Te Tari Taiwhenua
Internal Affairs

Te Kāwanatanga o Aotearoa
New Zealand Government

# A Guide to DIA's Anti-Money Laundering and Countering Financing of Terrorism Compliance and Enforcement Activities

# 2022

# Contents

# Purpose

This document sets out how the Department of Internal Affairs (DIA) uses compliance and enforcement tools to:

— build the capability and effectiveness of reporting entities in detecting and preventing their businesses from being used by criminals and terrorists, who seek to hide or move money through the financial system.

— support New Zealand and international efforts to make it difficult for criminals and terrorists to exploit financial systems.

It sits alongside DIA's Approach to Regulation of AML/CFT, which outlines our regulatory approach. The publication of a guide to our compliance and enforcement activities supports the embedding of regulatory foundations; a focus of DIA's **Regulatory Services Group Strategy 2021–2026**.

# Our approach to compliance and enforcement

We are a risk-based, intelligence-led, and outcome-focussed regulator. This means that we use risk assessment and analysis, along with our knowledge and expertise, to target and prioritise compliance and enforcement activities on the areas of greatest risk, or to have maximum impact on compliance with the AML/CFT legislation.

DIA uses a range of tools to support reporting entities to comply, to monitor compliance, and to enforce compliance when needed. When deciding which regulatory activity to use, we take a risk-based and responsive approach. This includes considering the reporting entity's attitude to compliance and applying regulatory activities that are appropriate and proportionate to the circumstances of each case.

# Operating context

# The money laundering and terrorism financing environment in New Zealand

**Money laundering** is the process criminals use to 'clean' the money or assets they make from criminal activity.

Money laundering involves concealing the origin of the proceeds of crime or converting it into another form of property, so that it appears to have been legitimately earned. It can then be enjoyed as property or luxury goods, or used to fund further criminal activity, or used for legitimate business.

Money laundering is an offence under the Crimes Act 1961 (section 243).

Money laundering is a significant problem in New Zealand. It is estimated that around $1.35 billion is laundered annually in New Zealand, primarily from drug offending and fraud.[1] This figure excludes domestic tax evasion and the laundering of the proceeds of crime overseas through the New Zealand financial system. The actual cost, including the harm to our iwi, hapū and communities from the criminal activity that generated the proceeds of crime, is much higher.[2]

Money laundering, in relation to money, is often thought of as a three-step process:

1. **Placement** – This involves introducing the proceeds of crime into the financial system. For some criminal offences, including drug offending, the criminally derived funds are likely to be held and placed into the financial system in cash.
2. **Layering** – The funds are moved or converted into other property to distance or disguise them from their criminal origin. This may involve breaking the funds up or moving them around in a series of transactions.
3. **Integration** – The funds re-enter the financial system in a form that appears legitimate.

Money laundering does not require completion of all three steps. For example, in some cases, the placement stage and the underlying criminal offending, that generates the proceeds of crime, occur together. An example of this could be fraud.

1. New Zealand Police Financial Intelligence Unit. 2019. *National Money Laundering and Terrorism Financing Risk Assessment.*
2. Department of Internal Affairs. December 2019. *Financial Institutions and DNFBP Sector Risk Assessments*

**Terrorism financing** is the process by which terrorists and their supporters raise and move funds to commit terrorist acts or fund ongoing operations to commit terrorist acts.

The movement of funds for terrorism financing may use similar methods to money laundering. While the value of the funds may be much lower than in money laundering transactions, the potential consequences of terrorism financing are catastrophic. The funds used for terrorism financing may come from both illicit and legal sources.

Financing of terrorism within New Zealand is most likely to relate to lone actors or small cells, using simple methods of organisation and corresponding small-scale or self-funding arrangements. There is also the risk that radicalised individuals in New Zealand will support overseas terrorist groups, with New Zealand used as a source or conduit for funds to finance terrorism offshore.[3]

**Proliferation financing** refers to funding or the provision of services related to the development of chemical, biological or nuclear weapons, commonly referred to as weapons of mass destruction (WMD). This includes any services involving the purchase, export, shipment or delivery of materials that can be used to manufacture WMD. There are various dual-use items and technologies available in New Zealand that could be used to manufacture WMD. As with terrorism financing, the potential consequences of proliferation financing are catastrophic.

3. New Zealand Police Financial Intelligence Unit. 2019. *National Money Laundering and Terrorism Financing Risk Assessment.*

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

The aims of the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 are to:

1. detect and deter money laundering and the financing of terrorism; and
2. maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the Financial Action Task Force; and
3. contribute to public confidence in the financial system.[4]

The Ministry of Justice (MoJ) is responsible for administering the AML/CFT Act and its six Regulations.

The Act places obligations on certain types of businesses, known as **reporting entities**, to detect and deter money laundering and terrorism financing.

## DIA functions under the AML/CFT Act

The **Department of Internal Affairs** (DIA) is one of three supervisors (government agencies with regulatory responsibilities), empowered by the Act, to assess the money laundering and terrorism financing risks across the reporting entities they supervise, and promote, monitor, investigate and enforce their reporting entities' compliance with the Act.

The other supervisors are the **Reserve Bank of New Zealand** (RBNZ) and the **Financial Markets Authority** (FMA).

Each supervisor supervises different types of reporting entities based on the services the reporting entity provides and the sector within which it operates. Supervisors are also responsible for producing guidance for reporting entities about meeting their obligations and evolving risks and trends, and for producing Sector Risk Assessments (SRAs).

4. Anti-Money Laundering and Countering Financing of Terrorism Act 2009. Retrieved from **www.legislation.govt.nz/act/public/2009/0035/latest/DLM2140720.html**

# Where we focus and why

# Where we focus and why

We want to ensure that our resources, and reporting entity resources, are used as efficiently as possible to best protect New Zealand businesses from money laundering or terrorism financing.

Reporting entities can expect the method, intensity and frequency of their compliance engagements with DIA to vary. This is because reporting entities have different ML/TF risk profiles, different levels of compliance, different levels of capability, and different attitudes towards compliance.

A significant part of our supervision is focussed on building reporting entity capability. We work on the understanding that most businesses want to comply and we aim to make it as easy for reporting entities to comply as possible. This includes helping those that are trying their best to comply, and proportionally using the tools and sanctions provided within the AML/CFT Act where non-compliance is identified.

We use our professional insight, expert knowledge and regulatory understanding to identify risks and determine the most appropriate activities to use to monitor and ensure compliances to use to monitor and ensure compliance.

# Risk-based and intelligence-led approach

We determine our monitoring activities for a reporting entity based on our knowledge of it and our assessment of the risk of it being used for ML/TF. This enables us to target and prioritise our resource so the frequency, timing, focus and types of compliance assessment we undertake have the maximum impact on individual reporting entity and sector compliance.

To understand the ML/TF risks for reporting entities, we use inherent risk profiles and combine this with other information to determine how DIA's compliance resources are targeted. Appendix A provides a summary of each sector's inherent risk profile and a brief descriptor on what contributes to that risk. More detailed information about inherent risk profiles can be found in sector risk assessments.

The additional information we consider includes:

- **Risk assessments** (National Risk Assessments, Sector Risk Assessments, and Reporting Entities' Risk Assessments)
- **Trigger Events** – such as tip-offs, suspicious activity reports, media reports, international AML/CFT events, criminal activity and intelligence from other agencies
- **Previous compliance engagement and activities**
- **International trends**

We use our professional judgement, our own experience, and information from other government agencies and domestic and international supervisory colleagues to determine which reporting entities and what compliance obligations we should focus on.

## Risk assessments

There are three levels of AML/CFT risk assessment in New Zealand:

- **National Risk Assessment (NRA)** – this provides an overall assessment of New Zealand's money laundering and terrorism financing risks and is published by the New Zealand Police Financial Intelligence Unit (FIU). The NRA uses a model based on international guidance, where risk is a function of threats, vulnerabilities and consequences. Information from suspicious activity reports (SARs), operational intelligence and investigations, sector surveys and international reports and guidance is used to develop the NRA.
- **Sector Risk Assessment (SRA**) – these are produced and published by each AML/CFT supervisor relevant to their own sectors. These SRAs are informed by the NRA and based on consultation with industry, supervisory experience, international guidance, and reporting entities' risk assessments.
- **Reporting Entity Risk Assessment** – all reporting entities must produce an assessment of the risk of money laundering/terrorism financing in their business. They must consider the nature, size and complexity of their business, the products and services provided, their methods of delivery, and their types of customers, countries, and institutions they deal with. Reporting entities must also use the guidance material provided by their supervisor and the FIU when developing their own risk assessments.

## Entity Risk Model (ERM)

DIA uses an entity risk model (ERM) to assess the ML/TF risk profile of a reporting entity.

The ERM is a risk calculation tool that uses data and information from various sources and activities to calculate a risk score for each reporting entity. Risk scores reflect the characteristics of reporting entities and their response to being regulated and provide us with an indication of their level of compliance and the ongoing risk of ML/TF.

The ERM uses:

- information that reporting entities submit in their Annual Report.
- risk scores derived from the services or captured activities entities provide.
- outcomes of our compliance assessments or inspections, such as whether there was the need for remediation work, formal warnings, or court proceedings.
- other information received about a reporting entity, such as adverse media. This information might be in the public domain or might be held by us or by other AML/CFT supervisors or government agencies.

# Choosing our regulatory activities

# What we consider when choosing our regulatory activities

We have a range of regulatory activities we can use to assist or ensure reporting entities comply with their AML/CFT obligations. These range from education and engagement initiatives, which are general and achieve a high level of coverage, to enforcement actions which are targeted to individual reporting entities.

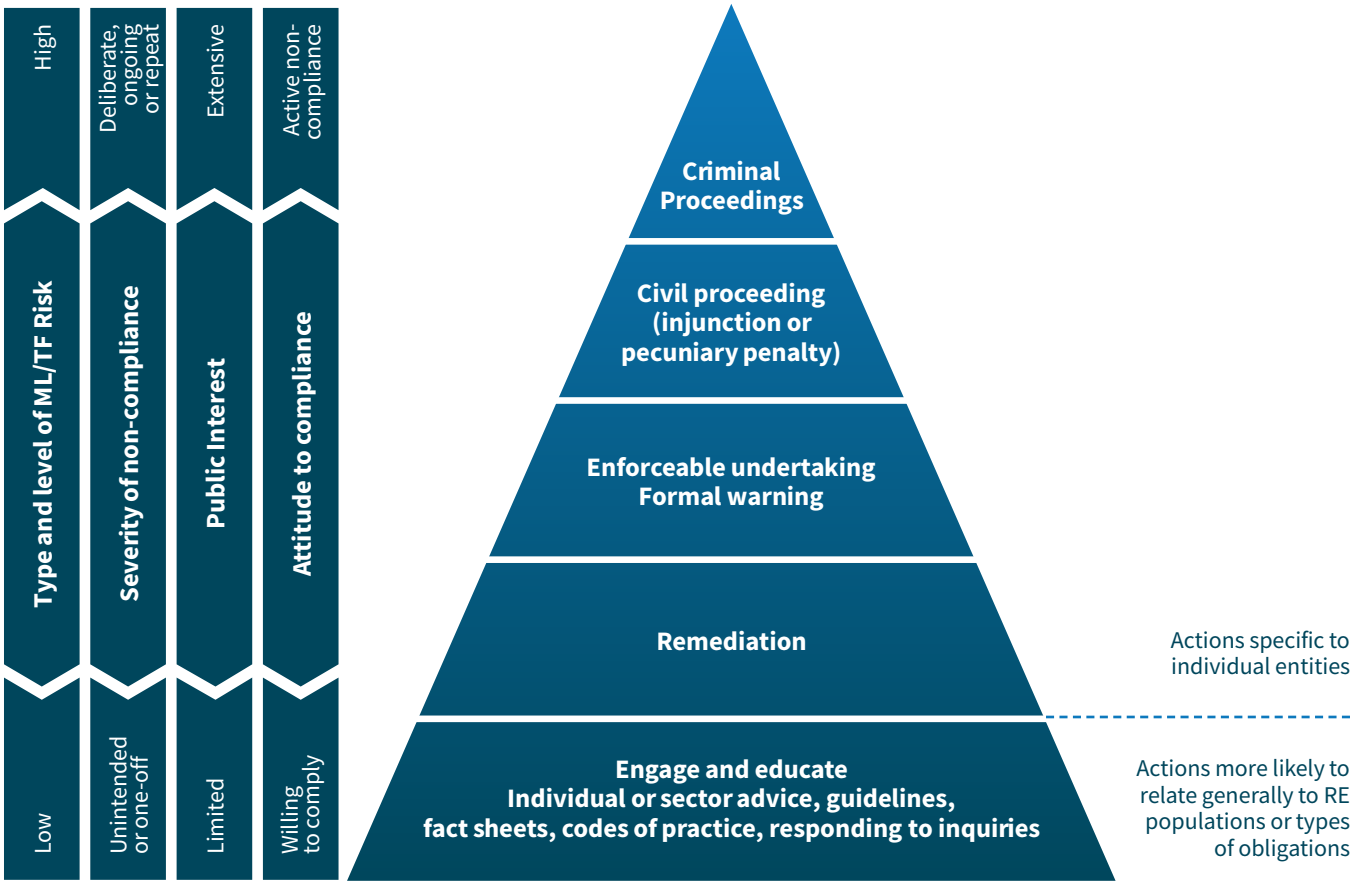
A number of factors help inform how we determine which activities we use for which situation to achieve our AML/CFT goals, including but not limited to:

- ML/TF risks associated with a reporting entity or a sector
- emerging or evolving ML/TF trends or issues in a sector or across sectors
- the potential severity of non-compliance
- public interest
- reporting entity attitude to compliance
- goals of the National Anti-Money Laundering and Countering Financing of Terrorism Strategy and of our AML/CFT partner agencies (i.e. other supervisors or Police).[5]

5. For the National AML/CFT Strategy, refer to the **cabinet paper** setting the strategic direction for New Zealand's Anti-Money Laundering and Countering the Financing of Terrorism Regime.

The following diagram shows how the factors we take into consideration influence the intensity of regulatory activity we choose.

**Diagram A: Factors that influence our choice of regulatory activity**




**Note:** regulatory activities are not applied in a sequence – education does not have to occur prior to enforcement

If we are determining a response to the non-compliance of an individual reporting entity, the decision is considered on a case-by-case basis and tested through a peer review process. This means our response is tailored to the particular reporting entity and the nature of its non-compliance.

If we are considering an enforcement action, this is also tested with a review panel. The panel consists of managers and technical specialists and supports robust, consistent, and appropriate operational decision-making capability. The panel can also examine a selection of cases after the fact to make recommendations about changes to our processes that would lead to improved performance in compliance and enforcement. The review panel does not replace the need for statutory decisions that require formal delegations to be made by the holders of those delegations, following appropriate processes.

## Engagement and education

### Engagement

We aim to build strong relationships with the sectors we regulate to understand how we can strengthen the effectiveness of the AML/CFT system and our regulatory activities.

- We have established a cross-sector group – the Industry Advisory Group (IAG) – as a formal channel for sector feedback and consultation. Members include experts and professionals in their areas of practice. The IAG is an important way for us to hear how the AML/CFT system is working, from the perspective of those being regulated, and helps inform our thinking about improvements to our regulatory approach.
- We work with peak bodies (i.e. organisations that represent reporting entities), to ensure we provide them with the best information and support for their members. We continuously explore how to best communicate and engage with the peak bodies.
- We use surveys and feedback from reporting entities, peak bodies and the IAG to identify which obligations reporting entities need support with and what improvements we could make to our regulatory activities to make AML/CFT compliance as easy as possible.
- We work with reporting entities and peak bodies to improve the design of our regulatory tools to make it as easy as possible for reporting entities to use our systems, such as annual report submission systems.

### Education

Education is a fundamental tool for promoting compliance and is designed to improve reporting entities general understanding of their obligations, their ML/TF risks and how to manage them. Education initiatives such as email-outs, newsletters, webinars, sector workshops, road shows, and industry guides, can achieve a high level of coverage across a large number of reporting entities. We may also tailor advice, or make education visits, to individual reporting entities, where a specific issue or event requires it or has been requested.

Education may be used when interacting with a new reporting entity, when triggered by a particular event or issue that needs to be communicated, or where there is an identified issue with misunderstanding obligations or ML/TF risk.

We work with AML/CFT supervisors and the FIU to produce joint guidance on matters that are applicable to all reporting entities. We also produce tailored guidance documents, fact sheets, explanatory notes and answers to frequently asked questions specific to the sectors and entities supervised by DIA. We consult with reporting entities via peak bodies and the IAG on draft guidance to ensure it is as useful as possible for reporting entities.

## Monitoring compliance

We use a range of monitoring activities to assess whether reporting entities are meeting their obligations and managing their ML/TF risks. Our monitoring activities help inform our understanding of ML/TF risks and help us determine our regulatory response.

When monitoring compliance, we may focus on a particular entity or across a sector or sub-sector that we supervise, and we may look at specific issues or obligations or consider a broad range of obligations.

The majority of our monitoring activities are **off-site assessments** (i.e. not conducted at a reporting entity's premises) and may involve any, or all, of the following:

- assessment of reporting entity's 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 conferencing.

We also use **on-site inspections** to test the implementation and effectiveness of a reporting entity's AML/CFT policies and procedures and controls in practice. Our on-site inspections are specific to individual reporting entities and may look at a broad range of obligations or we may focus on specific obligations, depending on the ML/TF risks associated with the reporting entity.

An on-site inspection involves us conducting an inspection of the reporting entity at its business premises. On-site inspections range from half a day up to a period of a couple of weeks depending on the size of the business and the scope of the AML/CFT obligations being reviewed.

Appendix B provides a summary of reporting entity obligations against which we monitor compliance.

## Enforcement actions

When reporting entities are not meeting their obligations under the AML/CFT Act, we can follow different courses of action depending on the circumstances specific to each case.

We can request the reporting entity agrees to a remediation plan which sets out the actions they will complete, within a set timeframe, to achieve compliance.

If there is more serious or systemic non-compliance we can:

- Issue a **formal warning**, detailing how a reporting entity is failing to comply with the AML/CFT Act and setting out what the reporting entity will need to do to ensure compliance.
- Accept an **enforceable undertaking** detailing the actions a reporting entity will take to ensure compliance with the AML/CFT Act. If DIA considers that a reporting entity has breached an enforceable undertaking, DIA can apply to the Court for orders to require the reporting entity to comply with the undertaking or pay a penalty.
- Seek restraining or performance **injunctions** and/or **civil penalties** in the High Court.
- Undertake a **criminal prosecution**.

Sanctions for civil liability acts or criminal offences may result in the imposition of:

- civil penalties of up to $200,000 in the case of an individual, and $2 million, in the case of a body corporate, and
- criminal penalties of imprisonment for up to two years or a fine of up to $300,000, in the case of an individual, and $5 million in the case of a body corporate.

## Factors for consideration

When considering whether enforcement action is appropriate, and which enforcement action to use, DIA consider the circumstances of each case including:

- the nature of non-compliance, e.g. the type and severity of the non-compliance, whether it is systemic, intentional, or an isolated/on-off breach
- the ML/TF risk associated with the reporting entity
- the reporting entity's willingness and effort to comply, e.g. compliance history, level of engagement with DIA
- whether the non-compliance was voluntarily reported by the reporting entity[6]
- the intended outcome of the enforcement action.

When considering a matter for prosecution, DIA acts in accordance with DIA's **Prosecution Policy** and the Solicitor-General's Prosecution Guidelines.

6. Voluntary disclosure does not preclude formal enforcement action but is an action we will consider. It may also be relevant to which enforcement action is taken and any penalty considerations.

Appendix A:

# Inherent risk levels of the sectors supervised by DIA

# Financial services

| Sector | Inherent risk of ML/TF | Summary of sector |
|---|---|---|
| **Money remittance** | High | Money remitters facilitate the rapid cross-border movement of funds from and to New Zealand. This includes an ability to transfer funds held in cash, which is accepted as a method of payment by many money remitters.<br><br>Money remitters can be used at all stages of the money laundering process. Criminals can enter money into the financial system (Placement), obscure the trail of dirty money through transfer (Layering), and re-enter the money into the market at the recipient financial system (Integration). This includes in another country. Informal systems of remittance are a particularly high risk of ML/TF. |
| **Virtual asset service provider** | High | VASPs facilitate the exchange of fiat currency for virtual assets, virtual asset for virtual asset, and the administration and safekeeping of virtual assets. The pseudo-anonymous nature of virtual assets allows beneficial ownership to be concealed, with the risks exacerbated by a history of criminals using virtual assets to purchase illegal items, or to store their wealth. |
| **Currency exchanges** | Medium-high | Currency exchanges facilitate the conversion of one currency for another. This often involves cash, including the ability to exchange low value notes for high value denominations that are more easily transportable. These services are attractive to money laundering and terrorism financing. Currency exchange services are often provided alongside money remittance, including the use of exchanged cash to settle remittance transactions, which elevates the level of risk. |
| **Payment providers** | Medium-high | The payment provider sector is broad and includes mobile and internet-based payment systems, digital wallets, electronic money and alternative banking platforms. The sector is rapidly growing, global and technology based, with the potential for cross border movement of funds. These services are attractive for money laundering or terrorism financing. |

| Sector | Inherent risk of ML/TF | Summary of sector |
|---|---|---|
| **Cash transport** | Medium | High volumes of cash being transported, including that of cash-intensive businesses, expose the cash transport sector to misuse for money laundering or terrorism financing. |
| **Non-bank non-deposit taking lenders (NBNDTLs)** | Medium | The NBNDTL sector is diverse, ranging from nationwide lenders, vehicle financing and payday loans, through to micro and social lending. Loans can be obtained, including by fraudulent means, and then repaid with the proceeds of crime. This may include repayments in cash, from third-parties, in full and/or ahead of loan agreement. |
| **Non-bank credit cards** | Medium | The money laundering and terrorism financing risks associated with credit cards are their use for cross-border transactions, ease of transport, and the ability to repay funds using cash or from payments by third parties. |
| **Stored value cards** | Medium | Stored value cards are a means of payment that differ from non-bank credit cards as they hold a prepaid balance that is debited rather than extend a level of credit. Stored value cards, particularly if purchased in bulk, can hold large amounts of value which can be used to facilitate the cross-border movement of funds. This makes them vulnerable to criminal exploitation. |
| **Financial leasing, factoring, debt collection, payroll remittance, safe deposit boxes and tax pooling.** | Low | The overall low risk ratings for these sectors reflect a variety of lower risk factors and vulnerabilities. These include small size, low levels of accessibility, low transactional value, volume and velocity, restricted exposure to higher risk customers and inherent difficulty as a method of money laundering or terrorism financing. |

# Casinos and TAB New Zealand

| Sector | Inherent risk of ML/TF | Summary of sector |
|---|---|---|
| **Casino** | Medium-high | Casinos provide a range of gambling and non-gambling services that are vulnerable to money laundering or terrorism financing. The frequency, volume and value of transactions through a casino, including large cash transactions, may make it difficult to distinguish between legitimate and illicit funds and provides opportunity to transact anonymously.<br><br>Casinos can be used at all stages of the money laundering process. Criminals can place illicitly earned money into the casino and obscure its trail by purporting it for gambling, layering it through the casino system (e.g. through chips, exchange, winnings/ intentional losses or accounts). The illegally-earned money can then re-enter the financial system presented as gambling winnings.<br><br>The use of casino deposit accounts, relationships with other casinos, international players, junkets, currency exchange and international wire transfer services all exacerbate the level of risk. Casinos are also noted as a place where criminals like to socialise, spend and launder their criminal proceeds, which further elevates the level of risk.<br><br>In addition to being the AML/CFT supervisor of casinos, the DIA regulates compliance with the Gambling Act 2003 and sets minimum operating standards regarding the day-to-day running of casinos. |
| **TAB New Zealand** | Medium-high | Similar to casinos, TAB NZ offers a range of gambling and non-gambling services that are vulnerable to money laundering or terrorism financing. The volume and value of transactions through TAB NZ may make it difficult to distinguish between legitimate and illicit funds.<br><br>TAB NZ services can be accessed online, over the phone and through in person transactions, including large cash transactions, across hundreds of retail outlets and locations. Criminal proceeds can be placed into the TAB NZ system, including on account or voucher, appearing to be for betting, be layered and re-enter the financial system as the person's winnings. Betting structures (such as syndicates or aggregating services) can be used to obscure the origin of funds or pool criminal funds with legal funds. |

# Gatekeepers

The trust and company service provider (TCSP), legal, conveyancing, accounting and real estate sectors are captured by the AML/CFT Act as designated non-financial businesses or professions (DNFBPs).

DNFBPs are often referred to as **gatekeepers**. This is because they provide specialist services that can be misused by criminals to facilitate the entry of illicit funds into the financial system. Gatekeepers can be used to create and administer legal persons and arrangements that conceal ownership of money or assets and also to act as a layer between the criminal and the proceeds of crime. At the same time, gatekeepers provide an impression of respectability and legitimacy to the criminals using their services.

When gatekeepers are used by criminals, it also frustrates the ability of law enforcement agencies to detect or investigate money laundering or terrorism financing. The types of services provided across the different gatekeeper sectors vary. So too do the ways that gatekeepers can be misused for money laundering, terrorism financing or other criminal activity.

| Sector | Inherent risk of ML/TF | Summary of sector |
|---|---|---|
| **Trust and company service provider** | High | TCSPs form, administer, act for or otherwise represent legal persons and legal arrangements (such as trusts) on behalf of underlying parties. This includes providing a company or trust formation service, a nominee director, nominee shareholder or professional trustee service, or a registered or virtual office service.<br><br>TCSP services can be used at all three stages of the money laundering process, for the commission of underlying criminal activity including tax evasion, or for terrorism financing. The money laundering and terrorism financing risks primarily relate to the ability to conceal or obscure ultimate beneficial ownership or effective control of companies, limited partnerships or trusts (and other legal persons or legal arrangements). This enables the ownership or transfer of funds or assets to be disguised, the underlying parties involved to be hidden and their financial or other activity to appear legitimate. |
| **Law firms** | Medium-high | Law firms provide various services at risk of money laundering or terrorism financing. This includes TCSP services (see above) and conveyancing, with real estate being a preferred asset for criminals to invest the proceeds of crime.<br><br>In addition, law firms may provide other financial or investment-related services or expertise, which can be misused by criminals. In particular, transactions undertaken for a client through a law firm's trust account, which may include international payments, provides opportunity for visibility of underlying parties to be obscured. |

| Sector | Inherent risk of ML/TF | Summary of sector |
|---|---|---|
| **Accountants** | Medium-high | Accountants provide various services at risk of money laundering or terrorism financing. This includes TCSP services (see above) and investment, business, financial advice, or other services involving the management or processing of financial transactions on behalf of clients.<br><br>These services may be provided alongside, or separate to, accounting services (such as bookkeeping, tax advice and preparation of tax returns). Similar to law firms, some accountants hold trust accounts through which funds may be held or transacted for clients. |
| **Real estate agents** | Medium-high | Real estate agents facilitate the sale and purchase of property and businesses. Real estate is a preferred asset for laundering and to invest the proceeds of crime. In addition, real estate agents have trust accounts, through which deposits for property purchases may be transacted. Payments through trust accounts provide opportunity for visibility of the origin of funds to be obscured, or for laundering through sales that do not proceed. |
| **Conveyancers** | Medium | Conveyancers also facilitate the sale and purchase of real estate, but without the range of other services provided by law firms. This results in a slightly lower level of exposure to money laundering or terrorism financing than the legal sector. |

# High Value Dealers

## Overall risk assessment rating: medium-high

The high-value dealer (HVD) sector includes persons that trade in a range of items including jewellery, watches, precious metals and stones, vehicles and boats, antiquities and fine arts. The sector includes registered auctioneers of these items.

| Sector | Inherent risk of ML/TF | Summary of sector |
|---|---|---|
| **High-value dealers** | Medium-high | The purchase and sale of high-value items is one of the most common and easiest methods of money laundering and terrorism financing, particularly where there is an illicit cash economy. Small items such as precious stones, gold or jewellery hold value and are easily hidden and transported. Many high-value items, including cars and boats, are also desirable to criminals as a way of spending the proceeds of their crime. |

Appendix B:

# Summary of key obligations for reporting entities

# Summary of key obligations for reporting entities

The AML/CFT Act requires reporting entities 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.

A reporting entity 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.

A reporting entity's AML/CFT programme must include its policies, procedures 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 (CDD**) – Some form of CDD (simplified, standard or enhanced) must be conducted whenever a reporting entity establishes a business relationship with a new customer, or if a person seeks to conduct an occasional transaction or an occasional activity with the reporting entity. For most occasions when CDD is required, a reporting entity must obtain identity information and verify this information from reliable and independent sources. A reporting entity must also conduct ongoing CDD and monitor customer activities and transactions to ensure those activities are consistent with its knowledge about the customer and their risk profile.

In higher risk circumstances, a reporting entity must conduct an enhanced level of CDD. This requires the reporting entity to verify the customer's source of funds or wealth or put other measures in place to mitigate the money laundering and terrorism financing risks.

In lower risk circumstances, reporting entities may conduct a simplified level of CDD.

**Suspicious activity reporting** – A suspicious activity report (SAR) must be submitted to the FIU where a reporting entity 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 SAR must be submitted as soon as practicable, but no later than three working days after forming the suspicion.

**Prescribed transaction reporting** – A reporting entity must also report a prescribed transaction report (PTR) to the FIU for certain types of transaction. This applies to any domestic cash transaction of $10,000 or more, or by an ordering or beneficiary institution of an international wire transfer of $1,000 or more. A PTR must be submitted as soon as practicable, but no later than ten working days after the transaction.

**Record keeping** – A reporting entity must keep records of all CDD and transactions undertaken by customers. 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.

**Managing compliance with AML/CFT programme** – An employee of the reporting entity must be appointed as an AML/CFT compliance officer to administer and maintain the AML/CFT programme. The reporting entity must also undertake vetting and training on AML/CFT matters for senior managers, the AML/CFT 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. A reporting entity must also submit an annual report to its supervisor and have its risk assessment and AML/CFT programme audited every three years.

**Note:** High-value dealers have slightly lesser obligations. CDD, record keeping, and reporting obligations only apply to cash transactions of $10,000 or more, or a series of related cash transactions of $10,000 or more.

Te Tari Taiwhenua
Internal Affairs

Te Kāwanatanga o Aotearoa
New Zealand Government