COUNTER FRAUD CENTRE
Tauārai Hara Tāware

Fraud Risks in Government Funded Initiatives

JULY 2023

Table of contents

1 Introduction

For the purposes of this guide government funded initiatives are defined as any public sector financial support (e.g. grants, funding, and subsidies) provided to individuals or organisations.

- **Grant** typically refers to a sum of money given by the government, an organisation, or institution to an individual, group, or entity for a specific purpose. Grants are usually awarded based on merit, need, or compliance with certain criteria. They are often non-repayable and are intended to support projects, research, education, or social initiatives.
- **Subsidy** is a financial aid provided by the government or an organisation to support specific industries, sectors, or activities. Unlike grants, subsidies are typically given to businesses or individuals to offset costs or encourage certain behaviours. Subsidies can be in the form of cash payments, tax incentives, reduced prices, or other financial benefits.
- **Funding** is a broader term that encompasses both grants and subsidies. It refers to the provision of financial resources to support projects, programmes, research, or initiatives. Funding can come from various sources, including governments, private organisations, philanthropists, or crowdfunding platforms. It can be in the form of a grant, subsidy, loan, investment, or sponsorship.

These initiatives play a vital role in supporting research and innovation, community projects, business development, education, and arts and culture.

Although this funding is intended to provide benefit(s) to the public, it can be exploited through fraudulent means. This risk is greater during times of crisis/disaster when programmes are administered under time pressure. There is also a greater risk of fraud when funding is administered with limited oversight or through a new system or process.

To minimise the opportunity for fraud against funding programmes, organisations should ensure staff are aware of the common fraud risks and the countermeasures that are effective within their organisation.

1.1 Purpose of this guide

Understanding fraud risks in government funded initiatives can help organisations to identify and prioritise countermeasures to implement to help mitigate these risks. This guide provides examples of these fraud risks and examples of countermeasures to prevent, detect and respond to them.

2 Administering government funded initiatives

Fraud risks in government funded initiatives refers to the possibility of fraudulent activity occurring in the administration of the initiative.

Examples of fraud risks include:

- **False representation:** using false or misleading information to support a government funded initiative application or report. This could include falsifying documents or inflating costs.
- **Misuse of funding:** using funding for purposes other than those that were applied for, or which were not the intended use of the funding. This could include unauthorised spending or using the money for personal expenses.
- **Double dipping:** claiming funding for the same purpose from more than one funding organisation.

Examples of fraud risks and countermeasures to mitigate these risks are contained in section 3 of the guide.

These risks increase when fraudsters have the motivation, opportunity, and rationalisation to commit fraud. These three factors are known as the fraud triangle.

2.1 The benefits of preventing fraud in government funded initiatives

Fraud has an impact on the lives of the every one living in Aotearoa New Zealand. Fraud may involve the theft of a person's identity or otherwise threaten their financial security. It reduces the government's ability to deliver services and provide support to those in need. Public funds that are taken away from essential public services and support can impact the integrity of public sector programmes and functions, as well as helping to fuel other serious crime. Specifically, fraud against government funded initiatives can be particularly attractive to organised crime groups, given the large amount of funds involved.

Surveys done by the Government along with other research does not provide a complete view of exposure to fraud in New Zealand government programmes. Based on international estimates and comparisons, the cost of fraud and error in New Zealand could be between 0.45% and 5.7% per annum. The loss to the taxpayer of that country could be as much as $570 million per annum[1].

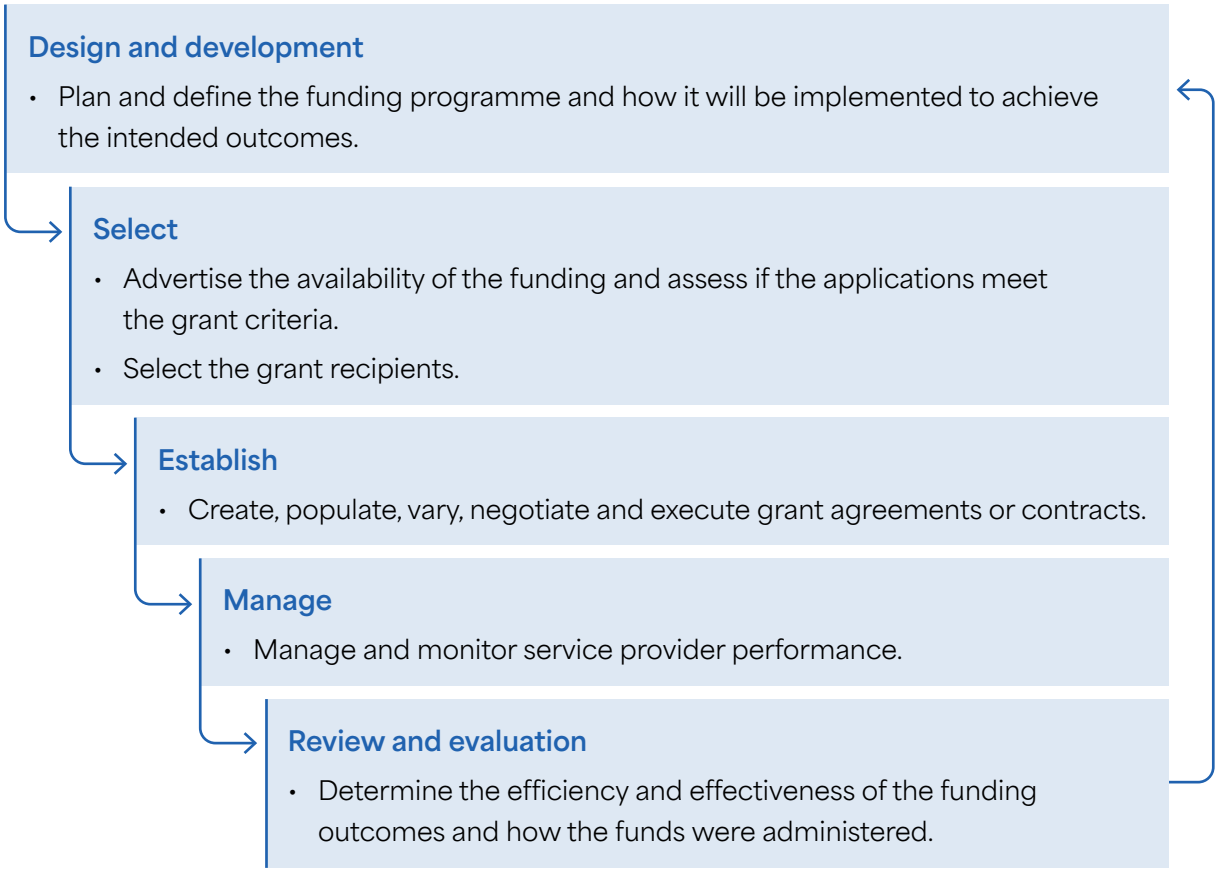
1 Calculated by applying 5.7% to $10 billion grant funding from 1 July 2021 to 30 June 2022.

As well as providing financial benefits, investing efforts in fraud prevention may also result in non-financial benefits across the public sector of New Zealand, such as:

- Improved effectiveness and integrity of programme delivery by helping to ensure government funded initiatives are delivered to groups and/or individuals who need them.
- Reduced administrative burden on the public sector. Responding to fraud can take significant effort through audits, inquiries, investigations, recovery, and prosecutions.
- Assuring New Zealanders that public sector organisations are serious about protecting the integrity of programmes and functions funded by the government.
- Protecting vulnerable New Zealanders. Those who rely on public services and support such as the elderly, the sick and the vulnerable are often the ones most harmed by fraud. This can have a devastating and compounding effect on victims, amplifying the disadvantage, vulnerability, and inequality they suffer.

2.2 Funding lifecycle

Fraud risks in government funded initiatives should be considered and continuously updated through the funding lifecycle. Countermeasures to reduce fraud should likewise form part of the thinking process throughout the funding lifecycle. The next section contains examples of fraud risks for government funded initiatives and the stage of the funding lifecycle at which they are most likely to occur.



2.3 How to identify fraud risks for government funded initiatives

A useful technique to identify fraud risks is to 'think like a fraudster'. The fraudster personas developed by the Counter Fraud Centre can help to recognise fraud risks throughout the funding lifecycle. In the subsequent sections of this guide, we had identified which fraudster persona is most likely to act on the fraud risks identified.

You can also use the fraudster personas to help identify other fraud risks within your funding initiatives, which may not be covered in this guide. Consider each persona and how they might defraud your programme.

The Fabricator invents or produces documents/ information that is false to dishonestly gain a personal benefit or a benefit for another person.

The Corruptor abuses their position of entrusted power to gain a benefit for themselves or another person.

The Impersonator pretends they are another person or entity to dishonestly gain a benefit for themselves or another person.

The Deceiver makes others believe something that is not true to dishonestly gain a benefit for themselves or another person.

The Enabler knowingly enables fraudulent activity to dishonestly gain a benefit for themselves or another person.

The Organised are groups which use the combination of methods in a planned coordinated way to dishonestly gain a personal benefit.

The Exploiter uses something for a wrongful purpose to dishonestly gain a benefit for themselves or another person.

Another useful technique to identify fraud risks is being able to recognise red flags. Red flags of fraudulent behaviour can be an indicator of a particular problem requiring attention, and which should be investigated further. This guide provides examples of red flags in Section three.

For more information about identifying fraud risks refer to our Fraud Risk Assessment Guidance.

For more information about the fraudster personas, and how to recognise and mitigate against their behaviours, refer to the Counter Fraud Centre Fraudster Persona Guidance.

2.4 How to mitigate fraud risks in government funded initiatives

An organisation's risk management practices usually include guidance about how countermeasures should be implemented to help prevent, detect and respond effectively to fraud. No system of countermeasures can completely eliminate fraud, however well-designed countermeasures can assist in deterring and detecting fraudulent activity and help to mitigate against such risk.

This guide provides examples of countermeasures that might help organisations to manage the identified fraud risks.

For additional examples of countermeasures refer to the CFC Countermeasure guides on the SFO website.

2.5 Key definitions

These are some of the key definitions throughout this guide.

Countermeasures

Also known as controls. The individual measures and processes that help agencies prevent, detect and respond to fraud. A collection of countermeasures makes up a control environment.

Fraud

The deliberate use of deception or dishonesty, to obtain a benefit or cause a disadvantage or loss to another person or party.

Fraudster personas

A collection of tried and tested methods that fraudsters commonly use when committing a fraudulent offence. Personas are useful to understand how fraudsters think and can help an organisation to put effective countermeasures in place.

3 Fraud risks in government funded initiatives

The table below lists some of the most commonly observed fraud risks in government funded initiatives, however it should not be taken as an exhaustive list. It indicates the stage of the funding lifecycle where the fraud risk is most likely to occur. Information about the associated fraudster personas, red flags and countermeasures relating to each risk are detailed in the following section. Case studies are also provided to show examples of how funding fraud occurred in New Zealand.

	Fraud risk type	Examples [Described using the actor, action, outcome format]	Design & development	Select	Establish	Manage	Review & evaluation
Applicants/ Funding recipients	3.1 Identity crime	Funding recipient uses false identity(ies) to apply for funding or receive payments.		✓	✓	✓	
	3.2 Fictitious organisation	Applicants create a fake organisation or shell company to apply for funding and pretend they are eligible.		✓	✓	✓	
	3.3 False information	Applicants fabricate eligibility information to receive funding. Recipients falsify performance data or mispresent the project status to continue to receive funding.		✓	✓	✓	✓
	3.4 Funds used for improper purpose	Funding recipients use funding for operating another business for which the funding was not intended or for personal gain. Funding recipients use funds for expenditure in contradiction with the funding criteria.				✓	✓
	3.5 Inflating costs	Funding recipients inflate costs for delivering a funding outcome or service to receive additional funding.		✓	✓	✓	

	Fraud risk type	Examples [Described using the actor, action, outcome format]	Design & development	Select	Establish	Manage	Review & evaluation
Applicants/ Funding recipients	3.6 Substituting materials	Funding recipients use cheaper and substandard products, materials, service models or a service type contrary to the funding agreement to receive a financial benefit.			✓	✓	✓
	3.7 Duplicate applications/ funding	Funding recipients apply for and receive funds from multiple different programmes for delivering the same service or bill more than one fundingfunding initiative for the same work.	✓	✓		✓	✓
Public Officials	3.8 Corruption	A public official exploits their position of trust, insider knowledge or authority to manipulate systems and processes for personal gain/the gain of the funding recipient.	✓	✓	✓	✓	✓
	3.9 Undeclared conflict of interest	A public official influences the selection of a funding recipient who is a friend or family member to obtain a personal benefit or a benefit to the funding recipient.	✓	✓	✓	✓	✓

3.1 Identity crime

Summary

Funding recipients use a false identity(ies) to apply for funding payments.

Fraudster Personas

The Impersonator

The Organised

The Fabricator

Red flags

- Identification documents appear to be altered or forged.
- Address or name does not match the information on the supplied identification.
- Other information, such as birth date, is different from information previously provided by the individual or that is already on file.
- Identifying information is the same as information provided by another individual.
- An individual refuses to provide identifying information.

Countermeasures

- Require applicants to provide certified copies of identification (passport, birth certificate, driver's license) and verify these using RealMe Identification.
- Use the Companies Office Register to verify the business details provided by applicants.
- Collect relevant data and match data against existing records.
- Conduct open-source checks, or 'digital footprint checks,' for publicly available information.
- Verify the identity during each interaction to confirm the person owns the record they are trying to access.

3.2 Fictitious organisations

Summary

Applicants create a fake organisation or shell company to apply for funding and pretend they are eligible.

Applicants may falsify information or documents to legitimise the fictitious organisation.

Fraudster Personas

The Organised

The Impersonator

The Deceiver

Red flags

- Organisation documents that appear to have been altered or forged.
- Organisation information, such as address, is different from publicly available information.
- Information is different from information previously provided or that was already on file.
- Identifying information is the same as information provided by another organisation.
- The organisation was created after the funding was advertised.

Countermeasures

- Collect relevant data and match data against existing records.
- Require mandatory information to complete requests or claims.
- Use the Companies Office Register to access data to identify and verify business details.
- Conduct open-source checks, or 'digital footprint checks,' for publicly available information.
- Automatically match data with another internal or external source to obtain or verify relevant details or supporting evidence.

3.3 False information

Summary

Funding applicants must meet a set of criteria to be deemed eligible to receive funding. Applicants may falsify information to qualify for funding, such as by falsifying financial statements to establish the need for funding or by falsifying the organisation's capacity to deliver the programme or function.

Fraudster Personas

The Enabler

The Deceiver

The Fabricator

Red flags

- Insufficient justification or documentation for applications.
- Funding recipients that do not respond to requests for additional information or documentation.

Countermeasures

- Verify information received with an independent and credible source and reconcile records.
- Publish funding recipients' details to allow the public to identify fabrications or falsehoods.
- Perform due diligence checks to:
  - confirm accreditations with professional boards and organisations.
  - collect relevant data and match data against existing records.
  - conduct open-source checks for publicly available information.
  - carry out quality assurance checks of funding programme activities and outcomes.
- Include a statement in the application that the information provided may be shared for the purposes of prevention and deterrence of financial crime.

3.4 Funds used for improper purposes

Summary

Funding that is spent for improper purposes and outside of it's intended use. For example, funding recipients may dishonestly spend funding on personal items or other companies.

Fraudster Personas

The Exploiter

The Enabler

Red flags

- Funding recipients that provide inconsistent or illogical explanations about how funding is being used.
- Vague or limited reporting about the use of the funding.
- Funding recipients that ignore requests for information about funding use or display aggressive behaviour following any questions about appropriation.
- Appropriation information that does not align with previous reporting.

Countermeasures

- Define the funding activity deliverables in the funding agreement.
- Define ineligible expenditure and/or activities in the funding guidelines and funding agreement.
- Apply parameters or limits on funding payments, such as scheduled payments.
- Specify reporting requirements (including for subcontractors) and proportionate acquittal procedures.
- Assess reported information against objectives and appropriate benchmarks to confirm the spending was appropriate.
- Require funding recipient or subcontractors to provide receipts and records that can be reconciled against funding conditions.
- Identify and recover fraudulent payments or debts owed by funding recipients.

3.5 Inflating costs

Summary

Funding recipients may inflate costs to receive additional funding. Applicants might also falsify records, inflating the amount of funding required to achieve the agreed funding outcome. Recipients might also deliver a lesser quality or quantity of product or service to increase the amount of funding they can retain. They may also change the date of invoices to make activities appear as if they fall within the funding criteria.

Fraudster Personas

The Enabler

The Deceiver

Red flags

- Rising costs with no apparent reason for the rise.
- Alterations or forgeries of cost reports/invoices.
- Claims for costs outside of the norm for the outcome sought.
- Supporting documentation for claims is not available or supplied on request.

Countermeasures

- Define expectations of all parties in relation to the funding.
- Define ineligible activities and ineligible expenditure clearly.
- Monitor the performance of how the funding is applied to assess that the objectives have been achieved.
- Require funding recipients and subcontractors to keep records of expenditure.
- Require funding recipients to provide reliable, timely and adequate evidence to demonstrate that the funding has been used in accordance with the terms and conditions of the funding agreement, and regularly review that evidence.
- Verify reasonable labour costs or hours with an independent and credible source.

3.6 Substituting materials

Summary

Funding recipients might deceptively use cheaper or substandard products, materials, service models or service type to receive a financial benefit. For example, individuals may receive funding to have home insulation installed, however the product used as part of the insulation process is inferior to the standard agreed. Duplicate applications/funding.

Fraudster Personas

The Exploiter

The Enabler

Red flags

- Unusual financial trends may indicate that suspicious transactions, including fraud, are taking place.
- Apparent substandard materials.
- High maintenance and repair costs.
- Discrepancies between product specifications and actual appearance.
- Early or frequent repairs or replacements.

Countermeasures

- Funding agreements that are well-drafted, fit-for-purpose, and clearly document the expectations of all parties in relation to the funding.
- Ongoing communication, active fund management, and performance monitoring requirements, which are proportional to the risks involved.
- Require funding recipients to provide reliable, timely, and adequate evidence to demonstrate that the funding has been used correctly.
- Access to and inspection of products and materials are agreed to in the funding agreement.

3.7 Duplicate applications/funding

Summary

Duplicate funding can occur where a funding recipient is able to obtain funding for the same or similar activity from more than one source.
This may involve fraud if the respective fundings are not intended to apply simultaneously, and the funding recipient fails to declare the other funding.

Fraudster Personas

The Deceiver

The Organised

The Enabler

Red flags

- Applications for the same project to different funding sources.
- Applications with similar or identical project descriptions and/or objectives.
- Multiple applications with inconsistent budgets may indicate an attempt to secure higher funding amounts from different sources.

Countermeasures

- Consider other sources of funding when designing funding initiatives to identify the possibility of duplicate applications/funding.
- Require the funding recipient to declare other contributions as part of funding agreement.
- Conduct data matching activities to verify declarations about other contributions are accurate, such as:
  - using data already held within your organisation about other funding payments.
  - using and disclosing information with other government organisations to prevent or detect funding recipients receiving duplicate funding for the same service (information sharing).

3.8 Corruption

Summary

A public official may exploit their position of trust, insider knowledge or authority to manipulate systems and processes for personal gain. The outcome does not necessarily need to result in a financial gain for the official. Internal exploitation could include awarding funding to ineligible applicants to meet performance targets.

Fraudster Personas

The Exploiter

The Enabler

The Organised

Red flags

- Funding applications submitted suspiciously quickly after funding is first advertised.
- Corresponding personal details, like address or contact number, of public official and funding recipient.
- Funding recipients receiving more than the entitled funding payments.

Countermeasures

- Establish solid governance structures and clear accountability for all parties involved.
- Establish effective internal whistleblowing avenues.
- Develop guidance that clearly sets out who the decision-makers are for different funding administration processes.
- Establish internal control mechanisms such as rotating staff in high-risk positions, separating duties and randomly allocating applications for processing.
- Require officials involved in funding initiatives to obtain and maintain a security clearance, disclose conflicts of interest, and conduct organisation-specific checks such as police checks.
- Conduct fraud awareness training for officials involved in funding initiatives.

3.9 Undeclared conflicts of interest

Summary

A conflict of interest arises where a person makes a decision or exercises a power in a way that is influenced by either material personal interests (financial or non-financial) or material personal associations. For example, an official could select a relative for a funding opportunity when they would not normally be deemed eligible against the selection criteria; or an official could specifically tailor a funding opportunity to ensure a friend's organisation is awarded the money.

Fraudster Personas	 The Exploiter	 The Enabler	 The Organised	 The Corruptor
Red flags	▸ Transactions with friends/relatives that are not disclosed/managed. ▸ A public official who receives gifts from a funding recipient that are not disclosed/managed. ▸ Previous collaborations between the applicant and an official that are not disclosed/managed. ▸ Funding initiative reviewers, evaluators or decision makers who have affiliations with applicants that are not disclosed/managed.			
Countermeasures	▸ Ensure no single employee can assess an application for a funding initiative, give financial approval for expenditure, and make an offer to the funding recipient. ▸ Regular self-disclosure and reporting process to require employees to disclose real or perceived conflicts of interests. ▸ Regular reviews of self-disclosures by employees. ▸ Ensure decisions relating to funding opportunities are impartial, appropriately documented and reported, publicly defensible, and lawful. ▸ Assess the integrity of employees, contractors or third parties by having entry level checks, probationary periods, suitability assessments and/or security vetting. ▸ Provide tailored fraud awareness training for officials involved in the funding lifecycle. ▸ Specifically mention how to manage conflicts of interest.			

4 Case studies

The following are examples of real life cases of fraud against government funded initiatives in New Zealand. Case studies are an effective way of communicating a fraud problem, identifying vulnerabilities in your organisation, or to promote fraud awareness.

Think about the following questions as you read the case studies and use the information you identify to support conversations and grow awareness about fraud risks in your organisation:

- **What government funded initiatives does your organisation have, which are administered similarly to the ones in the case studies?**
  This could be both the from administration of the fund or as a recipient of funding.
- **What impact would a similar fraud have on your organisation?**
  Remember to consider both the financial and non-financial impacts of fraud, such as how it could affect staff morale or the services it might take away from the community.
- **What are some of the control gaps you can identify in the case studies?**
  Does your organisation have countermeasures that could prevent or detect fraudulent acts similar to the ones described? How confident are you that these countermeasures are operating as they should?
- **What more could your organisation do to make sure it is not the target of a fraudulent activity like that seen in the case studies?**
  Consider any additional countermeasures that could be implemented or awareness campaigns that could promote the right behaviours.

4.1 Fraud against an educational institute

In 2020 a prominent Māori performing arts educator was sentenced to 12 months home detention for defrauding a tertiary education provider and a Crown agency of approximately $1.3 million.

An internal programme coordinator defrauded an educational institute and government funded programme of $1.25 million. To qualify for the funding, they received the organisation had to deliver of educational courses over 18 weeks with an agreed curriculum. The programme coordinator had created the 18-week training course and was then contracted by the institute to deliver it.

The grant funding received by the institute was obtained fraudulently by the programme coordinator. To facilitate the fraud, the coordinator created false attendance records and

fictitious enrolment forms to dishonestly represent that people had enrolled in and completed 18-week study courses. The people enrolled had in fact attended short workshops or community events that were unrelated to the course programme being funded by the government. The coordinator also forged communications and completion certificates to support the illusion that students had completed the full course of study.

In addition to the loss of funding to the organisation, the coordinator's actions caused reputational damage to the educational institute and led to the perception that the qualifications received by genuine graduates may not be credible. The coordinator's actions also distorted the students' training records and jeopardised their ability to receive government funded training in the future. The coordinator did not personally gain a financial benefit from her offending and was sentenced to 12 months home detention.

4.2 Fraud against a disability trust

In 2018 a Christchurch couple received community-based sentences for defrauding a government funded disability trust of nearly $500,000.

The trustees of a government funded disability trust defrauded that trust of $494,545. The grant funds were for community vocational and recreational services for people with intellectual disabilities, enabling participation in community-based activities.

The trustees, who were husband and wife, used the Trust's credit card for personal expenditure. This personal expenditure was deliberately miscoded as expenses for the Trust and was included in the Trust's financial statements. By using trust money, the trustees funded a lavish lifestyle for themselves.

The offending meant that vulnerable members of the community did not receive the level of care or support that the government funding was intended to provide. The trustees were ordered to pay full reparation of $494,545. One trustee was sentenced to 12 months home detention and 300 hours of community work. The other was sentenced to six months of home detention, 200 hours of community work.

4.3 Fraud against a community grant programme

In 2017 three people charged with offences in relation to a multi-million-dollar gaming machine fraud in the Wellington High Court were found guilty.

An individual in control of an operating license for gaming machines colluded with others to ultimately deprive community organisations of $11.57 million. Regulatory requirements for Class 4 gambling require there to be a separation between the holder of the operating license (who owns the machines), the holder of the venue license (where the machines operate)

and the recipients of community grants. This protects the integrity of the community grant distribution process, which is provided by the profits from gambling machines.

The parties were found to have fraudulently concealed the involvement of the operating license holder at the venues where the gaming machines were operating. The operating license holder influenced the distribution of funds to community organisations, most of which were racing clubs, in return for a fee paid to him.

The offending meant that the operating license holder significantly influenced which organisations received financial support, in return for personal benefit. The offending also undermined an important regulatory regime and led to an adverse impact on the gaming system, the regulatory controls and the community's confidence in the Regulations. The operating license holder was sentenced to four-and-a-half year's imprisonment and both co-offenders to 12 months home detention.

5 Self-assessments checklists

Please note: This checklist is for guidance only and is not intended to be exhaustive. It should be completed periodically to help provide a degree of assurance in relation to your organisation's overall grants process and can also be used in relation to individual grant schemes.

Good practice standard		Yes/No	Action required
1	**General**		
1.1	We have clear responsibilities, processes, and procedures in place for managing grants.		
1.2	All those involved in administering grant schemes receive annual fraud awareness training and are familiar with the concepts of professional scepticism.		
1.3	We ensure that those involved in administering grants, at any stage, must declare any potential conflicts of interest. Any conflicts are then appropriately managed.		
2	**Design and development**		
2.1	Our development of grant schemes includes input from an appropriate range of experts, e.g., financial, legal, counter fraud etc.		
2.2	We complete a proportionate fraud risk assessment as part of the development of each grant scheme and keep it under review.		
3	**Market Engagement**		
3.1	We engage appropriately, and in a timely manner, with the relevant market when developing a grant scheme, to help ensure that potential fraud risks are identified at an early stage.		

Good practice standard		Yes/No	Action required
4	**Application Assessment**		
4.1	We use a pre-qualification checklist to help identify fraud risk indicators in relation to grant applicants.		
4.2	We have a range of checks in place to establish that the grant applicant is bona fide, financially sound, and has appropriate ethical standards, e.g., web searches, checks with relevant regulators, review of key documentation etc.		
4.3	Our grant application forms include appropriate wording about consequences of fraudulent applications, as a deterrent.		
5	**Award of Grant**		
5.1	We have an appropriate grants approval process in place.		
5.2	We ensure appropriate committee/Board/Council involvement in decisions to award grant funding.		
5.3	We use a robust grant agreement template for all grant awards. The template can be tailored to suit the nature and magnitude of the grant.		
5.4	We ensure that the grant agreement is signed by the relevant parties before any grant monies are paid out.		
5.5	Our grant agreement is clear about outcomes, what is (and is not) eligible expenditure, and what should happen in the event of fraud.		
5.6	Our grant agreement includes robust clawback arrangements so the funding used for ineligible or fraudulent purposes can be recovered.		
5.7	Our grant agreement requires staff and Board members of recipient organisations to have fraud awareness training.		

Good practice standard		Yes/No	Action required
5.8	As part of our grant award process, we ask grant recipients to declare that the award will not result in duplicate funding.		
5.9	We review the Government Funders' database as appropriate to identify possible duplicate funding, and we update it in relation to any grant we award.		
5.10	We have arrangements in place to communicate with other grant funders, to reduce the risk of duplicate funding.		
5.11	We pay our grants in arrears or in instalments to reduce risk		
6	**Performance Monitoring**		
6.1	We require all grant recipients to keep a full audit trail of all grant expenditure, which should be available for review. Original supporting documentation should include invoices, receipts, bank statements etc.		
6.2	Those responsible for monitoring are appropriately trained to recognise grant fraud risk indicators, e.g., false or amended supporting documents.		
6.3	We require grant recipients to have a documented system of internal controls, so that grant funding is properly administered, and to ensure those controls are operating.		
6.4	We provide a reporting route for those wishing to raise concerns about possible fraud or irregularity in relation to grants.		
6.5	We have clear arrangements in place for regular performance monitoring, including (as appropriate) site visits, periodic financial reports, statements of grant usage by category etc.		
6.6	Where financial monitoring identifies any ineligible or fraudulent expenditure, we activate clawback arrangements to recover the funding.		

Good practice standard		Yes/No	Action required
6.7	We immediately report any actual, suspected, or attempted grant fraud to the C&AG or the local Government Auditor as appropriate (via our sponsor department).		
6.8	We recognise that grant fraud is a crime which should be reported to police in accordance with our fraud response plan.		
6.9	We challenge instances where a funded organisation seeks an addition to the agreed level of funding, to ensure there is a valid reason for the request.		
7	**Review and Evaluation**		
7.1	We complete an end of grant review and financial reconciliation. We ensure that any underspend of the grant is returned and not retained fraudulently by the grant recipient.		

COUNTER FRAUD CENTRE

Tauārai Hara Tāware