



COUNTER FRAUD CENTRE

Tauārai Hara Tāware



Prevention

Countermeasures

APRIL 2023

Table of contents

1	Introduction	2
	1.1 Purpose	3
	1.2 What is included	3
2	Prevention Countermeasures	4
	2.1 Identity verification	5
	2.2 Integrity checks and suitability assessments	7
	2.3 Eligibility requirements	9
	2.4 Access controls	11
	2.5 Limit access to sensitive information	13
	2.6 Fraud awareness training	15
	2.7 Parameters and limits	17
	2.8 Procedural instructions or guidance	19
	2.9 Automatic prompts and alerts	21
	2.10 Protect data from manipulation	23
	2.11 Segregation of duties	25

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 **prevention countermeasures** that can be applied or adapted to suit an organisation's fraud exposure and risk tolerance.

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

1.2 What is included

This guide contains high level information on **11 prevention countermeasures**. Not all countermeasures are appropriate for all organisations. Using this guide, practitioners will be able to determine whether it is appropriate to adopt the countermeasures, 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 Prevention Countermeasures




This guide contains **11 prevention** countermeasures and should not be considered an exhaustive list of all prevention 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 Identity verification




Authenticate client or third-party identities during each interaction. This involves testing the credentials supplied by the person making the 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"> ▶ using RealMe to confirm an individual’s identity online. ▶ performing entry level checks to confirm the identity of employees and contractors. ▶ requiring service providers to present evidence of identity for company directors.
<p>Why this is important</p> 	<p>Accepting claims or requests without confirming an applicant’s identity can lead to:</p> <ul style="list-style-type: none"> ▶ fraudsters impersonating customers or third parties in order to receive fraudulent payments or gain access to information. ▶ fraudsters using false identities to receive fraudulent payments or gain access to information. <p>Confirming the identities of individuals and third parties can help an organisation to:</p> <ul style="list-style-type: none"> ▶ ensure that it is dealing with the right person or company. ▶ make it harder for fraudsters to commit frauds that rely on identity takeover or business spoofing. Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Review identity verification policies to make sure it is clear when a policy applies ▶ Review a sample of completed claims to confirm correct processes are being carried out ▶ Review identified cases of fraud that used a false or stolen identity to confirm whether changes are required to identity verification processes ▶ Confirm that employees are applying processes consistently both within and across channels

Countermeasure supported by	<ul style="list-style-type: none">▶ Procedural instructions or guidance▶ Identity verification▶ Automatic data matching
Related Fraudster Personas	<ul style="list-style-type: none">▶ The Organised▶ The Exploiter▶ The Enabler

2.2 Integrity checks and suitability assessments

Undertake activities to assess and confirm the integrity and suitability of new employees, contractors or third parties.

<p>Examples</p> 	<p>This countermeasure targets internal fraud risks.</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none"> ▶ pre-employment checks e.g. criminal record and credit checks for all new employees, contractors, or third parties. ▶ robust reference checking processes. ▶ trial periods for all new employees, contractors, or third parties. ▶ requiring all employees, including contractors, to have and maintain the appropriate security clearance for designated roles, in accordance with protective security requirements. ▶ ongoing checks after onboarding employees or clients. ▶ verifying that businesses have a valid NZBN and confirming their details e.g. by searching the Companies Register website. ▶ checks in accordance with protective security requirements
<p>Why this is important</p> 	<p>Employees, contractors, or third parties who lack integrity can create insider threats or contribute to a dysfunctional organisational culture.</p> <p>Knowing who an organisation is employing or contracting to can help to mitigate costly frauds or errors and minimise reputational damage.</p> <p>Employees, contractors, or third parties can abuse their position of trust to commit fraud or act corruptly. These individuals can also be coerced to commit fraud for the benefit of another person or entity e.g. an employee is coerced to provide information or pay a claim</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Review the integrity checks process for new employees, contractors, vendors, or providers ▶ Review the process for ongoing suitability assessments throughout the employment/engagement period of employees, contractors, or third parties ▶ Review suitability assessment processes to confirm that they align with protective security requirements

Suggested measures cont'd	<ul style="list-style-type: none"> ▶ Identify whether there is a high number of contracts that are terminated during or after an initial trial period. A high volume of terminations may indicate that the initial screening process or suitability assessment is not operating effectively ▶ Analyse data from integrity checks and suitability assessments and confirm that these are always completed ▶ Undertake an employee survey that includes questions on awareness of integrity issues and how to report them ▶ Identify positions that require a security clearance and confirm that each employee has the required clearance
Countermeasure supported by	<ul style="list-style-type: none"> ▶ Procedural instructions or guidance ▶ Identity verification ▶ Automatic data matching
Related Fraudster Personas	<ul style="list-style-type: none"> ▶ The Corruptor ▶ The Organised ▶ The Deceiver

2.3 Eligibility requirements

Have clear and specific eligibility requirements and only approve requests or claims that meet the criteria

Examples



This countermeasure targets internal fraud risks.

Examples of this countermeasure include:

- ▶ income tests or requirements e.g. a claimant's taxable income/business turnover must be below \$100,000.
- ▶ age requirements e.g. programme recipients must be over the age of 67 years.
- ▶ residency requirements e.g. programme payments are only available to New Zealand residents.
- ▶ geographical requirements e.g. programme recipients must reside in a particular location.
- ▶ qualification requirements e.g. potential vendors must possess appropriate licences.
- ▶ preconditions e.g. employees cannot be issued with a building pass prior to the completion of an entry level check.
- ▶ expenditure requirements e.g. expenditure on a project must be above/below \$100,000.
- ▶ quantitative requirements e.g. claimants can only claim for a certain number of hours or people.
- ▶ Eligibility requirements can also be used to fast track or provide additional scrutiny for claims e.g. a family claiming for more than five children is required to undergo additional checks.


Why this is important



Failing to specify clear eligibility requirements or not verifying a person's eligibility for a request/claim can lead to:

- ▶ fraudsters exploiting weaknesses to receive payments or services they are not entitled to; or
- ▶ fraudsters accessing information or systems without a business need.

Someone can provide false information or evidence to support a request/claim or fail to disclose information that would affect their entitlement.

<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Review a sample of completed requests or claims to confirm that correct eligibility determinations are being made ▶ Review approval processes to see if there is a segregation of duties, if required ▶ Calculate how many reviews result in a reversal of the original eligibility decision ▶ Confirm that employees receive training about eligibility requirements ▶ Confirm employees have access to reference materials that set out required standards for eligibility requirements ▶ Confirm that employees understand what the eligibility criteria are and how to apply them consistently ▶ Undertake testing or a process walk through to confirm that eligibility determinations cannot be manipulated or bypassed (even when pressure or coercion is applied)
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Identity verification ▶ Verify information received
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Enabler ▶ The Deceiver ▶ The Exploiter

2.4 Access controls

Limit access to systems, data, information, physical documents, offices, and assets.

Examples



This countermeasure targets internal fraud risks.

Examples of this countermeasure include:

- ▶ login ID and password to access systems.
- ▶ approving a request from employees before providing access to internal systems.
- ▶ two-factor authentication to access an online account.
- ▶ restricted access to different parts of a building.
- ▶ restricting access to an online provider's system to registered providers.
- ▶ restricting employees' access to online email servers on work on computers.
- ▶ classified documents are stored in secure lockable cabinets.

Why this is important



Failing to implement effective access controls can lead to:


- ▶ fraudsters accessing or manipulating systems and information without authority.
- ▶ fraudsters facilitating fraudulent payments.
- ▶ fraudsters stealing data, information, physical documents, or assets to benefit themselves or others.

Employees or contractors can abuse their position of trust to:

- ▶ access or manipulate systems without authority.
- ▶ process fraudulent requests or claims for themselves or others.
- ▶ access, manipulate, or disclose official information without authority.
- ▶ steal monetary or physical assets.




The [protective security requirements](#) outline the Government's expectations for managing personnel, physical and information security.

Bribery of public officials and the corrupt provision of official information are offences under the Crimes Act 1961.

<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that controls comply with protective security requirements ▶ Review access control procedures to ensure that it is clear when a policy applies ▶ Confirm that ‘request for access’ processes are robust ▶ Confirm that only those who need access have been granted access ▶ Review processes that distinguish requests for access from individuals who do not need access ▶ Confirm that access is removed in a timely manner ▶ Confirm that employees understand how to process access controls correctly and consistently ▶ Confirm that employees cannot bypass standard process requirements, even when pressure or coercion is applied ▶ Review access breaches to identify how they occurred and how it can be prevented in the future
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Identity verification ▶ Limit access to sensitive information ▶ Protect data from manipulation
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Impersonator ▶ The Corruptor ▶ The Exploiter

2.5 Limit access to sensitive information

Limit access to sensitive information and records.

<p>Examples</p> 	<p>This countermeasure targets internal fraud risks.</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none"> ▶ restricting and monitoring access to records of high-profile individuals. ▶ restricting and monitoring access to sensitive information, such as commercial in confidence information. ▶ security classified information is stored in secure environments.
<p>Why this is important</p> 	<p>Allowing customers, employees or third parties to access sensitive information and records without authority can lead to:</p> <ul style="list-style-type: none"> ▶ fraudsters publicly releasing sensitive information. ▶ fraudsters using the information to improperly influence decisions. ▶ fraudsters using the information to coerce others to act fraudulently. <p>Employees or contractors can abuse their position of trust to:</p> <ul style="list-style-type: none"> ▶ access, manipulate, or disclose sensitive information without authority. ▶ steal physical documents or records. <p>The protective security requirements outline the Government's expectations for managing personnel, physical and information security.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that employees understand what sensitive information is ▶ Confirm that processes comply with protective security requirements ▶ Confirm that there is a process for requesting and approving access to sensitive information ▶ Confirm that employees are aware of the processes to limit access to sensitive information ▶ Review procedures for requesting access to sensitive information. Confirm the processes are robust and actively test them ▶ Confirm employees have the right level of security clearance to access sensitive information, if applicable ▶ Confirm through testing or a process walkthrough that access controls or processes cannot be circumvented

Countermeasure supported by	<ul style="list-style-type: none">▶ Procedural instructions or guidance▶ Access controls▶ Protect data from manipulation
Related Fraudster Personas	<ul style="list-style-type: none">▶ The Corruptor▶ The Exploiter▶ The Enabler

2.6 Fraud awareness training




Train and support employees to identify red flags as a way of detecting fraud, so they know what to do and how to report any suspected fraud.

<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"> ▶ completing fraud awareness training, as part of their induction. ▶ completing fraud awareness training every 12 months. ▶ running fraud awareness campaigns. ▶ having leadership send out strong and consistent messages about ethics and fraud awareness. ▶ providing clear and accessible fraud awareness content on the employee's intranet. ▶ having targeted training that is relevant to specific roles. ▶ educating providers or grant recipients on what fraud is.
<p>Why this is important</p> 	<p>Employees who are not trained to identify and report fraud/corruption may lead to:</p> <ul style="list-style-type: none"> ▶ dysfunctional workplace cultures. ▶ fraudulent or corrupt activity going unnoticed or unchallenged. ▶ fraudsters feeling more confident that their actions will not be identified and reported. ▶ less action and accountability for preventing, detecting, and responding to fraud and corruption. ▶ unknown and unaddressed systemic fraud or corruption.
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Review training materials to determine if messages about fraud control policies are clear and relevant to employees ▶ Determine if training or reinforcement messages are regularly provided as planned ▶ Conduct interviews, workshops, or surveys with employees to ensure that they understand fraud control policies ▶ Create case studies showing situations where employees who have completed fraud awareness training have subsequently gone on to report fraud or proactively fix vulnerabilities ▶ Check that employees can easily access training and other support materials ▶ Undertake an employee survey that includes questions about understanding fraud risk and corruption, and how to report it

Countermeasure supported by	<ul style="list-style-type: none">▶ Ethical culture▶ Governance and oversight▶ Avenues to report fraud
Related Fraudster Personas	<ul style="list-style-type: none">▶ The Deceiver▶ The Impersonator▶ The Corruptor▶ The Exploiter▶ The Organised▶ The Fabricator

2.7 Parameters and limits

Apply parameters or limits to requests, claims, or processes such as maximum claim amounts or time periods. Enforce these limits using IT systems controls.

<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"> ▶ setting transaction limits for credit cards. ▶ enforcing claim limits for programme payments. ▶ restricting particular items/payments that can be claimed together. ▶ requiring employees to book the cheapest available fare for work travel. ▶ only allowing customers/clients or registered nominees to make changes to bank accounts. ▶ restricting payments for programmes so that they are made to New Zealand bank accounts only. ▶ Requiring the use of only approved providers or vendors.
<p>Why this is important</p> 	<p>Not having clear parameters in place to keep requests, claims, or processes within set boundaries can lead to:</p> <ul style="list-style-type: none"> ▶ disorganised, inconsistent practices and decision-making. ▶ other control weaknesses. <p>Fraudsters can exploit dysfunctional processes to:</p> <ul style="list-style-type: none"> ▶ receive payments or services they are not entitled to. ▶ receive payments that are larger than they otherwise would get. <p>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>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Confirm that employees understand how to use parameters and limits correctly and consistently ▶ Review a sample of completed requests or claims to confirm that parameters and limits are being applied effectively ▶ Confirm that employees have a consistent and correct understanding of the parameters and limits

<p>Suggested measures cont'd</p>	<ul style="list-style-type: none"> ▶ Confirm that parameters and limits are used by doing active testing or a process walk through ▶ Confirm that individuals cannot override or bypass parameters and limits, even when pressure or coercion is applied ▶ Confirm that reporting/reconciliation processes exist and that claims, or requests are within limits /boundaries
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Procedural instructions or guidance ▶ Automatic prompts and alerts
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Enabler ▶ The Deceiver ▶ The Fabricator ▶ The Exploiter

2.8 Procedural instructions or guidance

Provide clear, documented processes and guidance related to activities or processes to employees.

Examples



This countermeasure targets both internal and external fraud risks.

Examples of this countermeasure include:

- ▶ programme procedures and processes, or instructions for internal functions e.g. credit card acquittals.
- ▶ instructions for collecting the right information e.g. to verify eligibility or entitlements.
- ▶ procedures to help employees apply processes consistently and correctly.
- ▶ guidance to help employees make correct and ethical decisions.
- ▶ clear instructions for third parties to follow.
- ▶ instructions that incentivise detecting and reporting fraud.
- ▶ Providing instructions make it easy for employees to comply with policies and procedures.

Why this is important



A lack of clear guidance and procedural instructions can lead to:

- ▶ dysfunctional and obscure processes.
- ▶ poor management of fraud and corruption risks.

Allowing employees to disregard instructions or guidance creates a culture where incorrect processes and workarounds become the norm.

Fraudsters can take advantage of loose rules and processes to commit fraud and avoid exposure or prosecution.

Suggested measures






- ▶ Confirm that procedural instructions or guidance materials exist
- ▶ Confirm that employees can easily find and reference procedural instructions and guidance materials
- ▶ Confirm that employees understand procedural instructions and guidance materials and use them
- ▶ Confirm procedural instructions and guidance materials are regularly reviewed and updated
- ▶ Review access records of procedural instructions and guidance material to confirm employees are using it

Countermeasure supported by	<ul style="list-style-type: none">▶ Procedural instructions or guidance▶ Automatic prompts and alerts
Related Fraudster Personas	<ul style="list-style-type: none">▶ The Enabler▶ The Exploiter

2.9 Automatic prompts and alerts

Set up system prompts and alerts to warn users when information is inconsistent or irregular.

<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"> ▶ informing users or claimants up front about their obligations. ▶ alerting users that transactions do not comply with company policy e.g. when the cheapest available fare is not selected. ▶ requiring an applicant to provide correct information in an online form e.g. alerting a user when an applicant mistakenly enters a future date for their date of birth. ▶ requiring employees/applicants to confirm the accuracy of information provided, when it appears that the information may contain errors.
<p>Why this is important.</p> 	<p>A lack of automatic prompts and alerts can lead to:</p> <ul style="list-style-type: none"> ▶ fraudsters feeling more confident that their actions will not be detected. ▶ individuals deliberately or accidentally not disclosing information that could affect entitlements. ▶ individuals deliberately or accidentally providing false information or evidence to support a request or claim. ▶ insiders deliberately or accidentally accessing information or systems they should not be accessing. <p>Allowing employees, customers, and third parties to perform actions without any alerts or warnings increases the opportunity for omissions and errors.</p>
<p>Suggested measures.</p> 	<ul style="list-style-type: none"> ▶ Check that prompts and alerts are easy for users to understand ▶ Confirm that prompts and alerts are set up exactly the same across systems ▶ Confirm that prompts and alerts are implemented correctly by doing active testing or a process walk through

<p>Suggested measures cont'd</p>	<ul style="list-style-type: none"> ▶ Confirm if claims still contain errors despite the prompts and alerts that exist ▶ Measure behaviour before and after the implementation of prompts and alerts ▶ Confirm that the number of requests with errors has decreased after prompts and alerts have been implemented ▶ Confirm that employees have received prompts or alerts and know what to do in response ▶ Consult with behavioural insights experts to see if they have identified a change in behaviour after prompts and alerts were implemented
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Eligibility requirements ▶ Parameters and limits ▶ Protect data from manipulation
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Reckless ▶ The Impersonator ▶ The Deceiver

2.10 Protect data from manipulation

Put protections in place to prevent data from being manipulated or misused.

Examples



This countermeasure targets both internal and external fraud risks.

Examples of this countermeasure include:

- ▶ securing pre-filled data on forms so that it cannot be changed.
- ▶ securing reports as 'read only' to prevent manipulation.
- ▶ ensuring that data coded directly into systems cannot be manually altered.
- ▶ restricting updates to production data by restricting a system's parameters.
- ▶ restricting alterations to a system's source code outside a prescribed change management process.
- ▶ restricting changes to audit logs.
- ▶ ensuring requirements under the protective security requirements are adhered to.
- ▶ ensuring that original copies of data are recorded and stored separately.

Why this is important




Allowing data within systems or prefilled forms to be manipulated by clients, employees or third parties could allow fraudsters to:

- ▶ submit false claims using manipulated information or evidence.
- ▶ conceal or erase information or evidence.
- ▶ facilitate fraudulent payments.
- ▶ update information without authority
- ▶ improperly influence decisions using false and manipulated information.




Employees or contractors can also abuse a position of trust to access and manipulate information without authority.

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"> ▶ Review procedures or guidance to confirm it clearly specifies how data should be protected from manipulation or misuse ▶ Review controls and policies to see if they conform with protective security requirements ▶ Confirm protections are in place to prevent data being manipulated or misused ▶ Confirm protections are always applied by employees ▶ Confirm that appropriate protections and classifications are being applied by reviewing a sample of completed data requests ▶ Confirm that data has not been manipulated by doing quantitative analysis such as the reconciliation of audit logs. ▶ Confirm that data has not been manipulated by reviewing a sample of data ▶ Confirm that data cannot be manipulated by doing active testing or a process walkthrough
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Access controls ▶ Limit access to sensitive information ▶ Automatic data matching
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Fabricator ▶ The Corruptor ▶ The Deceiver ▶ The Enabler

2.11 Segregation of duties

Distribute tasks and associated privileges for a specific business process among multiple users

<p>Examples</p> 	<p>This countermeasure primarily targets internal fraud but can also mitigate external fraud such as employees falling prey to coercion or spoofing (disguising communication from an unknown source as being from a known source).</p> <p>Examples of this countermeasure include:</p> <ul style="list-style-type: none"> ▶ employees who can create and maintain vendor records cannot also process invoices. ▶ the same employee cannot make, approve, and reconcile credit card payments. ▶ multiple employees are required to be involved in approving and processing grant payments. ▶ employees who ordered assets from suppliers cannot confirm the delivery of the assets in the accounting system. ▶ the same employee cannot record the payroll information in the system and verify the calculation.
<p>Why this is important</p> 	<p>Allowing a single individual to complete multiple functions that should be segregated can lead to:</p> <ul style="list-style-type: none"> ▶ fraudulent payments. ▶ unauthorised access, manipulation, or disclosure of information. ▶ poor management of decision-making and risks. <p>Allowing employees to create a vendor, record and pay an invoice, and reconcile the payment can lead to the creation of fake vendors and fraudulent payments.</p> <p>Fraudsters can also take advantage of unsegregated duties to conceal their activities.</p>
<p>Suggested measures</p> 	<ul style="list-style-type: none"> ▶ Consult employees or subject matter experts about segregation of duties processes ▶ Confirm employees have a correct understanding of the purpose of segregation of duties

<p>Suggested measures Cont'd</p>	<ul style="list-style-type: none"> ▶ Confirm that there is separation of duties within the system where segregation of duties should apply ▶ Confirm that someone cannot override or bypass segregation of duties, even when pressure or coercion is applied ▶ Carry out quantitative and qualitative analysis of user permissions to confirm if an individual can complete multiple functions that should be segregated ▶ Confirm that segregation of duties is being applied on all occasions by reviewing a sample of completed requests/claims ▶ Confirm that a review and reconciliation process would identify users who are able to perform multiple functions when they should not be able to ▶ Review any past access breaches to identify how they occurred and how it can be prevented in the future
<p>Countermeasure supported by</p>	<ul style="list-style-type: none"> ▶ Procedural instructions and guidance
<p>Related Fraudster Personas</p>	<ul style="list-style-type: none"> ▶ The Corruptor ▶ The Exploiter ▶ The Organised



COUNTER FRAUD CENTRE

Tauārai Hara Tāware