SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

Guide to Fraudster Personas

AUGUST 2024

Counter Fraud Centre

Who We Are

The Counter Fraud Centre - Tauārai Hara Tāware (CFC) is the prevention arm of the Serious Fraud Office (SFO) and leads counter fraud efforts in New Zealand's public sector. We focus on building the public sector's resilience to fraud and corruption.

Our Mission

Our mission is to lift counter fraud culture and capability in the New Zealand public sector. We do this by producing guides and tools for the public sector and working directly with agencies to advise them on implementing effective counter fraud systems.

How We Can Help

Our depth of experience means we are ideally placed to lead counter fraud activities. We share our knowledge and expertise on the causes and impacts of fraud and corruption, and how to effectively mitigate them to reduce harm across the public sector. Our international connections also help us leverage key insights and best practice generated by overseas organisations and agencies.

Wherever you are with your counter fraud efforts, we're here to help. From basic fraud prevention factsheets to specific good practice guides we offer a range of resources and tools to help build capability across your organisation. We also provide customised counter fraud advice, workshops, and opportunities for cross-government engagement.

See our Counter Fraud Centre webpage for more information sfo.govt.nz/counterfraud/cfc or get in touch with us at counterfraud@sfo.govt.nz

Table of Contents

1 Introduction 4

1.1 Purpose of this Guide 4

1.2 Who Should Use this Guide 5

2 Using the Fraudster Personas 6

2.1 Using the Personas to Identify Fraud Risks 6

2.2 Using the Personas to Implement and Assess Countermeasures 8

2.3 Using the Personas to Increase Fraud Awareness 8

2.4 Using the Personas to Design Fraud Resilient Programmes 9

2.5 Using Fraudster Personas as a Tool for Counter Fraud Reporting 10

3 The Seven Fraudster Personas 11

The Impersonator 12

The Corruptor 13

The Deceiver 14

The Enabler 15

The Exploiter 16

The Fabricator 17

The Organised 18

1 Introduction

The Counter Fraud Centre at the Serious Fraud Office has identified seven fraudster personas, which can help you to think like a fraudster. A persona can be described as the character that is assumed by a fraudster, in line with the methods that they use to commit a fraudulent act. For example, they may deceive a public official, impersonate another individual or fabricate evidence.

Knowing the methods commonly used by fraudsters can be beneficial when planning counter fraud initiatives as it can help to provide additional insight into how an operation could be targeted. Fraudsters will often use a variety of methods from several different personas, so by understanding the range of methods they might use it can help to better recognise where they might target a government programme or function.

1.1 Purpose of this Guide

This guide has been developed to outline common methods used by fraudsters, which are referred to as fraudster personas. The guide can be used to support fraud awareness and the development of fraud prevention initiatives for your organisation.

This guide is split into two sections to help with understanding the personas and how to use them.

The **first section** is designed to help organisations understand how the personas can be a useful tool to help identify fraud risks, help to foster fraud awareness throughout an organisation and be used as a reporting tool.

The **second section** identifies the seven different fraudster personas. It provides some examples of the actions the specific persona might take and some of the red flags that people should be on the look out for. It then provides a list of the countermeasures (also known as controls) that an organisation can put in place to help reduce the risk of that persona being able to target an organisation.

For a full list of countermeasures identified in this guide, see the Countermeasures Guides on our website.

1.2 Who Should Use this Guide

Being able to recognise the fraudster personas will be a useful tool for the people in your organisation who are responsible for developing, implementing, and improving the organisation's counter fraud strategy and approach. This guide should be used by anyone in an organisation who is responsible for identifying, assessing and managing fraud risks. This may include risk practitioners, integrity advisors, and assurance leads or people from finance teams.

Understanding and identifying fraud should be a priority for everyone in an organisation, and so this guide will also be useful for other key groups including managers and supervisors, policy, and human resources teams.

2 Using the Fraudster Personas

There are several ways you can use the fraudster personas to enhance an organisation's fraud response.

This section outlines how the personas can be used to identify fraud risks, foster a mature fraud awareness culture and serve as a reporting tool.

2.1 Using the Personas to Identify Fraud Risks

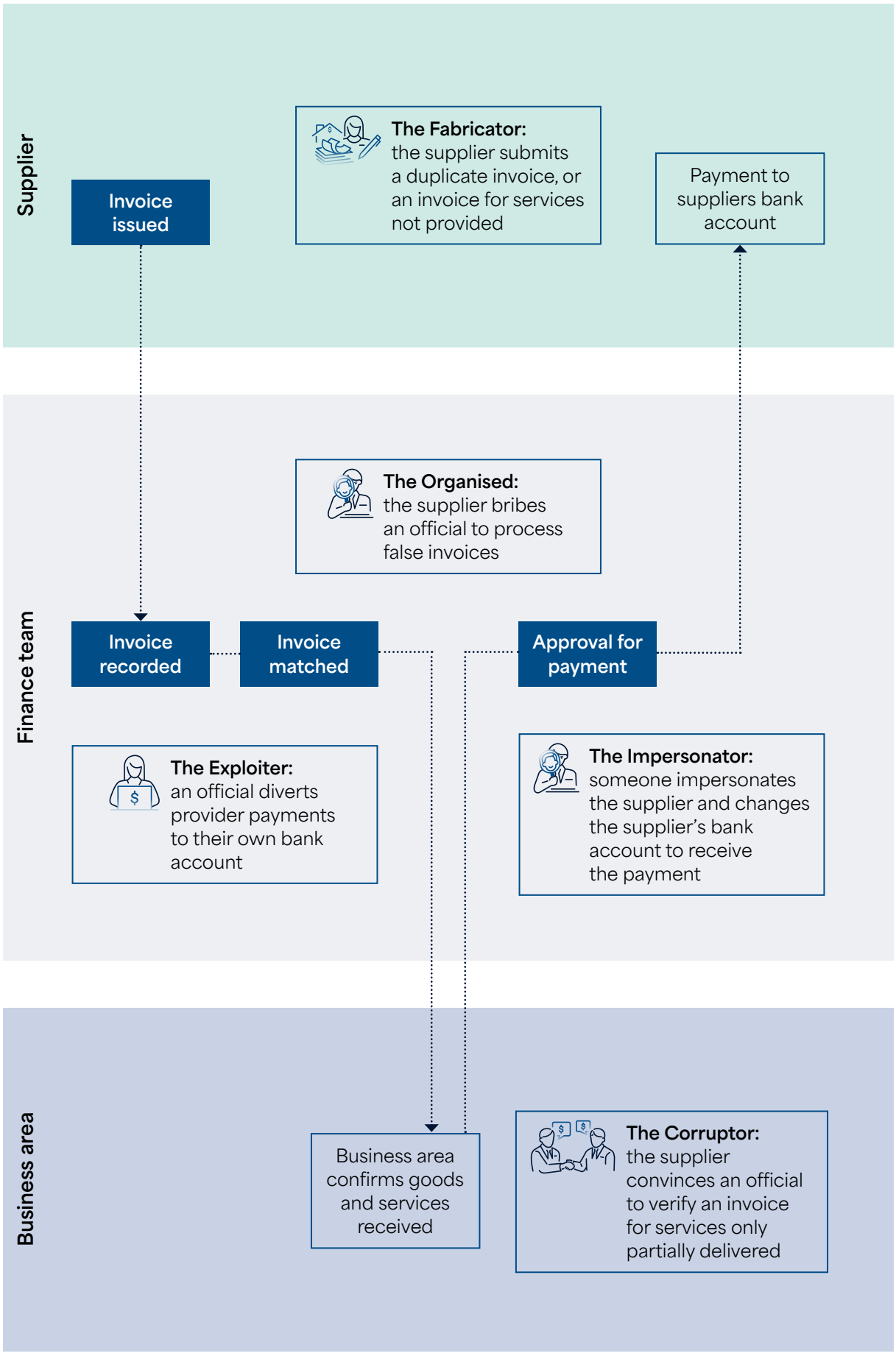
Individuals who have not been exposed to fraud often find it difficult to recognise fraud risk and pinpoint where fraud might occur. By understanding the methods of each persona, employees can better identify how a fraudster might target a business process or unit.

A good method for describing a fraud risk is to consider who is committing the fraud (the actor), how they are doing it (the action) and what the result is of the fraud (the outcome).

Fraudster personas can help to identify how and where an actor might be able to target government programmes and functions. For example, it might be more straightforward to pinpoint how 'the Fabricator' persona could exploit a business process – such as submitting a fake invoice – than to ask employees to list all possible fraud risks for their business unit.

Fraudster personas can also be useful when designing new processes to help consider how each fraudster persona might be able to exploit them at different steps. This approach means that organisations can implement specific countermeasures to effectively address and reduce the fraud risk.

One effective method for identifying fraudulent actions is to conduct a walk-through of a business process. For example, five different fraudster personas might be used in an invoice payment process as illustrated below.


Supplier
Invoice issued
The Fabricator: the supplier submits a duplicate invoice, or an invoice for services not provided
Payment to suppliers bank account
Finance team
The Organised: the supplier bribes an official to process false invoices
Invoice recorded
Invoice matched
Approval for payment
The Exploiter: an official diverts provider payments to their own bank account
The Impersonator: someone impersonates the supplier and changes the supplier's bank account to receive the payment
Business area
Business area confirms goods and services received
The Corruptor: the supplier convinces an official to verify an invoice for services only partially delivered

2.2 Using the Personas to Implement and Assess Countermeasures

Once you have identified fraud risks it is important to mitigate them using countermeasures. Countermeasures can be used to prevent, detect and respond to the identified risks, and are important to help limit the opportunities that fraudsters have to commit fraud.

The fraudster personas can be used to identify and implement countermeasures that specifically target the actions of a persona. Because fraudster personas display particular behaviours and use specific methods to succeed, being able to recognise them can help to identify targeted countermeasures to effectively counteract those methods.

For example, in the case of 'the Impersonator' persona the fraudster uses the method of impersonating other actors or creating entirely fictitious actors to deceive an organisation. By impersonating this other actor, they are then able to gain a benefit for themselves or another person.

To reduce the risk of 'the Impersonator' being able to target a programme, organisations can then implement countermeasures that are focussed on identity security and authentication.

Sometimes a countermeasure might have already been implemented but is not operating as designed or as effectively as it could. Fraudsters often exploit control vulnerabilities in processes, seeking opportunities to target organisations where these weaknesses exist.

Understanding which methods fraudster persona might use can reveal potential ways they could bypass controls. Identifying these potential bypasses allows you to prioritise addressing weaknesses and minimising opportunities for fraud. To learn more about the different countermeasures look at the Countermeasures Guides on our website.

2.3 Using the Personas to Increase Fraud Awareness

Fraud awareness is about raising the profile of counter fraud activities in an organisation. It also encourages employees to help prevent fraud and report suspicious behaviours they might see when performing their jobs.

Fraud awareness is one of the most effective tools to prevent fraud. According to the 2024 ACFE Report to the Nations, 43% of fraud is detected by tip-offs and more than half of these come from employees.[1] More than three times as many cases were detected through tip-offs than internal audit, the second next common detection method.

There are a number of ways to use the fraudster personas to raise awareness in an organisation and educate employees. Some examples are:

- Using fraudster personas in awareness campaigns, including posters, flyers, and screensavers.
- Using quizzes to educate employees about fraudulent behaviour using the fraudster personas.
- Including discussions of the fraudster personas in regular business meetings/stand ups.
- Distributing a link to our fraudster persona video.
- Demonstrating the fraudulent actions with a case study. The case studies on the Counter Fraud Centre's website identify the red flags and impacts of the fraudulent behaviour; and the countermeasures that can help to prevent, detect, and respond to different types of fraud.

2.4 Using the Personas to Design Fraud Resilient Programmes

Fraudster personas are not only useful to teams directly dealing with fraud prevention, such as those working in risk or finance, but also for policy teams. They can assist in co-designing fraud resilient programmes and functions by highlighting the common tactics used by fraudsters. Fraud resilient programmes and functions are achieved when the common methods used by fraudsters are considered during the policy design process.

To effectively identify where a fraudster might be able to target a new or renewed policy, policy teams should have a clear understanding of how fraudsters might attempt to deceive an organisation.

Using fraudster personas alongside other policy design tools, such as business process mapping and customer journey mapping, can also help to identify how and where non-compliant clients, employees, or service providers might be able to undermine the policy or programme outcomes and commit fraud against an organisation.

1 Association of Certified Fraud Examiners, Report to the Nations, (2024)

By adding the fraudster personas to an organisation's policy and programme design toolkit, the organisation will be better:

- Able to recognise fraud as a risk and its unintended consequence.
- Informed when undertaking fraud risk assessments.
- Placed to identify specific vulnerabilities and design specific countermeasures to mitigate them.
- Positioned to adjust policy settings or programme design to reduce the risk of fraud.

2.5 Using Fraudster Personas as a Tool for Counter Fraud Reporting

Fraudster personas can also be used as a visualisation tool for reporting fraud incidents. This can help leadership teams, stakeholders, and risk committees understand the types of fraud affecting an organisation's programmes and functions, and drive improvements to an organisation's fraud resilience.

For example, by identifying that an organisation faces a higher risk posed by fraudsters acting as 'the Impersonator' it can direct resources into strengthening identity countermeasures. Or, if an organisation identifies a higher risk from fraudsters exploiting payment processes, they can prioritise efforts to improve internal countermeasures and carry out awareness campaigns to help employees identify suspicious behaviours.

Fraudsters will often use a mixture of several different personas to gain a benefit from an organisation. For example, they may deceive an employee (the Deceiver), impersonate a person (the Impersonator) and fabricate evidence (the Fabricator). When using personas to report on specific fraud incidents it is important to highlight the different combinations of personas that an actor used to carry out the fraudulent action.

3 The Seven Fraudster Personas

This section provides detailed descriptions and examples of each of the fraudster personas. It also highlights key red flags to watch out for and outlines actions your organisation can take to mitigate the risk associated with these behaviours.

For a full list of countermeasures identified in this guide, see the Countermeasures Guides on our website.

Fraudster Persona	Description
The Impersonator	The Impersonator pretends they are another person or organisation to dishonestly gain a benefit for themselves or another person.
The Corruptor	The Corruptor abuses their position of entrusted power to gain a benefit for themselves or another person.
The Deceiver	The Deceiver makes others believe something that is not true to dishonestly gain a benefit for themselves or another person.
The Enabler	The Enabler knowingly or complacently enables fraudulent activity to dishonestly gain a benefit for themselves or another person.
The Exploiter	The Exploiter uses something for a wrongful purpose to dishonestly gain a benefit for themselves or another person.
The Fabricator	The Fabricator invents or produces documents that are false to dishonestly gain a benefit for themselves or another person.
The Organised	The Organised are a group of people who use a combination of sophisticated methods, in a planned and coordinated way, to dishonestly gain a benefit for themselves.

The Impersonator

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

This might involve using false or stolen identities, attributes, or credentials for personal gain.

Example of Impersonator actions

- An individual who poses as a vendor to divert a payment.
- An individual who uses stolen identities to receive a fraudulent payment.
- An individual who poses as an employee to authorise a transaction.

Red flags to look out for

- Email communication that does not sound like typical emails you may have received from company executives in the past.
- Multiple funding applications from the same IP address.
- Email request demanding urgent payments to be made.

Countermeasures to reduce the risk from an Impersonator

- **Governance, leadership, and culture**
  - Ethical culture
- **Prevention**
  - Identity verification
  - Automatic prompts and alerts
  - Parameters and limits
  - Fraud awareness training
  - Access controls
- **Detection**
  - Verify information received
  - Fraud detection software
  - Automatic data matching
  - Avenues for reporting fraud
- **Response**
  - Recovery and debt management processes

The Corruptor

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

This might involve negative incentives such as threats or intimidation, or positive incentives such as bribes.

Example of Corruptor actions

- Public service employees or officials who misuse their position of power to receive extravagant gifts.
- Public service employees or officials who misuse their position of power to award government contracts.
- Public service employees or officials who manipulate a process to pay a relative or friend more than other similarly suited people.

Red flags to look out for

- Purchasing of goods or services with no obvious business need.
- Over-inflated invoices or invoices that cannot be matched to any output.
- Continued acceptance of sub-standard goods or services despite complaints being made

Countermeasures to reduce the risk from a Corruptor

- **Governance, leadership, and culture**
  - Governance and oversight
- **Prevention**
  - Integrity checks and suitability assessment
  - Segregation of duties
  - Fraud awareness training
  - Access controls
  - Limit access to sensitive information
  - Protect data from manipulation
- **Detection**
  - Tip-offs and protected disclosures
  - Internal audits or reviews
  - Quality assurance checks
  - Evidence and document capture and storage
- **Response**
  - Fraud investigation policy

The Deceiver

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

This might involve providing false statements, deliberate misrepresentation or withholding facts or circumstances.

Example of Deceiver actions

- An individual who misrepresents facts or circumstances to receive a benefit.
- An individual who withholds key information to get increased payments.
- A vendor who withholds critical information to influence the award of a contract.

Red flags to look out for

- Individuals who do not answer questions. Individuals do not like to lie and will usually try to avoid answering a question before answering with a lie.
- Lack of detail on application documentation, only providing the bare minimum information or some not at all.
- Withdrawal of an application when questioned for additional information.

Countermeasures to reduce the risk from a Deceiver

- **Governance, leadership, and culture**
  - Ethical culture
- **Prevention**
  - Eligibility criteria
  - Fraud awareness training
- **Detection**
  - Verify information received
  - Fraud detection software
  - Automatic data matching
  - Avenues for reporting fraud
  - Internal audits or reviews
- **Response**
  - Recovery and debt management processes

The Enabler

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

This might involve an individual who intentionally keeps themselves unaware of the circumstances to avoid responsibility.

Example of Enabler actions

- An individual who approves an expense claim for another person knowing that the expense does not comply with the expense policy.
- An individual who approves a grant knowing that the applicant is using a false identity.
- An individual who processes a vendor invoice, knowing that the invoice includes fraudulent charges.

Red flags to look out for

- Approving high volume of payments to a vendor/supplier when you would expect a low volume of invoices.
- Use of vendors that are not on the authorised vendor list.
- Business activities that are targeted to specific individuals.
- Leaders proceeding with high-risk decisions outside the business risk appetite.

Countermeasures to reduce the risk from an Enabler

- **Governance, leadership, and culture**
  - Governance and oversight
- **Prevention**
  - Eligibility criteria
  - Procedural instructions or guidance
  - Automatic prompts and alerts
  - Fraud awareness training
- **Detection**
  - Quality assurance checks
- **Response**
  - Recovery and debt management processes

The Exploiter

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

This might involve misusing their position or privileges or dishonestly exploiting a vulnerability for personal gain.

Example of Exploiter actions

- An individual who splits a purchase into smaller contracts to keep it within their delegated authority to benefit a vendor.
- An individual who accesses permission to change their salary in the payroll system.
- An individual who exploits vulnerabilities to apply for emergency relief when they know they are not entitled to receive it.

Red flags to look out for

- Staff who have systems access which is broader than what their role requires.
- Inconsistent head count numbers between staff count and payroll processing systems.
- Multiple change requests for vendor contracts.

Countermeasures to reduce the risk from an Exploiter

- **Governance, leadership, and culture**
  - Ethical culture
- **Prevention**
  - Access controls
  - Limit access to sensitive information
  - Protect data from manipulation
  - Segregation of duties
  - Fraud awareness training
- **Detection**
  - Fraud detection software
  - Internal audits or reviews
- **Response**
  - Fraud investigation policy

The Fabricator

The Fabricator invents or produces documents that are false to dishonestly gain a benefit for themselves or another person.

This might involve creating false invoices or other types of records for personal gain.

Example of Fabricator actions

- An individual fabricates documents, for example property titles, to receive a mortgage for their business.
- A staff member fabricates receipts, for example restaurant receipts, to support a false expense claim.
- A trustee fabricates documents, for example financial statements, to qualify for funding.

Red flags to look out for

- Documents with inconsistent formatting, for example font type, size, and/or colour, misalignment of text.
- Documents with obvious omissions of information which would normally be expected on a document.
- Incorrect corporate information, such as logo, contact details, misspelled names and physical address.

Countermeasures to reduce the risk from a Fabricator

- **Governance, leadership, and culture**
  - Governance and oversight
- **Prevention**
  - Protect data from manipulation
  - Parameters and limits
  - Fraud awareness training
- **Detection**
  - Verify information received
  - Fraud detection software
  - Automatic detection software
  - Activity and exception reporting
  - Internal audits or reviews
  - Evidence and documents capture and storage
- **Response**
  - Fraud investigation policy

The Organised

The Organised are a group of people who use a combination of sophisticated methods, in a planned and coordinated way, to dishonestly gain a benefit for themselves.

This may involve using professional facilitators and service providers to help or facilitate their criminal activities.

Example of Organised actions

- An individual that collaborates with multiple people to submit fabricated documents to secure fraudulent mortgages.
- A group of people that collaborate with an accountant to falsify business records to receive grant funding.
- A group of people that collaborate with individuals to use stolen identities to apply for funding.

Red flags to look out for

- A vendor that was created shortly before or after the contract was awarded.
- Excessive amount of missing information about applicants who received funds.
- Procedural or computer-system inquiries or transactions that are inconsistent with the user ID's normal duties.

Countermeasures to reduce the risk from the Organised

- **Governance, leadership, and culture**
  - Governance and oversight
- **Prevention**
  - Parameters and limits
  - Fraud awareness training
- **Detection**
  - Verify information received
  - Fraud detection software
  - Avenues for reporting fraud
- **Response**
  - Recovery and debt management processes
  - Fraud investigation policy
  - Coordinated disruption activity

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

SFO | SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Te Kāwanatanga o Aotearoa
New Zealand Government