account are an immediate “red flag.”
[9] NRA 2024 at 24.

Tax non-compliance

NRA 2024:

63. Tax non-compliance, which is discrete from tax related fraud, relates to non-declaration of income for tax purposes. This could be unreported legitimate income or the proceeds of crime and is often transacted in cash.[10]

64. Accounting practices are unlikely to be directly associated with cash transactions related to tax non-compliance. However, an accounting practice could be misused for layering and integration the proceeds of these crimes. Legal persons or legal arrangements can also be misused for tax evasion. Across the range of activities captured by the AML/CFT Act, accounting practices are in a unique position to be able to detect and report tax non-compliance.

Relationship between tax evasion and tax fraud, and money laundering:

65. Generally, transactions that are conducted to launder the proceeds of tax evasion and tax fraud will be consistent with conventional money laundering typologies and will include transactional activity such as wire transfers to 'low tax' or 'no tax' jurisdictions; the involvement of cash in large deposits or withdrawals; or where transactions are conducted outside of a customer expected behaviour or financial profile.
66. However, there are also tax specific red flags which may provide accounting practices further opportunities to detect and deter money laundering, tax evasion and tax fraud. For further information, refer to Inland Revenue's Tax evasion, tax fraud and money laundering fact sheet.

Property crime

NRA 2024:

67. Robbery, burglary and theft of vehicles and other property occur in high volume across New Zealand. Although some of these crimes are high value, the majority derive limited proceeds for laundering compared to fraud and drug crime. Often the proceeds are self-consumed, transacted with third parties in payment for drugs, or sold for cash.[11]

68. Accounting practices are unlikely to be directly associated with stolen goods as the proceeds of crime, nor with cash obtained from selling them. However, an accounting practice could be misused for layering and integrating the proceeds of these crimes.

[10] NRA 2024 at 30.
[11] NRA 2024 at 31.

Lower threat predicate crimes

69. Lower threat predicate crimes for laundering in New Zealand are corruption and bribery, human trafficking, migrant exploitation, fisheries crime, illegal gambling, firearms trafficking, environmental crime, securities crime, child exploitation, and financially motivated murder, kidnapping, or other violence.
70. While these are serious crimes, they are assessed as occurring less frequently and/or generating lower volumes of proceeds in New Zealand, therefore presenting more limited exposure to money laundering for accounting practices. Accordingly, these offences are not assessed in detail in the SRA 2026. Note however, that the transnational laundering of foreign predicate crimes through the New Zealand system detailed above could relate to any offence.

Terrorism Financing

71. While money laundering is the process of concealing the illicit origin of proceeds of crime, terrorism financing is the process by which terrorist acts, or ongoing operations to perform terrorist acts, are funded.[12] Terrorists need financial support to carry out their activities and to achieve their goals.
72. Terrorism financing covers a wide range of activity that supports terrorism. This includes providing or collecting funds or providing other material support, whether directly or indirectly.
73. In the case of money laundering, the money or assets are always the proceeds of crime, whereas in the case of terrorism financing, funds can stem from both licit and illicit sources. Therefore, the primary goal of individuals or entities involved in terrorism financing is not necessarily to conceal the source of the funds but to conceal the nature of the funded activity.

Identifying terrorism financing:

74. The characteristics of terrorism financing can make it difficult to identify. Transactions can be of low value and may appear as normal patterns of behaviour. Nevertheless, identifying and reporting suspicious behaviour and transactions remains essential for identifying a possible domestic terrorist activity. The methods used to monitor money laundering can also be used for terrorism financing, as the movement of those funds often relies on similar methods to money laundering.

75. The terrorism financing threat to New Zealand, as assessed by the NRA 2024 is **Low**. The NRA 2024 identifies three types of terrorism financing threat:
    - **Domestic terrorism** – The threat of domestic terrorism comes primarily from isolated or disaffected individuals or small groups. These persons/groups are often self-funded, so the methods of financing can be varied.

[12] Terrorism Financing is an offence under s 8 of the Terrorism Suppression Act 2002.

- **Supporting terrorism overseas** – New Zealand based individuals may become inspired to contribute or collect funds for overseas terrorist groups. This could include raising funds to travel to, or near, conflict zones to support terrorist activity.
- **Diversion of funds intended for humanitarian purposes** - Donations from New Zealand to international aid or relief charities have historically been redirected to terrorist organisations.

76. The NRA 2024 determines that the terrorism financing threat is mostly to the banking, money remittance, and virtual asset service provider sectors.
77. There is no terrorism financing threat identified specific to accounting practices, although the NRA 2024 determines there is a possibility that New Zealand companies have or will at some future time be misused for terrorism financing.

Proliferation Financing

78. Proliferation financing is the act of raising or providing funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of weapons of mass destruction (whether nuclear, chemical, or biological). This includes financing their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes).
79. New Zealand's proliferation financing threat largely emanates from the Democratic People's Republic of Korea (North Korea or the DPRK) and Iran. Exposure to this threat also lies in transactions or activities involving intermediary jurisdictions with links to North Korea and Iran.
80. The proliferation financing threat to New Zealand is assessed as **Low**. This assessment includes the likelihood of potential breaches, non-implementation, and the evasion of targeted financial sanctions against designated persons or entities.
81. Notwithstanding the Low threat rating, the NRA 2024 recognises the increasing prevalence of cyber-crimes, potentially emanating from North Korea and Iran, targeting New Zealand. Criminals from these countries are known to conduct a range of crimes, including complex cyber-enabled frauds, to derive income.
82. While there is no proliferation financing threat identified specific to the accounting sector, the NRA 2024 determines that cyber-attacks, and the misuse of legal person and legal arrangement structures, are New Zealand's most significant vulnerabilities to proliferation financing.[13]

[13] The NRA 2024 also determines that improved understanding of proliferation financing risk is required by reporting entities.

Part 2: Sector risk - money laundering

83. Accounting practices in New Zealand offer a range of services, some of which are attractive to or needed by criminals to launder the proceeds of crime. The services most vulnerable to money laundering are trust and company services and trust accounts. Insolvency practice and other managing of client funds, accounts, securities, or assets, may also be exploited.

Nature, size, and complexity of sector

84. There are 1,444 known accounting practices[14] that are reporting entities distributed across New Zealand. These range from sole practitioners through to large nation-wide practices, including the "Big Four" that operate as part of global groups. Most accounting practices in the sector are small businesses. Of the 1,444 known accounting practices, 100 of them report that their only captured activity is "tax transfers" that are subject to a partial exemption from the AML/CFT Act (refer part 2.6 below).
85. In New Zealand "accountant" is not a protected title, meaning there are no restrictions on a person using the term to describe their occupation. However, only properly qualified and accredited professionals are allowed to call themselves and/or operate as a "chartered accountant", an "associate chartered accountant" (which is a legacy designation) or an "accounting technician". In addition, "insolvency practitioners" are considered part of the accounting sector for the purposes of the AML/CFT Act. An insolvency practitioner must be licensed.
86. For other types of accounting practices in the sector, there are lesser, or in some cases no, requirements to be able to operate nor ongoing professional obligations.
87. The accounting sector is therefore disparate in nature, with varying levels of regulatory oversight, professional standards and types of practitioners. Broadly, the sector comprises chartered accountants, other qualified statutory accountants, insolvency practitioners, bookkeepers, tax agents and PAYE intermediaries. However, there are other practitioners that do not clearly fall into these categories but still conduct activities subject to the AML/CFT Act.
88. Adding further complexity to the sector, only certain activities conducted by accountants are subject to the requirements of the AML/CFT Act. These are:
    - trust and company services (including forming legal persons or legal arrangements, acting as a nominee director or nominee shareholder or trustee);
    - managing client funds, accounts, securities, or other assets;
    - providing a registered office or other correspondence address (unless this is solely ancillary to an activity not subject to the AML/CFT Act); and

[14] As of 9 June 2026.

- carrying out, preparing to carry out, or giving instructions on behalf of a customer to another person for various specified activities or transactions.[15]

89. Some accounting practices may only provide a single captured activity, whereas others might provide multiple activities subject to the AML/CFT Act. There are also some activities conducted by accounting practices captured by the AML/CFT Act but subject to a partial exemption from AML/CFT obligations.
90. Overall, due to these characteristics of the accounting sector, there are challenges for DIA in identifying all accounting practices that are reporting entities under the AML/CFT Act. It is likely that not all are known to the DIA.

Department's view:

91. The Department considers that the following accounting services are **not** captured by the AML/CFT Act:
    - Tax accounting services (for example preparing and filing tax returns, as well as any associated instructions to Inland Revenue for payment of a refund).
    - Assurance and audit.
    - Management accounting or consulting.
    - Providing a registered office or other address service alongside other accounting services that are not captured by the AML/CFT Act.
    - Providing general advice prior to being instructed in relation to an activity subject to the AML/CFT Act.

Chartered accountants and other qualified statutory accountants

92. Chartered accountants and other qualified statutory accountants[16] may provide a range of services. This includes tax services, financial and tax planning, audit and assurance, valuation, insolvency and corporate finance, as well as management accounting and consulting. Only a chartered accountant or other qualified statutory accountant can ordinarily undertake certain specific activities.
93. Chartered accountants must meet fit and proper requirements set by Chartered Accountants Australia and New Zealand (CA ANZ).[17] Other qualified statutory accountants must also meet fit and proper requirements.

[15] For full list of captured activities, refer to the definition of 'designated non-financial business or profession' in s 5 of the AML/CFT Act.

[16] Qualified statutory accountants are defined in the Financial Reporting Act 2013 to include a chartered accountant (within the meaning of the NZICA Act 1996), a member of another accredited body that holds the full professional designation of that body, or certain members of religious societies or orders recognised as qualified statutory accountants.

[17] Note that the New Zealand Institute of Chartered Accountants is the statutory regulator for chartered accountants resident in or practising in New Zealand.

94. These fit and proper requirements are also assessed when applying for a certificate of public practice to be able to provide accounting services to the public. All chartered accountants and other qualified statutory accountants are also bound by a code of ethics. This means they are held to professional and ethical standards, with an accompanying disciplinary process for breaches.
95. The codes of ethics require professional accountants to operate with integrity, objectivity, professional competence and due care, confidentiality and professional behaviour. This includes adhering to all applicable laws and regulations, such as the AML/CFT Act. There are also specific professional standards and responsibilities when holding, receiving or otherwise dealing with client monies on behalf of clients, including operation of client bank accounts or a trust account.
96. There are approximately 26,000 full members of CA ANZ in New Zealand. However, only a proportion of these are in public practice and part of accounting practices providing services subject to the AML/CFT Act, such that the accounting practice is a reporting entity.[18]

Auditors:

97. Auditing is not an activity captured by the AML/CFT Act. However, any auditor (for a financial or AML/CFT audit) may report suspicious activity to the FIU identified during their work.[19] AML/CFT auditors are able to register with the goAML system for this purpose.

Insolvency practitioners

98. A licensed insolvency practitioner may act as the liquidator, receiver or administrator of an insolvent entity, or a trustee of an individual's creditor proposal.
99. Both the licensing and ongoing professional regulation of insolvency practitioners is conducted by the New Zealand Institute of Chartered Accountants (NZICA). Insolvency practitioners, many of whom are also chartered accountants, are subject to the same code of ethics and disciplinary processes set out above. Insolvency practitioners who do not hold a certificate of public practice must also be members of a recognised body, such as the Restructuring Insolvency & Turnaround Association of New Zealand (RITANZ).
100. There are approximately 130 licensed insolvency practitioners in New Zealand.[20]

[18] Note when a chartered accountant or other qualified statutory accountant is employed by or the owner a company in public practice providing accounting services, or a partner in a partnership, it is the company or partnership that is the reporting entity.
[19] Section 43 of the AML/CFT Act.
[20] When a licensed insolvency practitioner is employed by or the owner of a company providing insolvency services, or a partner in a partnership, it is the company or partnership that is the reporting entity.

Bookkeepers

101. Most bookkeepers in New Zealand are sole traders or small businesses. Many bookkeepers operate from home offices, in cloud-based environments with remote service delivery.
102. There are no licensing or fitness and propriety requirements to operate as a bookkeeper nor a requirement to belong to a professional body. There is also no requirement to register as a bookkeeper with Inland Revenue unless certain eligibility criteria are met.
103. There is no requirement to belong to a professional body. However, there are two membership bodies for bookkeepers - the Institute of Certified NZ Bookkeepers (ICNZB) (with over 300 members) and the New Zealand Qualified Bookkeepers Association (NZQBA) (with approximately 350 members).
104. Both membership bodies have professional codes of conduct requiring professionalism, integrity and compliance with all laws. This includes complying with the AML/CFT Act. There are disciplinary processes for breaches of the code of conduct, which can lead to warnings, suspensions or termination of membership.
105. Bookkeepers that are members of ICNZB or NZQBA are also able to register as a bookkeeper with Inland Revenue. This enables them to represent a client for GST and PAYE.
106. While a significant number of bookkeepers in New Zealand are members of either ICNZB or NZQBA, there are many that are not. The number of bookkeepers that are accounting practices but not members of ICNZB or NZQBA is unknown.

Tax agents

107. Tax agents prepare annual income tax returns for their clients and act for them with Inland Revenue. Additionally, tax agents may provide tax advisory, bookkeeping and PAYE services.
108. The membership body for tax agents is the Accountants and Tax Agents Institute of NZ (ATAINZ), which has over 470 members. Members must have professional qualifications and submit a criminal history check as part of their application. ATAINZ members are subject to a code of ethics requiring integrity, trust and confidence, standards of service and professional conduct. This includes adhering to all applicable laws and regulations, such as the AML/CFT Act. There are also specific responsibilities if holding funds for clients, which must be in a trust account. There is also a disciplinary process for breaches of the code of ethics.
109. Based on these professional obligations, ATAINZ members are eligible to register with Inland Revenue as tax agents. Tax agent status can be withdrawn by Inland Revenue on character grounds, including criminal offending, dishonest behaviour, breaching client confidentiality or serious or repeated performance issues.

110. The primary function of tax agents, being the preparation of tax returns, is not subject to the AML/CFT Act. Consequently, a tax agent is only subject to the AML/CFT Act to the extent is carries out other captured activities.

PAYE intermediaries

111. PAYE intermediaries manage employer obligations, including paying employees and meeting record-filing requirements with Inland Revenue. To qualify as a PAYE intermediary, they must meet strict integrity and compliance standards and be accredited by Inland Revenue. There are 17 current PAYE intermediaries registered with Inland Revenue.[21]

Composition of accounting practices that are reporting entities in New Zealand:

- 1% of accounting practices are large (with over 100 employees).
- 11% of accounting practices are medium sized (with 20 – 100 employees).
- 88% of accounting practices are small (with less than 20 employees).
- Accounting practices are well distributed across New Zealand, with 38% based in Auckland, 39% throughout the rest of the North Island and 23% in the South Island.
- Only 42 accounting practices have three or more office locations. Most have only one office.
- Less than 1% of accounting practices report a parent accounting practice in another country. However, some accounting practices in New Zealand are partly or fully integrated into large international accounting practices.

Volume of activities and transactions

112. Based on annual AML/CFT report data for 2024-2025, accounting practices report managing client funds, accounts, securities, or other assets with a total value of up to **$3.85 billion** for their clients. This includes international funds transfers with a total value of up to $916 million sent to, or received from, other countries on behalf of clients.[22]

Transactions through bank accounts:

113. The DIA has identified some accounting practices assume their clients' financial transactions are legitimate because they pass through the banking system. This is not accurate. Accounting practices have a unique view of their clients, their activities and transactions. This provides opportunity to detect criminal activity that might not be visible to banks or other reporting entities that interact with the same client.

[21] List of PAYE intermediaries.
[22] Based on responses to questions 7.4 and 7.10 of Annual Report.

114. Only 15% of accounting practices report accepting cash, with the percentage of their business involving cash averaging just 0.4%.[23]

Vulnerability of accounting services to money laundering

115. A vulnerability is a characteristic of a service that can be exploited by a criminal threat or may support or facilitate its activities.
116. The vulnerability rating (i.e. the level of inherent money laundering risk) of the different services provided by accounting practices to money laundering are set out below.

Services	ML Vulnerability Rating
1. Trust and company services	**Medium-High**

The trust and company services captured by the AML/CFT Act are:

(i) *acting as a formation agent of legal persons or legal arrangements:*
(ii) *acting as, or arranging for a person to act as, a nominee director or nominee shareholder or trustee in relation to legal persons or legal arrangements:*

117. **Note:** Acting as a nominee director or trustee in relation to legal persons or legal arrangement often also includes:
(iii) *providing a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal person or arrangement, unless the office or address is provided solely as an ancillary service to the provision of other services not subject to the AML/CFT Act.*
(iv) *managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.*[24]

[23] Based on responses to question 7.9 of Annual Report.
[24] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".

Key Statistics - Based on annual AML/CFT reporting from accounting practices:

- 64% of accounting practices form legal persons or legal arrangements.
- 35% of accounting practices act as, or arrange for a person to act as, a nominee director, a nominee shareholder, or trustee.
- 29% of accounting practices both form legal persons or legal arrangements and act, or arrange for a person to act as, nominee directors, nominee shareholders or trustees.

Of the accounting practices that provide these trust and company services, 23% report having one or more customers based overseas and 14% report using overseas intermediaries or agents to deliver their services.[25]

118. For most of the accounting practices that provide trust and company services, this is alongside other accounting services, which may or may not be captured by the AML/CFT Act.
119. Integral to providing trust and company services, many accounting practices will also manage funds, accounts, securities, or other assets (in the capacity as nominee or trustee) of the legal person or legal arrangement. This includes as part of estate planning, asset protection, tax planning and wealth management activities.

Money laundering through trust and company services

120. The NRA 2024 identifies that New Zealand legal persons and legal arrangements have been misused by both domestic and foreign criminals.
121. Most common is to both commit and launder the proceeds of predicate offences such as fraud and tax evasion, including transnationally. While legal persons or legal arrangements are not likely to be used to commit drug crime, there have been instances where they have been used to launder its proceeds.
122. Setting up and using legal persons or legal arrangements for money laundering or to commit other crimes is attractive to criminals for various reasons:
    - legal persons and legal arrangements can be used to conceal or obscure beneficial ownership or effective control of assets, activities, and transactions. This creates distance between criminals and their crimes, which frustrates detection and investigation by law enforcement agencies.
    - law firms, accountants, other professionals, family members, associates, or other persons (for a fee) can be engaged to create this distance. This includes setting up and acting as a nominee for a legal person or as a trustee of a legal arrangement, including opening bank accounts and managing funds or other assets.

[25] Based on responses to questions 7.1, 7.2, 8,2 and 8.3 of Annual Report.

- if lawyers, accountants or other professionals act for legal persons or legal arrangements, this creates a perception of respectability and legitimacy to activities and transactions.
- legal persons and legal arrangements often have larger and more frequent transactions, providing opportunities to transact in large amounts or hide criminal proceeds within legitimate business activity. Or alternatively, entirely fake businesses, such as consulting, investment or import/export, may be established.
- complex legal structures, particularly when spanning multiple jurisdictions and/or involving gatekeepers, make it particularly difficult for beneficial ownership to be identified by reporting entities and law enforcement agencies alike.
- if the proceeds of crime are detected, investigation and confiscation proceedings become harder when ownership and control of assets are held through legal structures.

Characteristics of trust and company services that can be exploited:

- Complex and/or opaque ownership structures, combined with the lack of a beneficial ownership register for legal persons or legal arrangements in New Zealand increases the risk of these structures being exploited by a criminal seeking to hide ownership or control of a legal person or legal arrangement.
- New Zealand's trust and company services landscape is also complex, with many thousands of nominee or trustee companies incorporated and used by accounting practices and other professionals to deliver their services. The use of other gatekeepers, intermediaries and agents is also common, including internationally, which adds further complexity to the sector. Alongside New Zealand's open business environment, the ease and low cost of formation of legal persons and legal arrangements, provides opportunity for misuse of legal structures without detection.
- Furthermore, New Zealand legal persons and legal arrangements are particularly attractive to overseas based criminals because of our reputation of being regulated, a stable economy and trustworthy financial system. This gives structures incorporated or established here a veneer of legitimacy.
- Shell companies (with no liabilities or assets), including "shelf" companies that may have been established years ago, are not illegal and commonly available for purchase. These can also be used for illegal purposes.

Trusts

123. The misuse of trusts for money laundering is a global issue. Once funds or assets are held in a trust, there is an appearance of distance from the settlor, when in reality the settlor may maintain a level of control. Furthermore, with no central registry of trusts, there is an immediate barrier to visibility of financial activity and asset ownership.[26]
124. While the inherent characteristics of trusts makes them attractive to criminals, not all trusts have the same level of risk. Risks and instances of misuse, particularly of high value, are higher when the trust is part of a wider corporate structure, including with companies, limited partnerships, or other trusts. This provides opportunity for criminally derived funds or assets to be introduced or transferred, under the guise of legitimate activity. For example, through loans made or paid back in criminal proceeds, or entirely fake businesses. Alternatively, through fake non-profit organisations or charities that channel funds under the guise of philanthropy.
125. The involvement of other gatekeepers, as intermediaries or agents, particularly internationally, compounds the level of risk.

Lower risk trusts:

126. The risks associated with a trust will usually be lower when there is less complexity. This includes simple structures, with the settlor and enduring and identified beneficiaries, all in New Zealand and a trust that is non-income generating. Commonly, this will include a simple family trust, for example holding a family home, for which there is a mortgage being paid off incrementally over a long time period.
127. Also of lower risk are Māori land trusts. These legal arrangements differ from other trusts in that they are established by an order from the Māori Land Court rather than being formed by settlors. They are difficult to establish and Te Ture Whenua Māori Act 1993 establishes a regime to minimise the risk of abuse for criminal purposes. Community involvement and oversight make the risk of abuse of Māori land trusts for money laundering or other criminal activity less likely.

Foreign trusts

128. New Zealand foreign trusts are trusts that are established by a non-resident settlor and have a trustee resident in New Zealand. If the trust does not derive income in New Zealand or distribute income to New Zealand resident beneficiaries, there is an exemption from New Zealand tax. Foreign trusts are therefore attractive to foreign investors, including those of high net worth.

[26] Note that income-generating trusts are required to file tax returns where information on trustees is provided and, in case of income distributions to beneficiaries, details of beneficiaries.

129. Following the Panama Papers in 2016, a government inquiry found that the foreign trust disclosure rules were insufficient. This led to the creation of the Foreign Trust Registry, held by Inland Revenue, requiring information on settlements, beneficiaries and distributions and annual reports. [27]
130. From a peak of nearly 12,000 foreign trusts in 2016, there are only 2,066 foreign trusts effective as of 1 October 2025. While the international nature of foreign trusts, and often high value of assets involved, necessitates ongoing vigilance, their level of inherent vulnerability to money laundering is assessed to have reduced significantly.

Limited partnerships

131. Limited partnerships have two types of partners: limited and general partners, with different functions and legal liability:
    - Limited partner - In New Zealand, a limited partner must not take part in the management of the limited partnership. Additionally, their liability is only to the extent of the financial contributions made.
    - General partner – Unlike a limited partner, a general partner is responsible for the management of the limited partnership and may, but does not have to, make a capital contribution to the limited partnership.
132. The relationship between general partners and limited partners can vary and will depend upon the terms of the governing document between them. The general partner may also be a nominee general partner. In addition, and importantly, a limited partner's details are not publicly available on the Limited Partnerships Register. Only the general partners' details are listed. This characteristic of limited partnerships may increase their attractiveness to criminals.

Limited liability companies

133. The vast majority of legal persons in New Zealand are limited liability companies. These companies are easy to form and can quickly access financial services including banking facilities and other types of financial products.
134. There are no prohibitions on a New Zealand limited liability company having a nominee director or nominee shareholder. The nominee's legal liability is the same as it is for any director or shareholder, regardless of whether the nominee is acting for an underlying person (i.e. the beneficial owner).
135. While there are legitimate reasons for a having a nominee director or shareholder (for example privacy, safety, and/or commercial confidentiality), criminals can exploit these arrangements. Importantly in relation to the vulnerability of nominee arrangements to money laundering, only the nominee director or nominee shareholder's details are on the publicly available Companies Register. Any underlying beneficial owner remains hidden.

[27] The New Zealand Police and DIA can access this register.

Red flags for trust and company services include:

- Creation of complicated ownership structures, including cross-border structures, which are unusual and/or when there is no legitimate or economic reason.
- Requests to form or act for a legal person or legal arrangement without seeking advice on the appropriateness of the structure or related matters.
- Use of an intermediary without good reason.
- Frequently changing legal structures and/or managers of legal persons, including use of family members without appropriate business experience.
- Payments from unrelated or unknown third parties without legitimate explanation.
- Involvement of pre-existing entity in business activity without adequate explanation (indicating wanting to have a transaction or activity chain more well-established that it is).
- Loan arrangements involving related entities are paid back in larger amounts and/or before the set term of the loan.
- Unusual beneficiary (of a trust) structures, including use of offshore entities or nominee beneficiaries.
- Any involvement of a company with shares in bearer form.[28]

Services	ML Vulnerability Rating
2. Managing client funds – trust accounts	**Medium-High**

Operating and transacting funds for a client through a trust account is captured under the AML/CFT Act as:

> *(iv) managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.*[29]

[28] A New Zealand incorporated company is prohibited from having shares in bearer form (s 51 of the Companies Act 1993).
[29] AML/CFT Act, s 5(1) definition of “designated non-financial business or profession”.

136. Only a small proportion of accounting practices operate a trust account[30] to hold funds for clients. The value and volume of transactions through accounting practice trust accounts is significantly less compared to law and conveyancing firms. Furthermore, it typically does not relate to real estate which is an asset of choice for the proceeds of crime.
137. Nonetheless, for those accounting practices that do have trust accounts, this is attractive to criminals and provides opportunity for criminal proceeds to be inserted. This may include illicit funds already in the financial system, but for which previous steps in the laundering process involved different financial institutions or gatekeepers. From there:
    a) Once funds are in trust account, the origin of the money is obscured, and the payer of any subsequent payment shows as the accounting practice (rather than the client);
    b) Payments from an accounting practice's trust account appear legitimate and trustworthy; and
    c) If the proceeds of crime are detected, investigation and tracking the movement of funds may require extra steps when funds have routed through an accounting practice's trust account.

Services	ML Vulnerability Rating
3. Insolvency practice	**Medium**

Insolvency services are captured under the AML/CFT Act as:

> *(iv) managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.*
>
> *(vi) carrying out, preparing to carry out, or giving instructions on behalf of a customer to another person for:*
>
> > *(E) a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement.*[31]

[30] A trust account "means an account or other arrangement for the purpose of holding funds that belong to more than 1 client of a reporting entity". Approximately 18% of accounting practices that are chartered accountancy practices operate a trust account. The proportion of other types of accounting practice that hold trust accounts is not known.

[31] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".

138. Effective 31 July 2023, new regulations clarified some obligations and partially exempt insolvency practitioners from other requirements of the AML/CFT Act in relation to liquidations. These amendments accord with a recommendation from the Ministry of Justice's AML/CFT Statutory Review, which was completed in 2022.
139. The new regulations recognise the unique circumstances in which liquidators operate and align with the money laundering and terrorism financing risks faced in this sector. There are regulations applicable to both court and non-court-appointed liquidations relating to both companies and limited partnerships. For further information, refer to the DIA's **Guidance: New AML/CFT regulations for liquidators**.
140. These regulations/partial exemptions do not apply to insolvency practitioners that act as a receiver, administrator or deed administrator of a company in voluntary administration or a trustee or provisional trustee of personal insolvency creditor proposals.

Money laundering through insolvency practices

141. The nature of insolvency practice means that the money laundering risks manifest differently to other accounting services subject to requirements of the AML/CFT Act.
142. At the point of liquidation, receivership or administration, the insolvency practitioner assumes control of the insolvent entity, and/or its assets, depending on the nature of the appointment. This means the direct money laundering risk arises from criminals seeking to exploit both the insolvency process (and the insolvency practitioner).
143. Criminals may seek to exploit an insolvency process so that audit trails are obscured and proceeds of crime are presented as legitimate realisations, creditor payments or asset distributions. This could involve collusion between persons associated with the insolvent entity and its creditor(s). This could also be accompanied by asset stripping or concealment of assets in the period prior to or during insolvency.
144. Additionally, there may have been underlying criminal activity associated with the insolvent entity. This may in some cases have been historical. An insolvency practitioner is well placed to identify, investigate and report suspicious activity, including activity occurring prior to the appointment, whether legal transactions or attempts to hide illicit funds among legitimate ones.

Red flags for insolvency practice include:

- Complex or opaque ownership structures, especially when inconsistent with the company profile or when nominee or trusts are involved.
- Large or unusual transfers or payments made by the company shortly before the insolvency process, including to unrelated third parties.
- Attempts to conceal assets through transfers to related parties, swap of properties, or undervaluation of assets.
- Lack of or sudden changes in accounting records or missing or inconsistent documentation.
- Sudden moves to insolvency without typical warnings signs, or unusual creditor activity.
- Requests inconsistent with normal insolvency processes, including that funds or assets be distributed in favour of certain interests or creditors.
- Involvement of persons with negative media/reputation, or from high-risk jurisdictions, or other customer risk signs.

Services	ML Vulnerability Rating
4. Other managing of client funds, accounts, securities or assets	**Medium**

Other managing of client funds, accounts, securities, or assets, by accounting practice is captured under the AML/CFT Act as:

> (iv) *managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.*[32]

Key statistics: Based on annual AML/CFT reporting from accounting practices:

- 28% of accounting practices handle the receipt or transmission of client money.
- 38% of accounting practices managing client bank accounts.[33]

[32] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".
[33] Based on responses to questions 9.3 and 9.4 of Annual Report.

Department's view:

145. The DIA considers that DNFBP activity (iv) "managing client funds, accounts, securities, or other assets" is not restricted to circumstances in which the accounting practice has direct or discretionary control. Rather, it applies in any situation where the accounting practice:
    - has a degree of control over the flow of a client's funds; and/or
    - has authority over a client's bank or other type of account(s), securities, or other assets.[34]
146. The DIA therefore considers DNFBP activity (iv) arises across various types of accounting services, in circumstances when an accounting practice carries out any of the following:
    - having full discretionary authority over a client's funds, account, securities, or other assets, including making discretionary investments on behalf of the client.
    - being an authorised signatory over a client's bank account, for example to make tax payments.
    - being an authorised signatory over a client's bank account as part of a bookkeeping service.
    - acting for a client as a signatory or otherwise as authorised person in relation to a client's financial investments or assets.
    - as part of a trust and company service (see part 2.1 above), receiving, holding or transacting client funds in or from a trust account (see part 2.2 above), for insolvency practice (see part 2.3 above), conducting tax transfers in the Inland Revenue system (see part 2.6 below), or as a PAYE intermediary (see part 2.7 below).

Money laundering through management of funds, accounts, securities, or other assets

147. It is common for an accounting practice to have authority over, or other management of, a client's funds, accounts, securities, or other assets.
148. This occurs as part of providing trust and company services, including estate planning, asset protection, tax planning, wealth management, or other involvement in financial or business activities for a client. This includes when an accountant acts in the capacity of a trustee over assets transferred into a trust. When provided as part of trust and company services, there is the potential for misuse to create distance between ownership and control of funds or assets, such that underlying parties can be hidden. In these circumstances, the **Medium-High** vulnerability rating of trust and company services applies.

[34] Note: the only exception to this relates to funds of the client that are fees paid in advance (for example as a retainer) for the service the accounting firm will provide to this client. This is excluded from DNFBP (iv).

149. In other circumstances, the management of client funds, accounts, securities, or other assets does not occur as part of a trust or company service. In these situations, funds or assets are usually held directly in the name of the owner, with the accountant authorised to act as a representative on their behalf. This includes when a client requires ongoing assistance from an accounting practice in their financial affairs, including as an authorised signatory on a bank account, for other business activity or in relation to investments.
150. The level of vulnerability will vary depending on the services being provided. In any situation where the accounting practice's services enable underlying parties to be concealed or obscured, the vulnerability is higher.
151. Conversely, in situations where an accounting practice acts as an authorised signatory (for example on a bank account or other investment) the ability to conceal or disguise underlying ownership or control of funds or assets is harder. That said, the involvement of an accounting practice still provides an impression of respectability and legitimacy to financial transactions, which may not be the case.

Red flags for other managing of client funds, accounts, securities, or assets include:

- Client directs transactions or activities for no reasonable economic benefit.
- Client instructs and authorises an accounting practice to act for financial transactions in situations when there is no apparent or visible reason for needing to do so.
- Customer terminates relationship with accounting practice quickly and unexpectedly.
- Funds received are not expected or more than expected, with subsequent directions for their use or payment.
- Transactions involve third parties without legitimate explanation.
- Activities and transactions involve values inconsistent with the socioeconomic profile of the client.
- Activities and transactions involve high-risk countries, or other countries where there is no apparent connection to the customer.
- Significant changes to instructions and parties to those instructions after initial engagement.
- Complex or opaque (potentially layered or cross-border) ownership structures with no clear commercial rationale.
- Transactions involving accounts of another gatekeeper in circumstances that are not expected.
- Involvement of offshore trusts, shell companies, or entities registered in high-risk jurisdictions.
- Involvement or acquisition of dormant or cash-heavy businesses.
- Unexplained or unusually high valuations.
- Quick turnover of ownership of assets or business.
- An absence of documentation to support the client's stated reason for engaging the accounting practice, their previous transactions, or business activities.
- Client's documents not in expected formats, and/or appear altered or inconsistent.

Services	ML Vulnerability Rating
5. Bookkeeping	**Low-Medium**

Depending on the nature of the bookkeeping service, this may be captured under the AML/CFT Act as:

(iv) managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.

In some circumstances, a bookkeeper may also be captured for:

(vi) carrying out, preparing to carry out, or giving instructions on behalf of a customer to another person for:

(E) a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement.[35]

152. A bookkeeping service may include any of the following:
    - bank reconciliations for clients or payment schedules for supplier invoices.
    - accounts payable and receivable.
    - payroll.
    - GST support.
    - management reporting.
153. A bookkeeper typically provides services to small-medium sized businesses that are local or domestically focussed. Both the bookkeeper and their clients may be within a particular urban centre, town or region. There is limited exposure to international transactions, to complex ownership structures, or to situations where underlying parties to activities or transactions are concealed.
154. A bookkeeper's money laundering risk is primarily **indirect**. The main area of money laundering vulnerability is that the client could provide false or manipulated records, including invoices, receipts or other financial information or documents. By engaging a bookkeeper to provide services relating to this information or documents, underlying criminal activity could be masked, furthered, or given false legitimacy. The involvement of a bookkeeper as an intermediary also frustrates detection or investigation by law enforcement agencies.

[35] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".

155. As part of their service, a bookkeeper may also have authority over a client's Inland Revenue account. Additionally, a bookkeeper may be a signatory and authorised to make payments from a client's bank account. In these situations, or in any other circumstances were a bookkeeper to receive, hold or pay funds for a client, the money laundering risk is also **direct**.

Bookkeepers' visibility of clients:

156. Bookkeepers may have ongoing, sometimes daily, involvement in their client's financial transactions. This provides a bookkeeper with unique visibility and opportunity to identify financial inconsistencies, and unusual or changing activity or transactions requiring examination. For example, cash payments into the client's bank account or large transactions that are not consistent with its business profile.

157. Combined with often local business knowledge, bookkeepers are therefore well placed to detect atypical records or engagements that may indicate criminal misuse of their services.

Red flags for bookkeeping:

- Large payments into a bank account by cash deposit.
- Unexplained or late changes in payment arrangements.
- Client receives or directs payments that are unusual or with no legitimate or economic reason.
- Client instructs a bookkeeper in situations when there is no apparent or visible reason for needing to do so.
- Activities and transactions involve values inconsistent with the socioeconomic profile of the client.
- Cash intensive business (or links to cash intensive business).
- Client's records are not in expected format and/or appear altered or inconsistent.

Services	ML Vulnerability Rating
6. Tax transfers	**Low**

Conducting tax transfers within Inland Revenue system is captured as one or both of the following:

(iv) managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.

(vi) carrying out, preparing to carry out, or giving instructions on behalf of a customer to another person for:

(E) a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement.[36]

158. A tax transfer involves the transfer of excess tax within the Inland Revenue system to another tax period, to another tax type of the taxpayer or to another taxpayer. An accounting practice may conduct a tax transfer when it has authority to act on a client's Inland Revenue account.
159. While conducting tax transfers is a captured activity under the AML/CFT Act, accounting practices have a partial exemption from AML/CFT obligations in respect of **most types** of tax transfer.
160. This reflects that most types of tax transfer are assessed to present a low money laundering or terrorism financing risk. The only requirements that apply are to report any suspicious activity and keep associated records, as well as to conduct enhanced customer due diligence if a customer seeks to conduct a complex, unusually large tax transfer or unusual pattern of tax transfers that have no apparent economic or lawful purpose. Or when a reporting entity considers that the level of risk involved is such that enhanced due diligence should apply.
161. There is one type of tax transfer that is **not** subject to the partial exemption, this is tax transfers to **unrelated parties**. If an accounting practice conducts tax transfers to unrelated parties, full AML/CFT obligations apply. These types of tax transfer pose considerable money laundering vulnerability.
162. For further information relating to the class exemption, refer to the DIA's **Tax Transfers Class Exemption Guidance**.

[36] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".

163. **Note:** For some accounting practices, tax transfers are the only activity they carry out that is captured by the AML/CFT Act. By ensuring that tax transfers to unrelated parties are **never** undertaken, an accounting practice will minimise the application of the AML/CFT Act to its business.
164. Note that any accounting practice for whom the only captured activity is tax transfers (and who decides to never conduct transfers to unrelated parties) is still required to register for goAML with the FIU to be able to report suspicious activity. An accounting practice to whom this applies should also notify the DIA of this decision.

Services	ML Vulnerability Rating
7. PAYE intermediary	**Low**

Acting as a PAYE Intermediary is captured as one or both of the following:

(iv) managing client funds (other than sums paid as fees for professional services provided by the business or profession), accounts, securities, or other assets.

(vi) carrying out, preparing to carry out, or giving instructions on behalf of a customer to another person for:

(E) a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement.[37]

165. PAYE intermediaries calculate payroll information, deduct taxes and pay Inland Revenue directly from a trust account set up for this purpose.
166. PAYE intermediaries have a class partial exemption from the AML/CFT Act,[38] reflecting that their activities are assessed to present a low money laundering or terrorism financing risk. The only requirements that apply are to report any suspicious activity and keep associated records.
167. The class exemption applies to transfers between New Zealand bank accounts only. It does not apply in relation to the use of a payroll remittance card or to any other activities an accounting practice that is a PAYE intermediary conducts that is subject to the AML/CFT Act.

[37] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".
[38] Part 4 of the AML/CFT (Class Exemptions) Notice 2018.

Services	ML Vulnerability Rating
8. Providing a registered office or other address	**Low**

Providing a registered office or other address for a client is captured under the AML/CFT Act as:

> *(iii) providing a registered office or a business address, a correspondence address, or an administrative address for a company, or a partnership, or for any other legal person or arrangement, unless the office or address is provided solely as an ancillary service to the provision of other services not subject to the AML/CFT Act.*[39]

168. Provision of a registered office or other address for a client is common amongst accounting practices, with 70% of accounting practices reporting they do so.[40]
169. Using the address of an accounting practice can be attractive to a criminal as it allows them to distance themselves and their location from the transactions they are undertaking. Using an accounting practice's address also gives the appearance of legitimacy to their activities and complicates investigation by law enforcement agencies.
170. In most circumstances, accounting practices may provide a registered office, business, correspondence or administrative address in conjunction with other services subject to the AML/CFT Act. In these situations, the service is of itself assessed as being of low ML vulnerability. However, any circumstances where a registered office or other address is provided as a standalone service poses heightened risk.

Red flags for providing a registered office or other address include:

- Request for provision of a registered office or other address as a standalone service.
- Request for accounting practice to provide correspondence or administrative address when this would not be expected, for example a business that has a physical local office that is staffed.
- Individuals associated with the company (i.e. directors/shareholders) also list the same address.
- Multiple previous changes to address and/or use of "virtual office" provider.
- Contact from unknown persons seeking to locate the client.
- Advertising by the client that the accounting practice's address is its place of business.

[39] AML/CFT Act, s 5(1) definition of "designated non-financial business or profession".
[40] Based on response to question 7.3 in Annual Report.

Services	ML Vulnerability Rating
9. Other accounting services subject to the AML/CFT Act	**Low**

Accounting practices may carry out other activities that are subject to the AML/CFT Act but do not directly involve trust and company services or managing client funds, accounts, securities, or assets. This includes preparatory work or giving instructions on behalf of a customer to another person for various specified activities or transactions. In these situations, the accounting practice's money laundering risk is indirect.

171. These additional situations are subject to the AML/CFT Act due to the following DNFBP activity:
   (vi) carrying out, preparing to carry out, or giving instructions on behalf of a customer to another person for:
      (A) any conveyancing activity within the meaning of section 6 of the Lawyers and Conveyancers Act 2006) to effect a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008; or
      (B) a transaction (within the meaning of section 4(1) of the Real Estate Agents Act 2008); or
      (C) the transfer of beneficial interest in land or other real property; or
      (D) a transaction on behalf of any person in relation to the buying, transferring, or selling of a business or legal person (for example, a company) and any other legal arrangement; or
      (E) a transaction on behalf of a customer in relation to creating, operating, and managing a legal person (for example, a company) and any other legal arrangement.[41]

172. These other activities that accounting practices carry out that are captured by the AML/CFT Act are assessed less vulnerable to money laundering. Similarly to bookkeeping (refer paragraph 154 above), the primary area of money laundering vulnerability is that the client will provide the accounting practice with false or manipulated records, or other financial information or documents.

173. By engaging the accounting practice to provide services relating to this information or documents, underlying criminal activity can be masked or furthered. The involvement of the accounting practice creates false legitimacy to criminal activity and frustrates detection by law enforcement agencies.

[41] Note that DNFBP activity (vi) "*carrying out, preparing to carry out, or giving instructions*" overlaps with activity (iv) "managing client funds, accounts, securities or other assets." For the purposes of the SRA 2026, this is separately covered under part 2 section 2 above.

Supply chain risk:

174. An accounting practice may only be involved in a component part of a complex business merger, acquisition or other business activity. There may be no indication of criminality by the time the accounting practice is instructed, but the accounting practice should be alert to potential earlier criminality in the supply chain.

Red flags for other accounting activities subject to the AML/CFT Act include:

- A level of cash intensity in a business that exceeds normal levels for the industry with no clear rationale.
- High value or unexplained asset or funds transfers.
- Loan arrangements involving related entities are paid back in larger amounts and/or before the set term of the loan.
- A client making frequent changes of accounting practice with no clear rationale.
- An absence of documentation to support the client's stated reason for engaging the accounting practice, their previous transactions, or business activities.
- Clients unable or unwilling to explain the purpose or origin of funds used for tax payments, due diligence, valuations and/or mergers and acquisitions.
- Complex or opaque ownership structures with no clear commercial rationale.
- Pressure to expedite deals without proper documentation.
- Client's documents not in expected formats, and/or appear altered or inconsistent.

Overall inherent vulnerability rating for accounting practices

Inherent ML vulnerability rating for accounting practices	Medium

There is easy access to services and a wide coverage across New Zealand. Some accounting practices provide multiple gatekeeper services that can be exploited in different money laundering typologies, which compounds the level of risk.

However, of the captured activities provided by accounting practices, only trust and company services and trust accounts are rated Medium-High vulnerability.

All other captured activities provided by accounting practices are assessed as Medium or Low vulnerability and are often secondary to activities not captured by the AML/CFT Act. Notably, accounting practices also have limited involvement in real estate transactions (compared to law and conveyancing firms and real estate agents). This supports an overall inherent sector vulnerability rating of Medium.

Strength of Controls

175. Effective implementation of AML controls by all accounting practices mitigates the money laundering risk at a sector level, making it a harder target for misuse by criminals.
176. To support this, there have been various amendments or clarifications to requirements though regulations that have strengthened the AML/CFT settings for the sector. This includes:
    (i) prescribing that when acting as a nominee of a legal person or trustee of a trust, it is that legal person or legal arrangement that is the customer for the purposes of the AML/CFT Act.[42]
    (ii) prescribing that when forming a legal person or legal arrangement as an occasional activity, it is the person that instructs the formation that is the customer, but that the beneficial owner must also be identified and verified.[43]
    (iii) clarifying that a beneficial owner of a client includes a person with ultimate ownership or control of the customer, whether directly or indirectly.[44]

[42] AML/CFT (Definitions) Regulations 2011, reg 5G.
[43] Definitions Regulations, reg 5F.
[44] AML/CFT Act, s 5(1) definition of “beneficial owner”.

(iv) clarifying that ongoing customer due diligence and account monitoring is not restricted to financial transactions but also includes other accounting services that are subject to the AML/CFT Act.[45]
(v) an exemption from the wire transfer provisions of the AML/CFT Act, instead a prescribed transaction reporting obligation for international funds transfers (on behalf of a client) in or out of a trust account.[46][47]
(vi) clarifying that a corporate trustee or nominee company that is a subsidiary of, is controlled by, and delivers services on behalf of a parent accounting practice in New Zealand is exempt as a reporting entity when the parent accounting practice has established, implements and maintains an AML/CFT programme.[48] In turn, trustee or nominee companies that do not meet these conditions are reporting entities in their own right under the AML/CFT Act.

177. In addition, two new regulations prescribe requirements that all reporting entities must undertake when onboarding a new client that is a legal person or legal arrangement. This requires information to be obtained, and according to the level of risk verified, relating to the legal form and proof of existence, ownership and control structure, powers that bind and regulate and the existence of any nominee (for a legal person) or settlor or protector (for a trust).[49]

178. Furthermore, accounting practices have now been regulated by the DIA for AML/CFT compliance for approaching eight years. This enables increased understanding of the risks associated with the sector and the effectiveness of controls by accounting practices to be assessed.

Supervisory activity and findings

179. From 1 October 2018 to 31 December 2025, DIA conducted 244 offsite desk-based reviews or onsite inspections of accounting practices' compliance with the AML/CFT Act. This included 134 reviews or inspections since 1 January 2023.

[45] AML/CFT (Requirements and Compliance) Regulations 2011, reg 15J.
[46] Definitions Regulations, reg 15A.
[47] AML/CFT (Prescribed Transaction Reporting) Regulation 2016, reg 8.
[48] AML/CFT (Exemptions) Regulations 2011, reg 24AF. (Also refer DIA's **Guidance: New regulations clarifying AML/CFT requirements for DNFBPs providing trust and company services**).
[49] Requirements and Compliance Regulations, regs 11-11A.

Supervisory tools:

Offsite desk-based reviews (i.e. not conducted at a reporting entity's premises) may involve any, or all, of the following:

- assessment of written risk assessment and AML/CFT programme.
- requests for further documentation or evidence of compliance and its effectiveness.
- follow-up questions.
- interviews or discussions on issues by phone or video conference.

Onsite inspections test the implementation and effectiveness of a reporting entity's AML/CFT procedures, policies, and controls. Onsite inspections are specific to individual reporting entities and may look at a broad range of obligations or a specific obligation, depending on the risks associated with the reporting entity.

An onsite inspection occurs at the reporting entity's business premises. These range from a day up to a period of a couple of weeks depending on the size of the business and the scope of AML/CFT obligations being reviewed.

Establishing, implementing, and maintaining an AML/CFT programme

180. Almost all accounting practices known to the DIA have appointed a compliance officer and have a written risk assessment and AML/CFT programme:[50]
    - Some accounting practices, including most larger practices, have implemented strong training, governance and compliance frameworks to ensure AML/CFT obligations are met.
    - In other circumstances, the DIA's reviews and inspections have identified compliance frameworks that are less robust, with compliance officers lacking understanding of risks and/or commitment to AML/CFT obligations. The circumstances in which accounting services are subject to the AML/CFT Act is not always understood. It is these accounting practices where more significant AML/CFT non-compliance has typically been identified.
    - For the year ending 30 June 2025, approximately 89% percent of accounting practices known to the DIA that were required to submit an annual report did so, indicative of engagement with AML/CFT obligations:
        - Responses indicate risk assessments and AML/CFT programmes are mostly being reviewed, independently audited and kept up to date, with products and services, transaction and customer information accurately reported.

[50] AML/CFT Act, ss 56-58.

  - However, in 35% of annual reports,[51] responses indicate that independent audits had not been completed. Where independent audits had occurred, adverse findings by the auditor had not always been remediated. In other cases, annual report data is incomplete.
  - As well as the 11% of known accounting practices that did not submit annual reports to the DIA, there are also practices that do not advise DIA when they commence operations as, or become, reporting entities. This means DIA is not aware of all new accounting practice reporting entities.[52]
  - Any accounting practice not known to the DIA is more likely to be non-compliant with AML/CFT obligations without direct access to relevant guidance and risk updates or active supervision.
- Approximately 75% of accounting practices known to the DIA are now registered with the FIU's goAML system to be able to submit suspicious activity and prescribed transaction reports.

Written risk assessment and AML/CFT programme

181. The DIA's reviews of accounting practices' written risk assessments and AML/CFT programmes reflect increasing understanding of their money laundering risks and AML/CFT obligations.
182. Many written risk assessments and AML/CFT programmes are still assessed as not fully meeting the requirements of sections 57-58 of the AML/CFT Act. However, where the DIA has identified these deficiencies, they have generally been of a nature that warranted remediation rather than enforcement action.
183. After approaching eight years of being subject to AML/CFT requirements, the proportion of risk assessments and AML/CFT programmes that require fundamental change or amendment is low.

Customer due diligence including ongoing CDD and monitoring, record keeping

184. The DIA's reviews and inspections show that accounting practices are implementing customer due diligence requirements (as set out in their AML/CFT programmes) to varying extents.
    - Most accounting practices conduct standard customer due diligence on their clients. Information is also obtained on the nature and purpose of the business relationship, as part of the instructions to act.
    - Less consistently implemented by accounting practices are ongoing customer due diligence and account monitoring obligations, along with associated requirements to conduct enhanced customer due diligence and examine and keep written findings for high-risk clients, activities, or transactions. This is an area of concern.

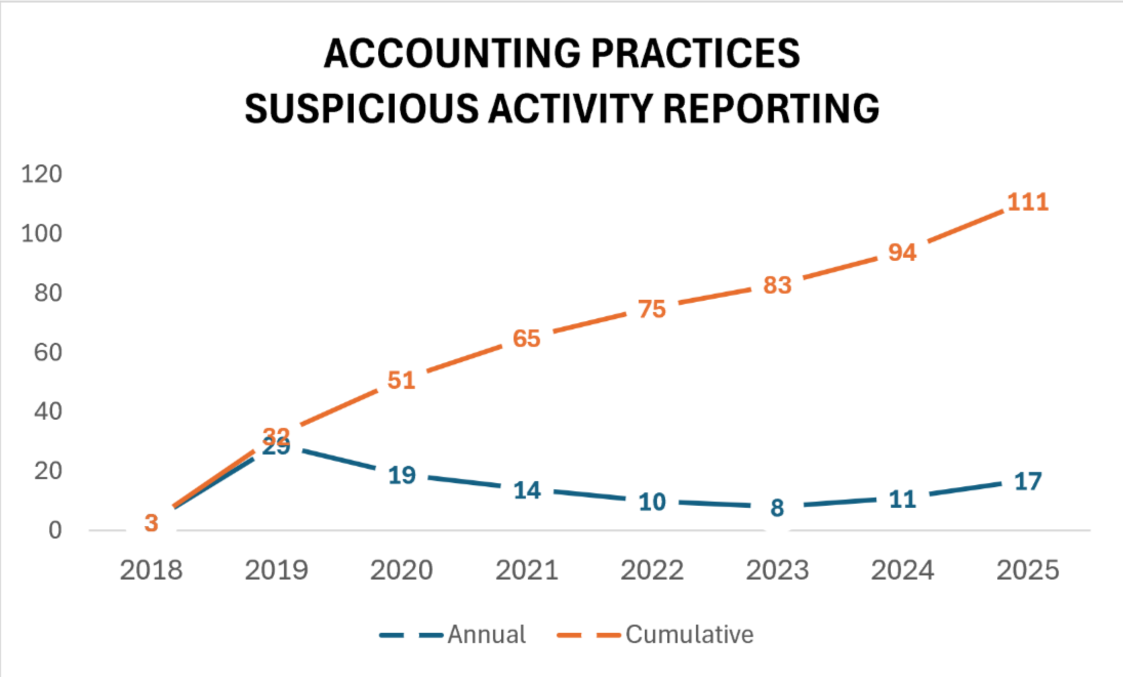
[51] Based on response to question 6.4 in Annual Report.
[52] This is the result of there being no mandatory registration requirement with the supervisor, such that the DIA does not have full visibility of its reporting entities.

- Specific to accounting practices providing trust and company services, there are still some instances when an instructing law firm, trust and company service provider or accounting practice is treated as the customer (rather than the legal person or legal arrangement being acted for).
- Most accounting practices are compliant with record keeping requirements (other than relating to keeping written findings from examination of high-risk customers, activities, or transactions).

Suspicious activity reporting

185. From 1 October 2018 to 31 December 2025, there were 111 suspicious activity reports submitted by accounting practices, with approximately 6% of practices having submitted at least one report.[53]

186. Despite the suspicious activity reports that have been submitted:
    - the overall number of suspicious activity reports from accounting practices is low, indicating not all circumstances in which a suspicious activity report is required are being identified. This is also consistent with the DIA's findings during reviews and inspections.
    - there are not many suspicious activity reports being submitted relating to trust and company services.

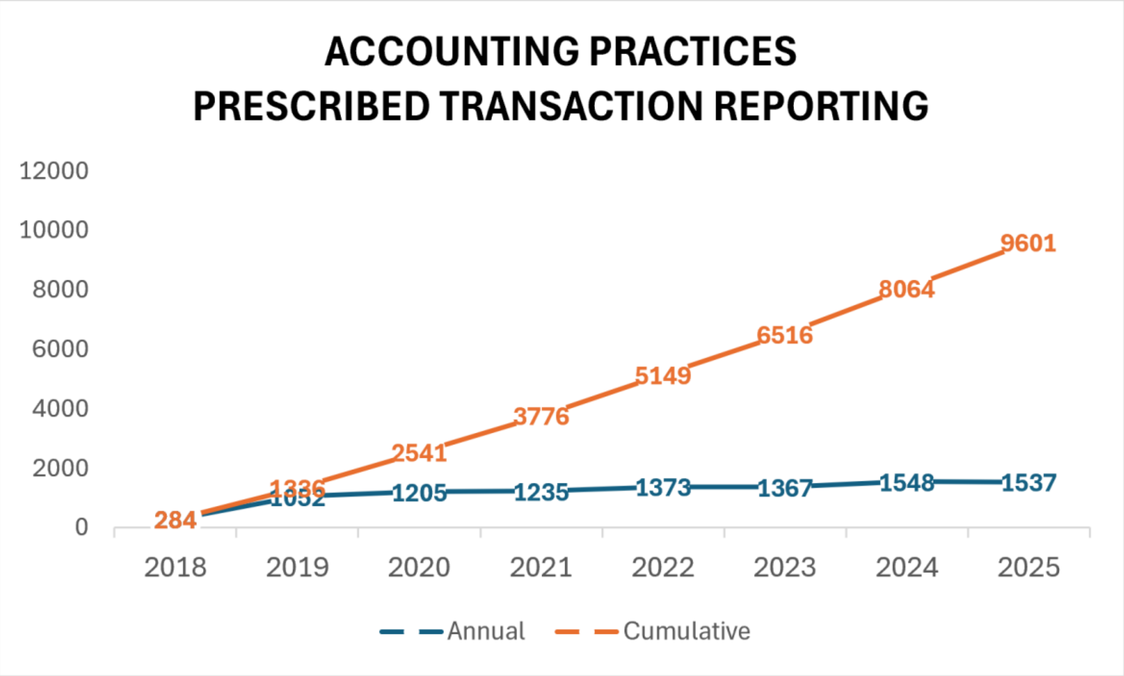


[53] Based on FIU data - goAML category and listed report date. By comparison, the law and conveyancing sector submitted 812 reports over a marginally longer period, albeit predominantly focussed on real estate conveyancing related matters.

187. The top six reasons for suspicious activity reports from accounting practices are:
    1) Suspected tax offending
    2) Suspicious source of funds
    3) Large volume of cash deposits into client bank accounts
    4) Refusal to provide information/complete customer due diligence
    5) Reluctant or hesitant to provide information
    6) Possible scam or fraud victim

Prescribed transaction reporting

188. From 1 October 2018 to 31 December 2025, there were 9,601 prescribed transaction reports submitted by accounting practices (covering 13,444 transactions).[54] Only 43 of the reports (covering 45 transactions) related to large cash transactions (of $10,000 or more). All others related to international funds transfers (of $1,000 or more).
189. The number of prescribed transaction reports submitted by accounting practices is increasing. This likely reflects increased understanding of requirements, including the clarification to the application of prescribed transaction reports in relation to international funds transfers in or out of trust accounts (refer paragraph 176 above).[55]



[54] Based on FIU data - goAML category and listed report date.
[55] For further information in relation to international funds transfer reporting, refer to: DIA's **Guidance: wire transfer requirements for designated non-financial businesses or professions**.

Complementary prescribed transaction reporting:

190. Prescribed transaction reports from accounting practices relating to international funds transfers are an important part of the financial intelligence picture. While there may also be a prescribed transaction report submitted by a bank in relation to the same transfer of funds, the two reports will never be identical.
191. Consequently, this is not considered duplicate but complementary reporting. The accounting practice and the bank will provide a different "snapshot" of the transaction. In particular, the report from an accounting practice provides important visibility of the underlying client in New Zealand that is sending or receiving funds internationally (that the banks' prescribed transaction report will not have).

Gaps in controls

192. The DIA identifies three factors impacting the effectiveness of AML/CFT controls at a sector level.

No registration requirement

193. There is no requirement that accounting practices register with DIA as the AML/CFT supervisor. This means DIA must proactively identify those accounting practices that do not make themselves known to DIA when they commence operations as, or become, reporting entities. Noting the disparate nature of the sector (refer paragraph 87 above), it is likely that not all accounting practices are known to the DIA or subject to active AML/CFT supervision.

Monitoring, examination, and enhanced customer due diligence

194. Despite having risk assessments and AML/CFT programmes in place, some accounting practices are not adequately implementing their own procedures, policies, and controls. In particular:
    - There are common deficiencies relating to requirements to monitor, examine and keep written findings for high-risk clients, activities, or transactions, and to conduct enhanced customer due diligence in all situations where the level of risk requires it.[56]
    - Monitoring, examining, and keeping written findings are key obligations that enable reporting entities to identify and respond to the circumstances in which their risks are higher in accordance with a risk-based approach.

[56] This is a deficiency that DIA identifies across many DNFBPs (real estate agents, accounting practices, trust and company service providers, law and conveyancing firms).

Suspicious activity reporting

195. The number of suspicious activity reports from accounting practices is consistently low. Noting the deficiency above relating to monitoring, examination and enhanced customer due diligence, it is possible that not all suspicious activity is being identified or reported to the FIU.

Reminder:

196. Any accounting practice not enrolled with the DIA as a reporting entity or registered with goAML should ensure it does so.
197. All accounting practices are also reminded of the requirements to monitor, examine and keep written findings relating to high-risk clients, activities and transactions, and to conduct enhanced customer due diligence as necessary. Without this, suspicious activity cannot be identified or reported to the FIU.

Overall residual sector risk rating – money laundering

198. Notwithstanding the gaps identified above, the DIA's AML supervision of the accounting sector assesses controls as **moderately** effective in managing and mitigating the sector's vulnerability to money laundering. This means that the accounting sector is a harder overall target for criminals compared to its inherent money laundering vulnerability rating.
199. Accordingly, the overall accounting residual sector risk rating after the implementation of AML controls is assessed as **Low-Medium**.

Inherent ML Vulnerability Rating	Strength of Controls Rating	Residual ML Risk Rating
Medium	Moderate	Low-Medium

Part 3: Sector risk - terrorism financing and proliferation financing

Vulnerability of accounting practices to terrorism financing

200. The overall terrorism financing threat to New Zealand is assessed as Low.

Trust and company services

201. While there is no terrorism financing threat identified specific to accounting practices, the NRA 2024 determines there is a possibility that New Zealand companies have or will at some future time be misused for terrorism financing.

Non-profit organisations and charities

202. As also identified in the NRA 2024, non-profit organisations and charities are internationally recognised as having vulnerability to terrorism financing.
203. Non-profit organisations and charities can be used to disguise the movement of funds to high-risk regions, and funds donated for humanitarian purposes can be diverted and misappropriated in the supply chain to support terrorism.
204. It is important to consider this vulnerability in the context of the lower risk New Zealand environment, and that this will not apply to the vast majority of New Zealand charities and non-profit organisations. That said, any accounting practice that provides services to charities or other non-profit organisations operating or providing humanitarian support to conflict zones, or to countries with terrorist groups, is exposed to some terrorism financing risk.
205. On the basis of the above, the inherent vulnerability to terrorism financing rating of the accounting sector as a whole is assessed as **Low**. However, accounting practices that provide trust and company services have an elevated inherent vulnerability assessed as **Medium-High**.

Strength of Controls

206. Money laundering and terrorism financing share many of the same typologies, indicators or "red flags".
207. Many accounting practices do not need to implement any specific measures to mitigate terrorism financing risk. To the extent there is risk, this can be mitigated by well-implemented AML controls across customer due diligence, monitoring for unusual and higher-risk activities or transactions, and suspicious activity reporting. These controls are assessed as **Moderately** effective at a sector level.
208. However, accounting practices should ensure they understand their terrorism financing risks. Those most exposed are:
    - Accounting practices that provide trust and company services involving clients, activities, or transactions internationally.

- Any accounting practice that provides services to charities or other non-profit organisations operating in, or providing humanitarian support to, conflict zones or to countries with terrorist groups.

209. Accounting practices should also remain alert to clients, whether in New Zealand or overseas, with observable behaviours of potential support and/or escalation towards politically motivated, faith motivated, identity-motivated or single issue-motivated violent extremism. For further information, refer to the NZSIS Know-the-signs guidance.

Overall residual sector risk rating – terrorism financing

210. The overall accounting residual sector risk rating for terrorism financing after the implementation of AML/CFT controls is assessed as **Low**.

Inherent TF Vulnerability Rating	Strength of Controls Rating	Residual TF Risk Rating
Low	**Moderate**	**Low**

Vulnerability of accounting practices to proliferation financing

211. The overall proliferation financing threat to New Zealand is assessed as Low.

Trust and company services

212. While there is no proliferation financing threat identified specific to accounting practices, the NRA 2024 identifies that the misuse of New Zealand's corporate structures and legal arrangements is (along with cyber-attacks) our most significant vulnerability to proliferation financing. This includes to support procurement of and trade in sensitive goods and revenue-raising activities for proliferation. As the NRA 2024 also identifies, proliferation financing internationally makes extensive use of shell companies and non-transparent corporate structures.
213. On the basis of the above, the inherent vulnerability to proliferation financing rating of the accounting sector as a whole is assessed as Low. However, accounting practices that provide trust and company services have an elevated inherent vulnerability assessed as **Medium-High**.

Strength of Controls

214. While the AML/CFT Act does not contain explicit requirements that a reporting entity has to assess (or manage and mitigate) its proliferation financing risks, doing so assists an accounting practice in complying with its AML/CFT obligations.

215. Furthermore, to the extent that proliferation financing involves criminal activity generating income (for example cyber-crimes), the requirements of the AML/CFT Act directly apply. In addition, a suspicious activity report under the AML/CFT Act must be submitted in relation to any activity or transaction suspected of being related to proliferation financing.
216. Many accounting practices do not need to implement any specific measures to mitigate proliferation financing risk. To the extent there is risk, this can be mitigated by well-implemented AML controls across customer due diligence, monitoring for unusual and higher-risk activities or transactions, and suspicious activity reporting. These controls are assessed as **Moderately** effective at a sector level.
217. However, accounting practices should remain vigilant and aware of proliferation financing risks. Those most exposed are:
    - Accounting practices that provide trust and company services involving clients, activities, or transactions internationally. This is particularly so if involving intermediary jurisdictions with links to North Korea or Iran, or if involving North Korea or Iran themselves.

Overall residual sector risk rating – proliferation financing

218. The overall accounting residual sector risk rating for proliferation financing after the implementation of AML/CFT controls is assessed as Low.

Inherent PF Vulnerability Rating	Strength of Controls Rating	Residual PF Risk Rating
Low	Moderate	Low

New Zealand's exposure to proliferation financing

219. Notwithstanding the low proliferation financing risk rating and absence of explicit obligations in the AML/CFT Act relating to proliferation financing, all accounting practices should understand New Zealand's exposure to proliferation financing. This includes understanding the sanctions in place relating to dealings with North Korea or Iran.
220. **North Korea** - the United Nations Sanctions (Democratic People's Republic of Korea) Regulations 2017 impose complex and wide-ranging prohibitions on dealings with North Korea, North Korean citizens, and North Korean companies.[57]

[57] For further information refer to the MFAT website: North Korea | New Zealand Ministry of Foreign Affairs and Trade.

221. The sanctions include an asset freeze – i.e. a prohibition on transferring, selling, or otherwise dealing with any property (including land, shares, or money) that is owned or controlled by the North Korean Government, a person or entity designated by the UN's North Korea sanctions committee, or any person who is assisting in evading the sanctions regime.

222. **Iran** – United Nations sanctions were reimposed on Iran in September 2025 after the triggering of the snapback mechanism under the Joint Comprehensive Plan of Action (JCPOA), in response to Iran's non-compliance with its nuclear obligations. The United Nations Sanctions (Iran) Regulations 2025 include the following obligations and restrictions:
    - prohibitions, including asset freeze obligations, on certain dealings related to designated persons;
    - a duty to exercise vigilance when doing business with entities incorporated in Iran or subject to its jurisdiction;
    - a compulsory business registration scheme (in force since 1 February 2026) and a requirement to keep business records for at least seven years; and
    - import, export and procurement bans relating to nuclear weapon, missile, or enrichment-related goods, and to arms.[58]

223. The Ministry of Foreign Affairs and Trade strongly recommends that anyone contemplating doing business with North Korea or Iran obtain independent legal advice to avoid breaching the sanctions.

224. **Export controls** - New Zealand assesses exports of military and dual use goods, software, and technology. Where an export is assessed as posing a risk to New Zealand's security or national interests, or as being inconsistent with New Zealand's international obligations, commitments, or policies, including those relating to international law, international human rights law, and international humanitarian law, the export may be denied if adequate safeguards cannot be put in place.

225. Controlled exports are identified in the New Zealand Strategic Goods List,[59] or may be captured under New Zealand's catch all controls where there is military end use. New Zealand also controls the import and export of the Organisation for the Prohibition of Chemical Weapons scheduled chemicals.

[58] For further information refer to the MFAT website: Iran | New Zealand Ministry of Foreign Affairs and Trade.

[59] Refer: New Zealand Strategic Goods List July 2026.

Red flags for proliferation financing include:

- **Transactions or activities involving:**
    - Countries subject to UN sanctions or known for weapons of mass destruction proliferation.
    - Use of intermediaries or shell companies in third-party jurisdictions with links to these UN sanctioned countries.
- **Unusual trade or payment activity:**
    - Payments for (which may or may not include shipping related costs) dual-use goods (civilian and military applications).
    - Transactions involving sensitive technologies or chemicals without export permits.
    - Mismatches between the customer's business profile and the goods/services traded.
    - Payments routed through multiple jurisdictions without clear business justification.
    - Unusual involvement of third parties in trade finance or logistics.
    - Payments for intellectual services in fields relevant to weapons of mass destruction.
- **Complex ownership structures:**
    - Use of trusts, nominee shareholders, or offshore entities that obscure beneficial ownership.
    - Client is reluctant to provide information about end-users, end-use, or counterparties.
- **Lack of economic rationale:**
    - Transaction or activity not consistent with a customer's profile or does not make commercial sense.
    - Use of shell companies with no real business activity, especially in international trade.
    - Frequent changes in shipping routes or documentation, especially when linked to high-risk countries or goods.

Part 4: Other factors that increase or decrease risk for individual accounting practices

226. Other factors increase or decrease the vulnerability to money laundering, terrorism financing or proliferation financing associated with an individual accounting practice's products and services.
227. These factors are:
    - the nature, size, and complexity of the accounting practice's business;
    - the types of customers dealt with;
    - the methods by which services are delivered;
    - the countries dealt with;[60] and
    - the institutions dealt with.
228. An accounting practice must have regard to each of these factors, alongside its products and services, when undertaking or updating its risk assessment (as required by section 58 of the AML/CFT Act).

Nature, size, and complexity of business:

229. The nature, size, and complexity of an accounting practice's business is an important factor in how vulnerable it is for money laundering or terrorism financing.
230. For example, a large business with a complex business model offers a greater degree of anonymity and opportunity for criminal activity to go undetected.

Increased risk	Decreased risk
• Multiple branches or offices with decentralised delivery of products and services. • Multiple services provided subject to the AML/CFT Act, including in conjunction with each other. • Large number of staff with high turnover or temporary staff.	• Strong governance and compliance framework. • Single or limited range of products and services. • Stable and well-trained staff that understand ML/TF risks and AML/CFT obligations.

Types of customers dealt with:

231. Some types of customers pose a higher risk than others, especially when combined with higher-risk products and services or countries.

[60] For further information on country risk, refer to the DIA's **Guidance: Assessing Country Risk**.

Increased risk	Decreased risk
• Clients involved in cash-intensive businesses. • Clients involved in other high-risk occupations and industries (for example money remittance, virtual assets, other new or developing technologies or gambling). • Clients with complex ownership structures (particularly if beneficial owner(s) cannot be easily identified). • High-net-worth clients. • Overseas-based clients and clients in New Zealand on temporary visas. • Politically exposed persons (PEPs). • Trusts or other legal arrangements. • Not-for-profit organisations that are subject to limited, or no monitoring or supervision by authorities.	• Stable and established client base. • Types of customers that are eligible for simplified CDD (as listed in section 18(2) of the AML/CFT Act). • Simple client types – individuals whose income is from regular salary payments.

Methods by which products and services are delivered:

232. The extent to which there is the opportunity for a customer to interact with an accounting practice remotely, anonymously, and/or through an intermediary or agent impacts its vulnerability to money laundering or terrorism financing.

Increased risk	Decreased risk
• Clients onboarded remotely — no face-to-face contact. • Indirect contact with clients, for example the use of other gatekeepers, agents or intermediaries to conduct customer due diligence. • Products or services provided to persons in overseas jurisdictions. • Transactions in cash or involving cash deposits to bank accounts.	• Clients onboarded face-to-face. • Customer due diligence conducted directly (rather than outsourced or relying on another gatekeeper or agent).

Countries dealt with:

233. The risks associated with the countries that an accounting practice deals with are an important factor when considering the vulnerability to money laundering or terrorism financing. It is also important to understand that the risks associated with a country are wider than whether that country has previously been assessed to have insufficient AML/CFT measures in place.

Increased risk	Decreased risk
• Any dealing with countries or jurisdictions (including clients, beneficial owners, intermediaries, activities or transactions) with high levels of: ○ bribery or corruption; ○ capital flight; ○ organised crime activity; ○ tax evasion. • Any dealing with persons or entities in jurisdictions: ○ in or next to a conflict zone; ○ known for the presence/support of terrorism; ○ known for the production and/or transnational shipment of illicit drugs; ○ with organised people trafficking; ○ with ineffective AML/CFT systems, measures or controls.	• No or limited number of clients, activities or transactions involving other countries. • Countries that are dealt with are considered low risk.

Institutions dealt with:

234. Some institutions dealt with present more money laundering or terrorism financing risk than others. This may be due to the nature of their industry or their association, or the types of business relationships that they have.

Increased risk	Decreased risk
• Other institutions (including other reporting entities, intermediaries or other service providers) dealt with when providing service that are: ○ previously identified as having AML/CFT deficiencies (such as public warnings/fines); ○ subject to adverse media coverage in relation to AML/CFT or other regulatory matters; ○ in a high-risk sector (for example money remitters or virtual asset service provider). • Use of other gatekeepers to: ○ access financial services; ○ act as intermediaries in transactions; ○ facilitate transactions through client trust accounts.	• n/a

Risk factors in combination:

235. Higher risk factors do not operate in isolation but in combination with others. Where two or more higher risk factors apply to a particular customer, activity or transaction, the level of risk compounds.
236. Conversely, accounting practices whose businesses do not include any of these higher risk factors have less risk of money laundering, terrorism financing, or proliferation financing.

237. As well as understanding the factors that will increase or decrease the risk, accounting practices should remain vigilant for unusual situations or requests by clients where the level of risk elevates.
238. Remaining alert and responsive to behavioural “red flags,” even in the absence of other higher risk indicators, is a key part of implementing an effective AML/CFT programme.

Behavioural red flags by clients include:

- Client is a type of business not normally cash intensive but appear to have substantial amounts of cash.
- Client is using cash in unexpected or unexplained circumstances.
- Client whose instructions are unusual and/or with no apparent visible or economic purpose.
- Client who appears to avoid face-to-face meetings.
- Client is reluctant to provide identification or behaves nervously.
- Client who appears to be acting on somebody else's instructions without disclosing the identity of that person.
- Client asks for shortcuts or unexplained speed in completing a transaction or activity.
- Identity or other verification documents provided are or look fraudulent.
- Client enquiring into whether a product or service would be considered suspicious or require reporting to authorities.
- An absence of documentation to support the client's stated reason for engaging the accounting practice, their previous transactions, or business activities.
- Client who offers to pay extraordinary fees for services that would not warrant such a premium.
- Client using a small or non-specialised practice to provide complex services.

Known clients or referrals via trusted third parties

239. When a client is a person known (for example a friend or family member) to a partner, manager, employee or agent of an accounting practice, this should not result in complacency that the client is low risk. This also extends to referrals via trusted associates, friends, or family members - the client does not automatically become legitimate or trustworthy.
240. While personal knowledge from a non-professional relationship may in many cases be useful in understanding the client's activities and transactions, assumptions should be challenged and the requirements of the AML/CFT Act still apply (including verification of information from reliable and independent sources).
241. Employees, agents or other persons involved in delivery of a reporting entity's services pose unique risks (known as an "insider threat"). These persons have knowledge of a reporting entity's AML/CFT programme and may be able to bypass requirements or otherwise use their knowledge to influence or manipulate compliance processes for the benefit of themselves and/or the client.

Appendix: Summary of key obligations for accounting practices

242. The AML/CFT Act requires accounting practices to establish, maintain and implement an AML/CFT programme to detect money laundering and terrorism financing, and to manage and mitigate the risk of it.
243. An accounting practice must undertake a risk assessment of its business to identify the money laundering and terrorism financing risks it may reasonably expect to face. The AML/CFT programme must then be based on its risk assessment.
244. An accounting practice's AML/CFT programme must include its procedures, policies, and controls for conducting customer due diligence, monitoring customer activities and transactions, reporting suspicious activity and certain types of prescribed transactions to the FIU, and for keeping records.

Customer due diligence

245. Some form of customer due diligence (simplified, standard, or enhanced) must be conducted whenever an accounting practice establishes a business relationship with a new client, or if a person seeks to conduct an occasional transaction or an occasional activity with the accounting practice.
246. For most instances when customer due diligence is required, an accounting practice must obtain identity information and verify this information from reliable and independent sources.
247. The accounting practice must also conduct ongoing customer due diligence and monitor client activities and transactions to ensure those activities are consistent with its knowledge about the customer and their risk profile.
248. In higher risk circumstances, an accounting practice must conduct an enhanced level of customer due diligence. This requires verification of the client's source of funds or wealth and potentially put other measures in place to mitigate the money laundering and terrorism financing risks. In lower risk circumstances, accounting practices may conduct a simplified level of customer due diligence.
249. If customer due diligence is not conducted or cannot be completed, then a business relationship must not be established, or an occasional transaction or occasional activity must be refused. If a business relationship has previously been established, it must be terminated.

Suspicious activity reporting

250. A suspicious activity report must be submitted to the FIU where an accounting practice has reasonable grounds to suspect that a transaction, service, or inquiry, is or may be relevant to the investigation, enforcement, or prosecution of crime. This is based on an objective test. A suspicious activity report must be submitted as soon as practicable, but no later than three working days after forming the suspicion.

251. Suspicious activity reporting obligations do not just apply in relation to an accounting practice's client, but also in relation to any other party dealt with in relation to an activity subject to the AML/CFT Act.

Prescribed transaction reporting

252. An accounting practice must also submit a prescribed transaction report to the FIU for:
    - any domestic cash transaction of $10,000 or more; and
    - any international wire transfer of $1,000 or more received or sent from a trust account for a client.
253. A prescribed transaction report must be submitted as soon as practicable, but no later than twenty working days after the transaction.

Record keeping

254. An accounting practice must keep records of all customer due diligence and transactions undertaken by clients. It must also keep any other records relating to a business relationship which may be needed to establish the nature of the business relationship, and activities relating to it. For example, this may include account files, business correspondence and written findings relating to examination of high-risk transactions. All records must be kept in a form that is readily accessible, and for five years after the transaction or end of a business relationship.

Managing compliance with AML/CFT programme

255. An employee, a partner, or a senior manager of an accounting practice must be appointed as a compliance officer to administer and maintain the AML/CFT programme. The accounting practice must also undertake vetting and training on AML/CFT matters for senior managers, the compliance officer, and any other employees engaged in AML/CFT duties. This is to ensure that its AML/CFT programme is complied with and effective.
256. An accounting practice must also submit an annual report to its supervisor and have its risk assessment and AML/CFT programme audited every three years.

Version	Date	Author	Description of Changes
1.0	December 2017	Department of Internal Affairs	Initial SRA for phase 2 sectors
1.1	December 2019	Department of Internal Affairs	Updated SRA for DNFBP sectors
2.0	July 2026	Department of Internal Affairs	Accounting SRA 2026