



COUNTER FRAUD CENTRE

Tauārai Hara Tāware



Detection

Countermeasures

APRIL 2023

Table of Contents

1	Introduction	1
	1.1 Purpose	2
	1.2 What is included	2
2	Detection Countermeasures	3
	2.1 Verify information you receive	4
	2.2 Automatic data matching	6
	2.3 Evidence and document capture and storage	8
	2.4 Quality assurance checks	10
	2.5 Activity reporting	12
	2.6 Exception reporting	14
	2.7 Internal audits or reviews	16
	2.8 Avenues for reporting fraud	18
	2.9 Fraud detection software	20

1 Introduction

Fraud risks involve deceptive behaviours carried out by people who try to hide their actions. Therefore, organisations are encouraged to put in place anti-fraud and corruption countermeasures that help minimise opportunities to commit fraud and maximise detection of fraud.

Fraud risks can be managed by establishing practices and countermeasures to mitigate the risks or by designing specific fraud evaluation procedures. An organisation's mitigation practices will differ based on its fraud risk tolerance and exposure to risks.

No system of countermeasures can completely eliminate fraud. However, well designed and effective countermeasures can assist in deterring and detecting fraudulent activity.

Countermeasures come under the following four categories:

- ▶ **Capability countermeasures** guide expected behaviours and determine organisational culture around fraud. These are important for providing direction to employees.
- ▶ **Prevention countermeasures** are the most common and cost-effective way of limiting the size of fraud risks, by reducing the likelihood of it occurring.
- ▶ **Detection countermeasures** help to identify when fraud has occurred, disrupt it and reduce the impacts.
- ▶ **Response countermeasures** respond to fraud after it has occurred to reduce or disrupt additional impacts. This includes investigation, prosecution, disciplinary action and recovery activities.

1.1 Purpose

The purpose of this guide is to provide fraud practitioners and risk managers with information about detection countermeasures that can be applied or adapted to suit an organisation's fraud exposure and risk tolerance.

Similar information about **capability, prevention** and **response** countermeasures can be found at [on the Serious Fraud Office website](#).

1.2 What is included

This guide contains high level information on **nine detection countermeasures**. Not all countermeasures are appropriate for all organisations. Using this guide, practitioners will be able to determine whether it is appropriate to adopt a countermeasure, based on an organisation's risk exposure and tolerance.

The guide includes the following information for each countermeasure:

- ▶ 'Examples' provides examples of how the countermeasure can be implemented.
- ▶ 'Why this is important' and 'Related fraudster personas' give examples of the fraud and corruption risks, as well as the fraudster personas.
- ▶ 'Suggested measurements' provides ways to test the effectiveness of the countermeasure.
- ▶ 'Vulnerability indicators' includes indicators where the countermeasure may not be effective.
- ▶ 'This type of countermeasure is supported by' lists complimentary countermeasures that can be used as part of an organisation's control environment. These countermeasures are included in the [capability, prevention, detection, or response countermeasure guides](#).

2 Detection Countermeasures




This guide contains nine detection countermeasures. It is not an exhaustive list of all available detection countermeasures.

Use this guide to:

- ▶ consider whether your organisation is exposed to the fraud risks and fraud personas described in the guide.
- ▶ consider whether these countermeasures are or should be in place to mitigate these fraud risks.
- ▶ understand how your organisation can assess the operating effectiveness of the countermeasures.
- ▶ understand how your organisation can identify if a countermeasure is not operating effectively.
- ▶ consider whether other supporting countermeasures should be implemented as part of an organisation's control environment.

2.1 Verify information you receive




Verify key information from requests or claims, with an independent and credible source.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks.</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none"> ▶ cross-referencing the provider number with provider register(s). ▶ verifying claim eligibility by cross-referencing details held by another programme or entity. ▶ obtaining corresponding evidence from both a client and provider. ▶ verifying professional qualifications with the education provider. ▶ confirming business details.
<p>Why this is important</p> 	<p>Not verifying the information that you receive may lead to:</p> <ul style="list-style-type: none"> ▶ fraudsters providing false information or evidence to support a request or claim. ▶ fraudsters hiding information that would affect their entitlements. ▶ fraudsters successfully using forged documents to support a request or claim. ▶ difficulties in responding to fraud. <p>Obtaining benefits or causing losses by deception or dishonestly using documents and forged ones to obtain financial advantages are offences under the Crimes Act 1961.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that reference and guidance materials regarding information verification processes are easy to understand ▶ Confirm that information is verified by reviewing a sample of completed requests/claims ▶ Confirm that processes cannot be circumvented by doing active testing or a process walk-through ▶ Review procedures and guidance to confirm it clearly specifies the requirements for verifying information ▶ Confirm that employees have a consistent and correct understanding of how to verify information ▶ Confirm that verification requirements are clearly communicated to employees, customers, and third parties

Suggested measures cont'd	<ul style="list-style-type: none"> ▶ Confirm that employees cannot bypass or manipulate the verification requirements, even when pressure or coercion is applied ▶ Confirm that reviewers document evidence of the information that information has been verified ▶ Confirm that employees receive training about how to verify information
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Automatic data matching
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Impersonator ▶ The Fabricator ▶ The Organised

2.2 Automatic data matching




Match data automatically with another source to obtain or verify details relevant to the request or claim.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks.</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none">▶ comparing claim or recipient data in a batch file with a corresponding data file.▶ populating claim data automatically by using a data link.▶ matching programme participants by sharing data files between organisations.
<p>Why this is important</p> 	<p>Not verifying the information that you receive may lead to:</p> <p>The absence of data matching with another source may lead to:</p> <ul style="list-style-type: none">▶ the inability to obtain or verify information.▶ false information being used to support a request or claim.▶ changes or information not being disclosed that would affect entitlements.▶ changes in circumstances being missed. <p>Individuals may provide false information to support a request or claim or fail to disclose changes or information that would affect their entitlement.</p> <p>Data matching is useful to identify or verify information from another source or identify changes in a claimant's circumstances.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none">▶ Consult subject matter experts about the data matching process.▶ Review the accuracy of the data match by doing quantitative analysis e.g. the percentage of successful matches▶ Undertake quantitative analysis to determine the reliability of the data match e.g. the data is reliable/trustworthy▶ Review the usefulness of the data match by doing qualitative analysis of the data and measuring its impact on data matching

Suggested measures cont'd	<ul style="list-style-type: none"> ▶ Confirm that data matching is working correctly by comparing a sample of completed requests/claims to the data matching information ▶ Confirm that the original data sources are impartial, reliable, and trustworthy ▶ Confirm that data matching is used to support decision-making by doing a process walk-through ▶ Confirm data matching is always on/available ▶ Confirm that employees cannot bypass data matching even when they are subjected to pressure or coercion
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Protect data from manipulation
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Impersonator ▶ The Fabricator ▶ The Organised ▶ The Enabler

2.3 Evidence and document capture and storage

Capture documents and other evidence to detect, analyse, investigate, and disrupt fraudulent activity.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks.</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none"> ▶ storing all claims forms on a secure system. ▶ scanning and uploading all evidence for a claim into a secure system. ▶ documenting decisions on a secure system before processing the request/claim. ▶ keeping all procurement decisions and documentation on file. ▶ This countermeasure is supported by the NZ Information and Records Management Standards and the Public Records Act 2005.
<p>Why this is important</p> 	<p>Poor (or absent) capture and storage of documents and evidence may lead to:</p> <ul style="list-style-type: none"> ▶ difficulty in detecting, analysing, investigating, and disrupting fraudulent activity. ▶ failure of criminal, civil, or administrative actions due to inadmissible evidence. ▶ inability to share information with other organisations. ▶ information being improperly accessed or released. <p>A lack of documentation and evidence can make it difficult to detect, analyse, investigate, and disrupt fraudulent activity.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that the capture and storage of documents and evidence follows NZ Information and Records Management Standards ▶ Confirm that investigators understand what the evidence requirements are and have access to evidence ▶ Confirm that evidence is sufficiently captured by investigators to support an investigation ▶ Confirm that storage of evidence is automatic and reliable ▶ Confirm that employees understand the processes for storing documents and evidence

Suggested measures cont'd	<ul style="list-style-type: none"> ▶ Confirm that access to documents is restricted to those who need it for business purposes ▶ Confirm that documents cannot be altered and that the original is retained ▶ Confirm that audit logging is automatically generated when accessing or updating documentation ▶ Confirm that investigators can access evidence held by another party, if required
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Procedural instructions or guidance
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Fabricator ▶ The Corruptor ▶ The Reckless ▶ The Organised ▶ The Enabler

2.4 Quality assurance checks

Conduct quality assurance checks to confirm that processes are being followed correctly and to a high standard, and/or that goods received are what they are claimed to be.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks.</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none">▶ randomly selecting work to quality check – for example, 2% of processed claims or decisions.▶ having an independent person to quality check high-risk activities on all occasions e.g. changes to vendor records.▶ having the procurement team quality check purchase orders above \$10,000 before they go to the spending approver.▶ selecting random or targeted samples of products to check that they are what they are claimed to be.
<p>Why this is important</p> 	<p>Quality assurance checks can:</p> <ul style="list-style-type: none">▶ increase levels of compliance and reduce errors due to consistent applications of processes, rules, and decision-making.▶ deter employees from committing fraud.▶ increase transparency of actions and decisions made by employees and third parties.▶ better manage performance, decision-making, and risk▶ increase detection and response to fraud or corrupt activity.▶ ensure that safe or 'fit for purpose' goods and services are received by organisations or the public. <p>Clients, suppliers, or businesses can provide faulty goods or services anywhere in the supply chain process.</p> <p>Quality assurance processes can also lead to the detection of more errors, making it more difficult for fraudsters to exploit organisations. Employees will also be deterred from committing deliberate acts of fraud because they will be cautious about being caught.</p>

<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Review quality assurance processes to see if they align with quality assurance policies and standards ▶ Compare data related to quality checks and measure results against key performance indicators ▶ Review quality checking processes to determine if the checks would identify fraud ▶ Confirm that employees know what quality assurance checks they need to do, by doing a process walk-through ▶ Confirm that employees understand how to perform quality assurance checks correctly and consistently by carrying out interviews, workshops, and surveys ▶ Confirm that processes for high-risk activities include an independent review aspect e.g. reviews by employees in other locations ▶ Confirm that processes are standardised across team members, by comparing completed work from various employees
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Governance and oversight ▶ Procedural instructions or guidance ▶ Fraud awareness training
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Fabricator ▶ The Reckless ▶ The Exploiter

2.5 Activity reporting

Prepare summary reports on activities for clients, managers, or responsible employees.

Examples



This countermeasure targets internal fraud risks.

Some examples of activity reporting include:

- ▶ programme or administrative budgets and expenses.
- ▶ programme claims, payments and other key performance indicators.
- ▶ employees' attendance and allowances, such as overtime payments.
- ▶ project or contract performance.
- ▶ procurement and vendor payments..

Reporting to clients and employees on:

- ▶ changes to their accounts.
- ▶ programme or organisational performance.
- ▶ programme or organisational change.
- ▶ trends and issues.

Why this is important




Reporting on activities may result in:

- ▶ increased transparency of actions and outcomes.
- ▶ better management of performance, decision-making, and risk
- ▶ more action and accountability to prevent, detect and respond to fraud and corruption.
- ▶ detecting fraudulent activity and responding to it.

Clients, employees, or contractors can take advantage of obscurity to commit fraud, act corruptly, and avoid exposure.

Lack of reporting may also lead to clients, employees, or contractors being confused about requirements and accidentally or recklessly engaging in non-compliant conduct that could lead to fraud.

Obtaining benefits or causing losses by deception or dishonestly using documents and using forged documents to obtain financial advantages are offences under the Crimes Act 1961.

<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that reports are produced and used ▶ Review a sample of reports to determine if they are clear, relevant, and would help someone detect fraud ▶ Review data related to reports to see how often they are reviewed ▶ Confirm that reports and data cannot be manipulated ▶ Confirm that reports are sent or readily available to the appropriate people such as: <ul style="list-style-type: none"> ▪ customers who can view reports via their online account. ▪ line managers receive the report via email. ▪ executives who review reports during committee meetings
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Procedural instructions or guidance
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Fabricator ▶ The Impersonator

2.6 Exception reporting

Establish exception reports to identify activities that are different from the standard, normal, or expected process, and should be further investigated.


<p>Examples</p> 	<p>This countermeasure targets internal and external fraud risks.</p> <p>Examples of types of countermeasures include:</p> <ul style="list-style-type: none"> ▶ unusually high payments. ▶ large salary changes. ▶ unusually high programme payments. ▶ excessive ordering of assets. ▶ employees who have made more expense claims than usual in a month. ▶ prices that do not match market variations. ▶ payments or claims repeatedly below reporting thresholds. ▶ claims that exceed a set frequency or threshold
<p>Why this is important.</p> 	<p>A lack of exception reporting may lead to:</p> <ul style="list-style-type: none"> ▶ disorganised or inconsistent practices and decision making. ▶ less transparency of actions and outcomes. ▶ poor management of fraud and corruption risks. ▶ less action and accountability to prevent, detect, and respond to fraud and corruption. ▶ fraud or corrupt activity going unnoticed or unchallenged. <p>Exception reporting increases transparency and reduces the opportunity for fraud.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that the exception tolerances or parameters are appropriate ▶ Confirm that the exception parameters or thresholds are not widely known ▶ Confirm that exception reports are produced and used, and that the process is adequate ▶ Confirm that exception reports go to the most appropriate team/employee for review

Suggested measures cont'd	<ul style="list-style-type: none"> ▶ Walk through processes with staff members while they review reports and respond to anomalies ▶ Review a sample of reports to see if they are clear, relevant to the user, and would help to detect fraud ▶ Review statistics related to reports, e.g. the quantity and frequency of exceptions that are reported ▶ Review who has access to exception reports. ▶ Confirm that someone cannot manipulate reports or the data they are based on
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Parameters and limits ▶ Automatic data matching ▶ Activity reporting
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Fabricator ▶ The Enabler ▶ The Exploiter

2.7 Internal audits or reviews

Conduct internal audits or reviews to evaluate and improve the effectiveness of risk management, control, and governance processes.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks. Clients, employees, or contractors can take advantage of weaknesses in government programmes and systems to commit fraud, act corruptly, and avoid exposure. Internal audits or reviews can identify these weaknesses.</p> <p>Examples of types of countermeasures include:</p> <ul style="list-style-type: none"> ▶ regular security audits of information and communications technology. ▶ programme performance audits. ▶ random site visits for providers. ▶ surveys to check the accuracy of regular payments. ▶ monthly audits of employee travel expenditure. ▶ regular reviews of grants allocations. ▶ regular audits of credit card spending.
<p>Why this is important</p> 	<p>Regular audits or reviews of activities can:</p> <ul style="list-style-type: none"> ▶ convey that actions by fraudsters will be detected. ▶ increase levels of compliance and reduce errors due to adherence with consistent and clear processes, rules, and decision-making. ▶ make it more difficult for fraudsters to commit fraud, due to consistent practices and processes being in place, and a fear of being exposed or prosecuted. ▶ more transparency of the actions and decisions of employees and third parties. ▶ reduce opportunities for employees or contractors to take advantage of positions of trust to act corruptly, commit fraud, and avoid exposure. ▶ detect and respond to fraud or corrupt activity. ▶ increase action and accountability for preventing, detecting, and responding to fraud and corruption. ▶ detect systemic fraud or corruption.

<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Review the outcomes of audits or reviews ▶ Confirm that audits or reviews are carried out ▶ Check that audits or reviews are performed regularly ▶ Confirm that the scope of audits or reviews consider fraud risks and controls ▶ Confirm that audits or reviews are independent, completed by qualified persons, and are resilient to corrupting influences ▶ Check what other reporting occurs, such as executive reviews of reports during committee meetings
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Governance and oversight ▶ Evidence and document capture and storage
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Fabricator ▶ The Corruptor ▶ The Exploiter

2.8 Avenues for reporting fraud




Put in place processes for employees or external parties to lodge tip-offs or provide protected disclosures.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks.</p> <p>Examples of types of countermeasures include:</p> <ul style="list-style-type: none"> ▶ a dedicated reporting line. ▶ an online form available through an internal or external website. ▶ avenues for protected disclosures if there is suspected wrongdoing within organisations. <p>Other ways of supporting individuals, third parties and employees to confidently report suspicions of fraud include:</p> <ul style="list-style-type: none"> ▶ offering rewards or compensation for reporting. ▶ providing immunity or deferred prosecutions for self-reporting.
<p>Why this is important</p> 	<p>Discreet and confidential ways for employees or external parties to report fraud and corruption may help to:</p> <ul style="list-style-type: none"> ▶ foster an ethical workplace culture. ▶ increase transparency and lead to fraudsters feeling less confident that their actions will not be detected. ▶ detect and respond to fraud or corrupt activity. ▶ increase action and accountability for preventing, detecting, and responding to fraud and corruption. ▶ detect systemic fraud or corruption. ▶ prevent further fraud or non-compliance from continuing. <p>Fraudsters are more likely to be deterred from committing fraud if they think that they could be exposed.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that a consistent process exists for reporting fraud and corruption ▶ Confirm that the process for reporting fraud and corruption is easy to find and understand ▶ Confirm that the options for reporting fraud and corruption are clearly communicated ▶ Consider if processes in place provide support to the person reporting fraud and corruption

Suggested measures cont'd	<ul style="list-style-type: none"> ▶ Confirm if processes are compliant with the Protected Disclosures Act 2000 ▶ Review any cases where reporting did not result in follow up action to see if any changes need to be made about how and what information is obtained when an allegation of fraud is made ▶ Confirm that processes allow employees or external parties to report different types of fraud and corruption ▶ Confirm that processes cater for a range of sources of allegations e.g. external individuals, employees, vendors, and other organisations
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Ethical culture ▶ Governance and oversight ▶ Fraud awareness training
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Impersonator ▶ The Corruptor ▶ The Organised ▶ The Fabricator

2.9 Fraud detection software

Use fraud detection software to automatically analyse data to detect any anomalies that may indicate fraud or corruption.

<p>Examples</p> 	<p>This countermeasure targets both internal and external fraud risks.</p> <p>Examples of types of countermeasures include:</p> <ul style="list-style-type: none"> ▶ analysing system access logs to detect unauthorised access to internal systems or online accounts. ▶ monitoring for suspicious changes to client or provider bank accounts such as common accounts being used. ▶ monitoring the use of compromised personal identity information. ▶ analysing bulk data sets to identify suspicious patterns and anomalies. ▶ automating reviews of system access logs to detect unauthorised access. ▶ analysing claims data to identify suspicious patterns and anomalies .
<p>Why this is important</p> 	<p>The implementation of fraud detection software programmes can lead to:</p> <ul style="list-style-type: none"> ▶ increased transparency and awareness amongst fraudsters that they will be caught. ▶ detection of fraud or corrupt activity. ▶ early detection, investigation, and response to allegations of fraud. <p>Customers, employees, or contractors are prevented from committing fraud due to heightened detection capabilities.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Conduct pressure testing to determine if fraudulent activity would be detected ▶ Confirm if subject matter experts are confident about how the detection programme operate ▶ Confirm that the detection programme settings are not widely known, allowing someone to deliberately avoid detection ▶ Confirm that the data/logs underlying the detection programme are adequate and reliable
<p>Suggested</p>	<ul style="list-style-type: none"> ▶ Confirm that detection programme reports are produced

measures cont'd	<p>and used, and the process is adequate</p> <ul style="list-style-type: none"> ▶ Confirm that detection programme results go to an independent and appropriate reviewer ▶ Review a sample of detected incidents to identify areas for improving processes
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Automatic data-matching ▶ Protect data from manipulation ▶ Evidence and document capture and storage
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Deceiver ▶ The Impersonator ▶ The Fabricator ▶ The Exploiter ▶ The Organised



COUNTER FRAUD CENTRE

Tauārai Hara Tāware