Te Tari Taiwhenua
Internal Affairs

Te Kāwanatanga o Aotearoa
New Zealand Government

Terrorism Financing

Terrorism Financing Risk Summary

Part 1: What is terrorism financing?

Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) reporting entities are required to identify and assess their terrorism financing (TF) risks they may reasonably face and put in place a compliance programme to mitigate risks.

To understand terrorism financing, we first need to understand what a terrorist act is.

Definition: terrorist act

A 'terrorist act' is defined in section 5 of the Terrorism Suppression Act 2002:

1. *An act is a terrorist act for the purposes of this Act if -*
   (a) the act falls within subsection (2); or
   (b) the act is an act against a specified terrorism convention (as defined in section 4(1)); or
   (c) the act is a terrorist act in armed conflict (as defined in section 4(1)).

2. *An act falls within this subsection if it is intended to cause, in any 1 or more countries, 1 or more of the outcomes specified in subsection (3), and is carried out for 1 or more purposes that are or include advancing on ideological, political, or religious cause, and with the following intention:*
   (a) to intimidate a population; or
   (b) to coerce or to force a government or an international organisation to do or abstain from doing any act.

3. *The outcomes referred to in subsection (2) are -*
   (a) the death of, or other serious bodily injury to, 1 or more persons (other than a person carrying out the act):
   (b) a serious risk to the health or safety of a population:
   (c) destruction of, or serious damage to, property of great value or importance, or major economic loss, or major environmental damage, if likely to result in 1 or more outcomes specified in paragraphs (a), (b), and (d):
   (d) serious interference with, or serious disruption to, critical infrastructure, if likely to endanger human life:
   (e) introduction or release of a disease-bearing organism, if likely to cause major damage to the national economy of a country.

A terrorist act advances an ideological, political, or religious cause, that is intended to intimidate a population or coerce a government or international organisation. A terrorist act is not limited to death, and can include damage to property, economic loss, or environmental damage where there is likely risk of serious bodily injury, serious risk to health and safety, or likely to endanger human life.

Definition: financing of terrorism

Under section 5(1) of the AML/CFT Act, 'financing of terrorism' has the same meaning as in section 4(1) of the Terrorism Suppression Act 2002.

Section 4(1) of the Terrorism Supression Act defines 'financing of, or provision of material support for, terrorism' -

> *(a) means an offence against sectiorn 8(1), (1A), (2A), or (2B); but*
> *(b) despite paragraph (a), in sections 18, 68, and 69, means an offence of that kind involving a terrorist act of a kind referred to in section 5(1)(b) or (c).*

Section 8 of the Terrorism Supression Act outlines the elements of a terrorism financing offence:

> *Wilful provision or collection of funds for use to carry out terrorist acts*
> *(1) A person commits an offence if the person provides or collects funds -*
> *(a) directly or indirectly; and*
> *(b) wilfully; and*
> *(c) without lawful justification or reasonable excuse; and*
> *(d) intending that the funds be used, or knowing that, or being reckless about whether, they will be used, in full or in part, in order to carry out 1 or more acts of a kind that, if they were carried out, would be 1 or more terrorist acts.*
>
> *...*
>
> *Wilful provision or collection of funds for use by entity known to carry out or participate in carrying out of terrorist acts*
> *(2A) A person commits an offence if the person provides or collects funds -*
> *(a) directly or indirectly; and*
> *(b) wilfully; and*
> *(c) without lawful justification or reasonable excuse; and*
> *(d) intending that the funds be used, or knowing that, or being reckless about whether, they will be used, by an entity that the person knows is an entity that carries out, or participates in the carrying out of, 1 or more terrorist acts.*
>
> *...*
>
> *Funds or material support need not be used to carry out terrorist act*
> *(3) In a prosection for financing of, or provision of material support for, terrorism, it is not necessary for the prosecutor to prove that the funds or material support collected or provided were or was actually used, in full or in part, to carry out a terrorist act.*
>
> *...*

Terrorism financing is providing or collecting funds for a terrorist act, or to fund activities that support terrorism. It is not necessary to prove that the funds were actually used, in full or in part, to carry out a terrorist act.

Comparison with money laundering

Although money laundering and terrorist financing share many similar methods, there are some differences between them.

Financing of terrorism within New Zealand is likely to be small scale and involve low value of funds compared to money laundering or other illicit financial activities.

	Terrorism financing	Money Laundering
Purpose	money for a criminal act	disguising the illegal origins of criminal profits to spend or fund further criminal activities
Process	1. Raising 2. Moving 3. Using	1. Placement 2. Layering 3. Integration
Source of funds	legitimate and illegitimate sources	illlegitimate sources
What to conceal	the nature of the funded activity	illlegitimate source of money
Methods used	Overlap of methods and financial channels used	

Process: raising, moving, using

Terrorism takes many different forms, including lone actors, small cells, command and control terrorist networks, and corporate groups. Each form of terrorism uses different financing methods - the financial needs of a large terrorist organisation will be very different from those of a small group or lone actor. Despite various methods used, terrorism financing is generally described as having three stages:

- **Raising funds:** Funds are raised through legitimate or illegitimate sources.
- **Moving funds:** Funds need to be moved to the place where they will be used, which often requires funds to be moved internationally.
- **Using funds:** Funds are used to conduct terrorist acts or to fund ongoing expenses and activities that support terrorism.

Raising funds

Common sources of legitimate funding for terrorist groups include membership fees, donations, organising events, and propaganda sales. Often, lone actors or small groups may self-finance their activities through using their own funds in bank accounts or taking out a loan[1]. In some cases, small businesses are established and used to generate revenue to support foreign fighter travel. There is also an emerging trend of raising money through social media content creators rather than through the activities of groups specifically.

Criminal activity identified as terrorism financing methods in the Asia-Pacific region from Australian Federal Agency AUSTRAC's Regional Risk Assessment on Terrorism Financing 2016 include violent robbery, fraud, cybercrime, scams, smuggling and trade of prohibited goods and weapons, trafficking of people and drugs, kidnap for ransom, and extortion. FATF has warned of terrorist groups exploiting COVID-19 by fraudulently raising and moving funds under the guise of humanitarian aid and assistance through legitimate charities or not-for-profits and use the internet to facilitate crowdfunding activities.

1 The Christchurch Mosque attack on 15 March 2019 was entirely self-funded, at a total estimated cost of NZ$60,000. https://christchurchattack.royalcommission.nz/the-report/firearms-licensing/planning-the-terrorist-attack/

Moving funds

Funds can be moved by physically couriering cash or high value commodities, through the international financial system, or alternative mechanisms for moving value. Abuse of not-for-profit organisations and shell companies are common methods of moving funds for terrorism financing.

Using funds

Funds are used to cover travel, living expenses and planning and preparation costs, including acquiring of the items used to facilitate a terrorist attack such as weapons.

Ongoing expenses and activities could include creating propaganda, organising marches and events, maintaining websites, paying legal fees, and establishing safe houses. Some groups provide specialised trainings to members, including in shooting and martial arts. Some pay salaries to members, and send funds offshore to support terrorist activities in other jurisdictions.

Part 2: The New Zealand risk environment

As described in the NZSIS Know the Signs, violent extremism becomes terrorism when a terrorist act is carried out. The violent extremism threat environment includes:

- politically-motivated violent extremism
- faith-motivated violent extremism
- identity-motivated violent extremism
- single issue-motivated violent extremism[2]

The National Risk Assessment 2019 notes that whilst New Zealand is not considered high-risk for terrorism financing, even small-scale financing within New Zealand could have significant impact.

- Our domestic terrorism risks relate primarily to lone actors or small cells for which self-funding has been assessed as the likeliest means of finance.
- Our international terrorism risks include the risk of New Zealanders providing financial support to overseas groups through our financial system and legal structures.

A country can be vulnerable to terrorist financing activity without being at significant risk of a terrorist attack. As described in the IMF publication on *Countering the Financing of Terrorism: Good Practices to Enhance Effectiveness*, terrorism risk and terrorist financing risk are not the same. Terrorism risk refers to the risk of a terrorist attacks occurring. Terrorist financing risk refers to the risk of terrorist funding activity.

New Zealand remains exposed to terrorism financing risk. New Zealand offers access to the global financial system, and funds flowing through New Zealand may appear less suspicious and subject to less scrutiny due to New Zealand's reputation. High levels of financial inclusion and ease of access to financial and non-financial services mean that funds can be easily moved in New Zealand. The comparative ease of doing business in New Zealand means that professional gatekeepers regularly facilitate business activity. Companies can be easily registered in New Zealand, with comparatively loose requirements and low levels of enforcement. Low perception of corruption reduces risk for global business. We have a stable financial system that offers reliability and established expectations of transacting for the safe movement of funds.

2 Single issue terrorism is a form of terrorism that focuses on a specific, singular issue instead of more encompassing social, political, or religious change. Examples of single-issue motivated terrorism includes acts of violence by anti-abortionists, animal rights activists, and environmentalists https://ctc.usma.edu/terrorist-groups/single-issue-terrorism/.

Part 3: Common vulnerabilities

AML/CFT regulated sectors can be used to raise funds, move funds, and use funds throughout the terrorism financing process. The following are common vulnerabilities that have been identified across DIA's supervised sectors.

Accessibility to funds: Some of our reporting entities provide an easy way to gain fast access to large sums of legitimate money that can be used to support terrorist activity. Some sectors have no oversight on where funds may be spent or transferred to.

Anonymity: Our reporting entities can increase anonymity and obscure the source and destination of funds. Some also offer prepaid accounts or instruments that are unattached to an established account with a financial institution and can be regularly reloaded remotely and anonymously by third parties. Anonymity makes it difficult to trace transactions.

Borderless: Some of our reporting entities can be accessed globally and enable transfer of funds domestically and internationally. This provides an avenue to financially support domestic and overseas terrorism, and enables offshore supporters to provide financial support to New Zealand actors and groups.

Circumvention of the formal banking system: Some of our reporting entities provide opportunities for co-mingling with legitimate financial transactions outside of the formal banking system. This avoids scrutiny from the formal banking system and there are less opportunities for oversight, scrutiny, and detection of suspicious activities.

Criminal use: Some sectors are used by criminals and organised-crime groups for illicit activity, such as scams and extortion. As criminal activity can be a method of raising funds for terrorism financing, sectors that are commonly used by criminals could increase exposure to terrorism financing risk.

Ease of access: It is generally easy to onboard customers and conduct transactions. Many of our reporting entities engage in non-face-to-face business relationships and transactions, such as online, phone, and mobile. Some services can be accessed by customers through third-party businesses without direct interaction with reporting entities. This may include on-boarding of overseas clients, intermediaries, and the use of other professional services/gatekeepers.

Gateway to the international financial system: Our reporting entities offer an entry point into the international financial system and provide a layer to obfuscate illicit financial activity. New Zealand's reputation means that funds moving through New Zealand may appear less suspicious and subject to less scrutiny.

Knowledge gaps: New Zealand is not traditionally associated with terrorism financing, and there is a general lack of understanding of terrorism financing risks. The lack of public awareness of terrorism financing is attractive as suspicious activities and transactions may be less likely to be detected and reported. Reporting entities may be less likely to look for terrorism financing or recognise it. Businesses not registered as an AML/CFT reporting entity may have no or limited awareness of terrorism financing risks or their AML/CFT obligations.

New technologies: Business relationships in some of our reporting entities are typically non-face-to-face. Electronic, online, and new payment methods and products can be accessed globally and used to transfer funds quickly. Online business relationships may be appealing to individuals and terrorist groups who radicalise, recruit, and communicate online.

Obfuscation: Our reporting entities can be used to hide the identity of beneficial owners, illicit origins of funds or conceal where funds are going to.

Part 4: Key AML/CFT requirements

The following are some key AML/CFT requirements that reporting entities that are vulnerable to terrorism financing risk should be aware of. ***It is not an exhaustive list of AML/CFT requirements.***

Risk assessment

As highlighted in Part 1, although money laundering and terrorist financing share many similar methods, there are some differences between them. Many AML/CFT risk assessments assess money laundering and terrorism financing risks as the same when they are conceptually different risk categories.

Country risk: Jurisdictions with poor AML/CFT controls are likely to be attractive for terrorism financing. Finance and trade hubs in regions affected by terrorism, or jurisdictions bordering conflict zones, may also act as conduits for terrorism financing. Reporting entities should consider not only high-risk countries but also their neighbouring countries, as terrorism financing often involves the movement of funds across borders.

Methods of delivery: Non-face-to-face business relationships are attractive for terrorism financing purposes as they obfuscate transacting parties' identities. Reporting entities should apply increased identity verification measures where there is increased terrorism financing risk.

Nature, size and complexity: Our reporting entities have varying levels of risk profiles, size, resources and sophistication for detecting and monitoring terrorism financing activity. There may also be a perception that smaller reporting entities are less likely to be able to detect terrorism financing than larger and well-resourced institutions. Some of our reporting entities process a large volume of transactions that can make detection of suspicious transactions difficult.

Products and services: Our reporting entities offer a range of products and services that can be used to create complex layers or distance between an individual and their intended use, which hides suspicious activity. Financial institutions may offer international money transfer and exchange services to high-risk jurisdictions. They can also be a source of legitimate funds, or facilitate the movement of funds, for terrorism activity. Designated non-financial businesses can act on behalf of a client, providing a false impression of legitimacy. They also facilitate the setting up of legal structures to hide the identity of the beneficial owners such as companies, trusts and charities. Trust accounts can be used to hide funds from scrutiny.

Compliance programme

Any terrorism financing risks identified in your risk assessment should be mitigated through policies, procedures, and controls in AML/CFT programmes.

The following are examples of obligations reporting entities should review and are not exhaustive:

Customer due diligence (CDD): It is important reporting entities identify and verify their customers identity using independent sources, and assess any relevant terrorism financing risks when onboarding, such as whether the customer is based in, or transacting with, a high-risk jurisdiction. Gathering good information on the nature and purpose of the business relationship and expected patterns of transaction/activity will help you identify any unusual or suspicious activity.

Enhanced due diligence: There are various circumstances where enhanced customer due diligence is required. Reporting entities should be identifying and verifying the source of wealth or funds of their customers where the level of terrorism financing risk posed is greater. If reporting entities are unable to complete enhanced CDD on a customer, they must not carry out any occasional transaction or activity for them, nor establish a business relationship with them. If a reporting entity already has a business relationship with the customer, this must be terminated.

Ongoing due diligence: Not all terrorism financing risk factors will be apparent at onboarding and may emerge only once business relationships have been established. Adverse information, such as media reports, linking customers to possible violent extremism, could increase terrorism financing risk. Reporting entities should consider implementing checks on customers and transacting parties against the list of all individuals and entities subject to counter-terrorism sanctions regimes on the New Zealand Police website and notification updates via goAML.

Politically exposed persons: Some terrorist organisations have been, and continue to be, financially supported by states. PEP customers from jurisdictions known to support terrorism could increase terrorism financing risk.

Staff training: Reporting entities should maintain awareness and training in terrorism financing as the dynamic nature of the risk environment changes. Reporting entities should also ensure that their AML/CFT measures are both adequate and effective as the risk environment changes.

Suspicious activity reporting: One of the most important ways of preventing and detecting terrorism financing is through reporting information to the Police Financial Intelligence Unit. This ensures relevant agencies can investigate, mitigate, and manage threats to keep New Zealand safe from a terrorism incident.

Transaction monitoring: Conducting transaction monitoring and reviewing this information against existing knowledge of customers and their established and expected transactions and activity will assist in identifying potential terrorism financing red flags. Reporting entities should investigate unusual transaction patterns and account activity, and any possible references of alpha-numerical terms or combinations associated with violent extremist ideologies.

Wire transfers: Customer due diligence requirements for wire transfers are designed to enable information on the parties to a wire transfer to be immediately available to hinder the anonymous use and misuse of wire transfers by financiers of terrorism.

Part 5: Red flags

Money laundering and terrorism financing share many red flags. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of terrorism financing but could prompt further monitoring and examination. A customer may be able to provide an explanation to justify the red flag indicator.

Examples of red flags may include:

Customer behaviour

- Customers emptying out bank accounts and savings, sale of assets including personal belongings
- Customers utilising financial services at retailers to buy equipment that could be used for terrorist activity
- Funds received from and sent to unrelated businesses that do not align with the client's business profile, including an absence of regular salary payments and business-related activity
- Multiple customers using the same address or phone number
- Parties to the transaction are linked to known terrorist organisations, entities or individuals that are engaged, or suspected to be involved, in terrorist activities
- Requesting multiple cards linked to common funds or purchasing multiple stored-value cards
- Use of false identification or fraudulent documents

High-risk jurisdictions

- Funds transfers to multiple beneficiaries located in high-risk jurisdictions
- Multiple customers conducting funds transfers to the same beneficiary in a high-risk jurisdiction
- Parties to the transaction are based in countries or returning from conflict zones known to support terrorist activities
- Transfers to and from high-risk jurisdictions, at multiple branches of the same reporting entity
- Vague justifications and a lack of documentation for requests to transfer funds to high-risk jurisdictions or entities

Transaction monitoring

- A sudden increase in business/account activity, inconsistent with customer profile
- Absence of expected transactions such as regular income or unemployment benefits, normal debit and credit account activity and/or paying bills
- Numerous and frequent transfers into personal account described as donations, humanitarian aid, or similar
- Transactions referencing numerical combinations or terms associated with terrorist ideologies
- Transactions to accounts associated with known terrorist organisations, entities or individuals that are engaged, or suspected to be involved, in terrorist activities

ENDS

Disclaimer

Note: This document is intended to provide an overview of terrorism financing risk factors relating to sectors supervised by the Department of Internal Affairs. It does not assess every terrorism financing risk that sectors may reasonably expect to face in the course of its business. It does not set out the comprehensive obligations under the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009, associated regulations and codes of practice. It does not constitute, nor should it be treated as, legal advice or opinion. The Department of Internal Affairs (DIA) accepts no liability for any loss suffered as a result of reliance on this publication.

Version history

Version	Date	Author	Description of changes
1.0	03/11/2022	Department of Internal Affairs	Initial version
2.0	05/07/2024	Department of Internal Affairs	Design format