

# New Zealand's Latest Risk Assessment Will Trigger AML/CFT Programme Reviews

By [Nathan Lynch](#), Regulation Asia

Published on 20th March 2025

**New Zealand's latest National Risk Assessment should act as a trigger for organisations to review their risk assessments, internal systems and controls, writes Nathan Lynch.**

Banks and other reporting entities will need to review their AML/CFT compliance frameworks in view of New Zealand's latest **[National Risk Assessment \(NRA\)](#)**, which is the first such update in more than five years. The New Zealand Police Financial Intelligence Unit (FIU) has detailed a rapidly changing threat landscape, with fraud and cybercrime rising amid more traditional risks such as drugs and transnational organised crime. The latest risk assessment is also the first to include a nation-wide Proliferation Financing Risk Assessment, which is now a requirement from the Financial Action Task Force (FATF).

Businesses that are subject to the AML/CFT regime need to consider changes to the national risk profile when assessing their own organisational risks. NRAs are a fundamental tenet of the AML/CFT framework, as they form a baseline for reporting entities to consider the specific threats that they need to manage and mitigate in their operations. As such, the release of the latest NRA should act as a trigger for organisations to review their risk assessments

and adjust their internal systems and controls in response to any changes.

## **Rising risks**

The latest NRA underscores the vulnerabilities in New Zealand's financial system, particularly with regard to the rising challenges associated with fraud, scams and the criminal exploitation of government welfare programmes.

The NRA identified the proceeds of crime — primarily from drug trafficking, fraud, and tax evasion — as flowing through both traditional and emerging digital channels. Real estate, trusts and cash-intensive businesses remain prime vehicles for laundering illicit funds, exploiting gaps in oversight, and threatening New Zealand's reputation as a stable, low-corruption jurisdiction. The report highlights how criminals are increasingly using professional facilitators (such as lawyers and accountants) to obscure the origins of dirty money and avoid AML/CFT controls.

This has sent a clear message to so-called Phase 2 reporting entities to ensure they have an appropriate AML/CFT compliance programme in place. A change in the national risk framework is likely to flow through to compliance and enforcement priorities, particularly with the FATF's fifth round mutual evaluations underway.

Terrorism financing, while less prevalent, is also an ongoing concern for New Zealand authorities. The FIU says New Zealand's exposure is largely linked to small-scale, domestic self-funded cells, rather than large international networks. There is also an ongoing risk of funds being funnelled overseas to support foreign terrorist groups, fuelled by online radicalisation and crowdfunding platforms. The report called for reporting entities to exercise greater vigilance as global geopolitical tensions amplify these threats.

## **A pandemic of fraud**

A clear theme of the report is the rapid rise of scams and technology-driven financial crime.

As with many similar countries, New Zealand has been experiencing a post-Covid surge in fraud and scams with cumulative losses estimated to exceed NZD 2 billion. Fraud is now the most common type of offence reported to the NZ Ministry of Justice's crime and victims survey.

New Zealand financial crime barrister Gary Hughes, of Britomart Chambers, endorsed this recognition of the scale and impact of fraud.

"Although this Police NRA document is many months overdue, it is pleasing that it finally recognises what those of us in the field — or those poor individuals hit by ever-increasing scams — have known for years. Fraud deserves to be in the top-tier of risks and criminal threats. We need to have all the guns of the anti-money laundering system trained on it," Hughes said.

Online commerce has enabled fraud on a scale never seen before, and greater sums are being lost to more sophisticated financial scams, he added. Many of these scams are perpetrated from overseas with a local bank account or money mule potentially involved. Hughes, who has acted for financial institutions as well as groups of fraud victims, pointed to the public exposure of up to 30 cases involving New Zealand victims.

"This includes the well-educated and business-like — even a former MP — losing hundreds of thousands of dollars in very convincing investment scams," Hughes said.

The largest of those involved losses of around NZD 1.7 million, most of which was sent offshore with the help of a local Whanganui money mule. Another case involved a Justice of the Peace (JP) who was charged with money laundering after allegedly acting as a money mule.

“There seems no shortage of people willing to rent their bank account out, for a small cut, before the bulk of the money is wired abroad,” Hughes said.

In emphasising the fraud problem the latest NRA is, in effect, telling AML reporting entities to prioritise this issue when assessing their own risks. As such, they will be expected to pay closer attention to the problem.

Hughes said this was only the beginning of a turnaround, with much more work still to be done.

“It’s encouraging that the FIU is starting to grasp the nettle here but it also highlights fundamental problems in our systemic approach to fraud. Until recently, the banks have not been bothered to implement even basic account payee matching into online banking systems. Plus, we do not have a National Anti-Scam Centre like Australia, and only a voluntary ad hoc compensation scheme. The industry self-regulatory Banking Ombudsman Scheme has shown itself to be hopelessly out of depth on victim compensation disputes,” Hughes said.

“On top of that, at an ordinary policing level I have seen some appalling apathy among regular units towards scam victims. That can lead to slow, inadequate or poorly done prosecutions — even where there is a defendant mule in the jurisdiction. So the Police FIU’s message still faces a huge challenge to filter through to their front-line police responses.”

## **Digitising financial crime**

In keeping with the prominence of fraud in New Zealand’s top-tier threats and vulnerabilities, cryptocurrencies are cited as a growing area of risk. Digital assets offer greater speed and anonymity than traditional banking channels and are often linked to laundering the proceeds of scams. Cybercrime, particularly phishing and ransomware, is also on the upswing, generating proceeds that feed into money laundering schemes. As with AUSTRAC in Australia, the

New Zealand supervisors are likely to increase their focus on digital asset exchanges in response to these changes in the risk landscape.

The NRA warned that New Zealand's payments infrastructure, while advanced, is increasingly becoming a target for exploitation. Some of the most vulnerable sectors include money transfer services, money remitters and digital currency exchanges.

"This NRA identifies that fraud-related crime, drug crime and transnational money laundering are the highest threat, with fraud accelerating and seeing both 'defrauding' and the subsequent 'laundering' occurring within the financial system," the Reserve Bank of New Zealand (RBNZ) said in a [statement](#).

"This means the banking sector remains highly vulnerable to money laundering, along with any sector that offers services and products enabling movement of proceeds out of or into New Zealand."

In keeping with this messaging, banks operating in New Zealand will need to review their controls in response to the material in the latest NRA.

## **Nuclear proliferation risks**

On the proliferation financing (PF) front, the assessors found that New Zealand is not considered a "high-risk" jurisdiction. Despite this, the economy is "well-integrated and connected to the global financial system", which creates a risk of exploitation from rogue nation-states such as North Korea and Iran, which are pursuing nuclearisation in defiance of international sanctions.

Banks and other reporting entities will now need to incorporate this into their own AML/CFT frameworks.

“We must ensure our financial system is not misused to fund the development and manufacture of weapons that threaten global safety and security,” the report says.

Reporting entities that fail to incorporate a PF risk assessment are likely to face scrutiny during upcoming supervisory visits, particularly if they are exposed to cross-border value transfers.

Hughes, who works as a trans-Tasman expert across NZ and New South Wales matters, draws attention to the challenges reporting entities will have in making this meaningful.

“Just like in Australia, PF analysis and documentation is now required by the FATF, but it will be such an uphill battle to make those risks and concepts meaningful for SME reporting entities in either country. Particularly with the new Australian Tranche 2 entities, who will take months to get themselves acquainted with even domestic drugs, organised crime or fraud risk measures – how on earth do you make the geopolitical risks of nuclear weapons proliferation relevant and meaningful? It will be challenging to have anything inserted in their compliance programs about PF that isn’t just waffle or regurgitation,” Hughes said.

### **Next steps in the battle**

The FIU has also called for stronger collaboration between the public and private sectors, emphasising that intelligence sharing will be critical to staying ahead of increasingly sophisticated criminal groups.

Looking ahead, the New Zealand Police said demand for illicit drugs would remain a major law enforcement priority in the country, which creates an ongoing ML/TF risk for businesses. In addition, high-tech advances such as generative AI will continue to be exploited by criminal entities, which needs to be considered in risk assessments.

“The increased prevalence of fraud will see more reporting entities and customers becoming victims. NZ is likely to remain a

marketplace of choice for foreign transnational serious organised crime groups to launder funds,” the police said.

Usually a National Risk Assessment in New Zealand would be followed by ‘Sector Risk Assessments’ from each of the three AML/CFT supervisors. With supervision due to be consolidated into the Department of Internal Affairs, potentially in 2026, it remains unclear whether anything will be published in the meantime.

### **Key considerations for reporting entities:**

- Have you appointed someone to review the latest NRA and consider the findings in the context of your business?
- Do you need to update your AML/CFT programme in response to key changes in the national risk landscape?
- Have you included proliferation financing risks in your organisation’s risk assessment?
- Have you documented these risks in your AML/CFT programme, and are you managing and mitigating these risks through your internal controls?
- Are you taking measures to address the rising risk of scams, including the potential laundering of proceeds of financial crime through your organisation?
- Does your organisation’s training programme need to be revised in view of the new NRA?

—

*Nathan Lynch is a financial crime writer who has spent two decades investigating the hidden world of dark money that fuels organised crime, corruption and violent extremism. Nathan has trained police, government officials and bankers across Asia and the Middle East on the techniques the world’s criminals use to conceal their dirty money.*