SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter
Fraud Centre
TAUĀRAI HARA TĀWARE

Fraud Risk Assessment Good Practice Guide

OCTOBER 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

All organisations are exposed to various forms of internal and external fraud risk. When that risk becomes reality, the impact goes well beyond financial loss. Fraud against the public sector diverts resources from essential services, undermines the integrity of publicly funded programmes, and fuels ongoing criminal activity.

Understanding fraud exposure and weaknesses helps to raise awareness and inform the implementation of an effective fraud prevention programme. Because fraud is a hidden and unreported crime, the risks and impacts are often underestimated and overlooked.

Fortunately, identifying and mitigating fraud risks does not need to be difficult. A great starting point is a fraud risk assessment which helps an organisation understand their exposure to fraud risks and design and implement a fraud risk management plan. Additionally, preventing fraud ensures funds reach the people, communities, and organisations that depend on it.

1.1 Purpose of this Guide

This guide is split into three sections to help with carrying out a comprehensive fraud risk assessment:

- The **first section** is designed to help agencies plan a fraud risk assessment. It also outlines information that should be considered before beginning the fraud risk assessment.
- The **second section** sets out the fraud risk assessment process. The process consists of four steps – risk identification, risk analysis, risk evaluation and risk treatment. Each step is broken down to provide a task-by-task process for the reader.
- The **third section** provides a high-level overview and introductory insight into post-fraud risk assessment activities.

1.2 Who Should Use this Guide

This guide should be used by anyone in an organisation who is responsible for conducting fraud risk assessments. It will be of particular interest to risk owners, business unit managers, risk practitioners, assurance leads, business unit leaders and finance teams.

1.3 Key Definitions Used in this Guide

These are some of the key definitions used throughout this guide.

Countermeasures

These are policies, systems and processes put in place to mitigate risks, including fraud risks, and increase the likelihood that an organisations' objectives will be achieved. These are sometimes referred to as controls.

Fraudster Personas

The collection of tried and tested methods, or 'personas' that fraudsters commonly adopt when committing a fraudulent offence. Understanding these personas can help you to identify how a fraudster might target an organisation. You can read more about the personas in this section.

Inherent Risk

The risk to an organisation assuming there are no countermeasures in place. This is sometimes referred to as gross risk.

Residual Risk

The risk remaining to an organisation once countermeasures have been successfully applied. This is sometimes referred to as net risk or fraud risk exposure.

Risk Appetite

The type and amount of risk that an organisation is willing to accept to meet its strategic and business objectives.

Risk Tolerance

The maximum level of risk that an organisation is willing to accept.

2 Key Considerations Before Starting a Fraud Risk Assessment

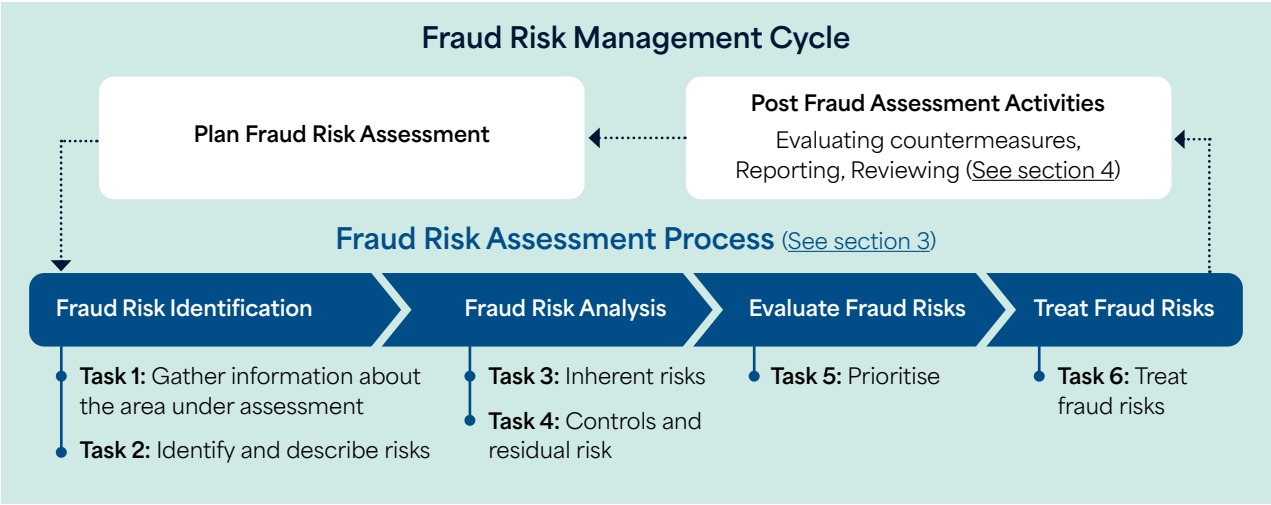
2.1 Fraud Risk Assessment Purpose

A fraud risk assessment is a fundamental part of any fraud risk management programme. It is a process to identify, describe and evaluate fraud risks within an organisation.

A fraud risk assessment helps an organisation by identifying the risks that are unique to its programmes, functions and units. It can also help those within the organisation to mitigate risks, identify gaps or weaknesses in controls, and be used as a tool to develop a practical action plan for targeting resources to reduce those risks. The information gathered within a fraud risk assessment forms an integral part of an effective counter fraud strategy.

2.2 Fraud Risk Management Cycle

Fraud risk assessments are part of the continuous fraud risk management cycle moving from planning a fraud risk assessment to the fraud risk assessment process and post-fraud risk assessment activities. By viewing a fraud risk assessment as an ongoing cycle of activity, it can help an organisation to ensure new risks and emerging threats are considered, evaluated, and then prioritised.



2.3 Enterprise Risk Management

Most organisations have an enterprise risk management framework that directs how they manage risks. Fraud risk is a type of organisational risk and should be treated in parallel with an organisation's risk management framework. This will help to ensure alignment with the organisation's overall risk management practices. For this reason, the person conducting the fraud risk assessment should coordinate with their organisation's risk management function to ensure consistency with current risk management processes.

The risk management framework for many organisations is designed following the ISO 3100:2018 Risk Management Standard ("the Standard"). The fraud risk assessment process described in this guide aligns with the Standard.

2.4 Fraud Risk Assessment Roles and Responsibilities

The "three lines of defence" model, is a widely accepted framework for effective risk management within organisations. This model helps to maintain a comprehensive and structured approach to enterprise risk management.

The three lines help to ensure that there is clarity around roles and responsibilities so that risks can be appropriately addressed and mitigated. Many organisations have a separate governing body that oversees these lines to ensure comprehensive oversight and accountability.

Here is how each of the three lines of defence can be applied in the context of a fraud risk assessment.

Line of defence	Responsibilities in the context of a fraud risk assessment
First line of defence lies with business- and process-owners and those employees responsible for day-to-day risk management and control activities.	• **Fraud risk identification:** Operational staff should be directly involved in identifying fraud risks as they work directly with organisational processes and transactions. • **Implementation of controls:** Responsible for implementing and maintaining countermeasures designed to prevent, detect and respond to fraud. • **Reporting of issues:** Report any suspicious activities or countermeasure weaknesses to the appropriate people within an organisation.

Line of defence	Responsibilities in the context of a fraud risk assessment
Second line of defence includes risk management and compliance functions that provide oversight and guidance, ensuring that the controls implemented by the first line are effective.	• **Fraud risk assessment:** Lead or facilitate the fraud risk assessment process, develop frameworks, methodologies, and tools to evaluate fraud risk across an organisation. • **Support and advice:** Support the first line in developing and enhancing controls, they can also provide training on fraud prevention and detection.
Third line of defence consists of internal audit or assurance functions, which provide independent assurance on the effectiveness of governance, risk management, and controls.	• **Independent review:** Conduct independent assessments of the fraud risk management framework and evaluates how well fraud risks are managed across an organisation. • **Audit reports:** Review and report on the effectiveness of controls, highlighting any gaps or deficiencies in fraud risk management. • **Recommendations:** Provide recommendations for improvements and then follow up to ensure that management addresses any issues identified.
Governing Body typically a board of directors or an equivalent oversight committee ensures that each line of defence is functioning effectively and that risk management practices are integrated into an organisation's strategic objectives. The governing body provides the necessary support, accountability, and oversight to enhance the overall risk management framework.	• **Approval and oversight:** Approve an organisation's fraud risk management policies and frameworks, ensuring they are comprehensive and aligned with an organisation's risk appetite. • **Strategic direction:** Define the strategic objectives for fraud risk management, including ensuring that adequate resources are allocated for fraud risk management activities. • **Review and challenge:** Challenge assumptions and conclusions drawn from fraud risk assessments to ensure they are robust and that all significant risks have been identified and addressed. • **Ensure accountability:** Hold senior management accountable for the effectiveness of fraud risk management activities. • **Promote a fraud-aware culture:** Promote a culture of integrity and ethical behaviour throughout an organisation, reinforcing the importance of fraud prevention, detection and response.

2.5 Levels of Fraud Risk Assessment

A fraud risk assessment is typically conducted at one of three levels: enterprise level, thematic/group level or detailed level.

The level an organisation chooses to conduct its fraud risk assessment will depend on several factors, including:

- size of the function, programme or unit being assessed
- complexity of the organisation and its functions
- time and resourcing constraints
- existing understanding of the fraud risks
- current fraud risk controls.

The different levels of assessment are described below in further detail to help you decide which is most appropriate for your organisation. Large or complex organisations may conduct multiple assessments at different levels to gain a clearer understanding of their fraud risk landscape. Regardless of the approach chosen, it is important to identify and consult with stakeholders from across the areas being assessed.

2.5.1 Enterprise Level Fraud Risk Assessment

An enterprise level fraud risk assessment is the most general level of assessment and gives an overview of the main fraud risks an organisation faces. It looks at the organisation and its business activities, identifying how vulnerable to fraud it might be.

This is a high-level assessment that can be used to communicate fraud risk at the board/governing body level and establish ownership of the fraud risks so they can be effectively managed.

An enterprise level fraud risk assessment should consider all the different programmes, functions or units in an organisation, as well as the overall environment. An enterprise level fraud risk assessment can help make sure that overlapping risks are considered. For example, there is often overlap between fraud and cyber security risks which can be captured at this level of assessment.

The different areas identified in an enterprise-level fraud risk assessment can then also be used to inform a thematic/group-level fraud risk assessment.

An enterprise-level assessment should be time-limited. This means that it should be updated at least annually, to ensure that any new risks are captured and that controls can be put in place.

An enterprise level fraud risk assessment may consider:

- The organisation's budget and expenditure categorised by the likelihood of fraud risk
- Identification of known and perceived drivers of fraud
- Evaluation of overall fraud risk level to the organisation
- Assessment of the organisation's fraud risk appetite
- Findings from previous audits and audit reports regarding fraud exposure
- Review of any previous fraud incidents
- Any planned new programmes or significant changes to current programmes
- Areas of uncertainty or assumptions made during the assessment.

2.5.2 Thematic or Group Level Fraud Risk Assessment

A thematic or group-level fraud risk assessment focuses on identifying and evaluating the fraud risks associated with specific themes or department in an organisation. This approach helps to pinpoint vulnerabilities and tailor risk management strategies to the unique risks facing that specific area.

This level of assessment is useful for identifying internal controls that might already be in place, vulnerable, or missing altogether. It is also important during a thematic assessment to include any activities undertaken by third parties on behalf of the organisation.

It can be helpful to use an enterprise-level fraud risk assessment to identify the high-risk areas of an organisation, which can then be prioritised for a thematic-level assessment. This might be a business unit such as people and culture, or a business process such as procurement.

In addition to the considerations for an enterprise level assessment a thematic/group level assessment may consider:

- The scope and associated business activities of the specific area
- The expenditure level of areas under assessment
- A summary of the key identified risks within the area
- Fraud risks in business areas with similar expenditure or processes.

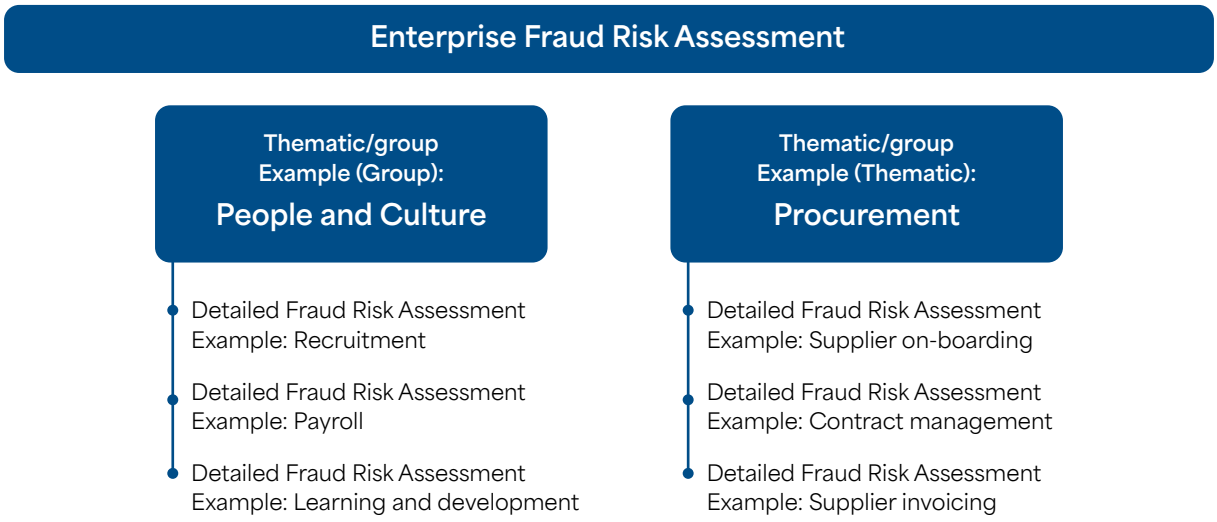
2.5.3 Detailed Fraud Risk Assessment

A detailed fraud risk assessment focuses on and provides an in-depth assessment of specific fraud risks within an individual activity. This means that instead of looking at all the functions of a business unit (e.g. all of People and Culture), it looks at a specific process or area of expenditure within that business unit. For example, it might look specifically at the recruitment process within the People and Culture area, or contract management within the organisation's procurement process.

It is recommended that this level of fraud risk assessment is conducted for higher risk operations, functions, or programmes. It can be helpful to use a thematic-level fraud risk assessment to identify which areas of the organisation these might be.

A detailed fraud risk assessment is likely to require coordination and collaboration across multiple business units. This means that they can be more resource intensive and time-consuming than other levels of fraud risk assessment.

The diagram below shows the relationship between each level of fraud risk assessments.



2.6 Document Fraud Risk Assessment Plan

It is important to have a plan for completing fraud risk assessments before you begin. This will help ensure important decisions are made before starting and that everyone involved understands roles and responsibilities.

A fraud risk assessment plan could outline:

- The overall approach to fraud risk assessment
- The scope, extent and coverage of the level of fraud risk assessment planned
- Any high profile/notable fraud risks that will be reviewed
- The rationale for the chosen area(s)
- A timeline for the delivery of the fraud risk assessment
- The key stakeholders for each fraud risk assessment.

A fraud risk assessment should be captured in a fully populated fraud risk register. To get you started we have provided a list of key data points that are typically included in a fraud risk register in Annex A. We've also created an excel version of a fraud risk assessment template with the relevant data points, so that you don't have to create your own.

3 Fraud Risk Assessment Process

Once the fraud risk assessment plan is completed it is time to start the assessment process.

A fraud risk assessment approach consists of four steps and six tasks. Each level of a fraud risk assessment involves distinct tasks to complete the assessment as shown below.

Steps of fraud risk assessment	Tasks to complete each step	Levels of a fraud risk assessment and the tasks required
One: Risk Identification 	1. Gather information about the area under assessment 2. Identify and describe fraud risks	Enterprise level up to task 1
Two: Risk Analysis 	3. Analyse the inherent risk of fraud 4. Identify countermeasures and analyse residual risk	Thematic/group level up to task 3
Three: Risk Evaluation 	5. Evaluate the fraud risks	
Four: Risk Treatment 	6. Treat fraud risks	Detailed level up to task 6

3.1 Step 1, Tasks 1 & 2 – Fraud Risk Identification

For all levels of fraud risk assessment, the initial task is to gather information about the area being evaluated. For both the thematic/group and detailed fraud risks assessments, continue on to complete the identification and description tasks in this step.

3.1.1 Task 1 - Gather Information About the Area Under Assessment

This task is essential for effective risk management and informed decision-making. To identify fraud risks, the person doing the assessment will need to gather information about the area being evaluated.

The CFC have developed a fraud risk self-assessment scan to help organisations proactively identify potential areas of fraud risk within their organisation.

Information gathering in this task includes looking in-depth into areas under assessment, and may also include identifying:

- Governance arrangements and accountability structures for fraud risk management in the organisation.
- The general types of fraud risk that are common to the area being evaluated.
- Types of fraud that have occurred in similar processes or business areas elsewhere across the organisation.
- Findings from previous audits regarding fraud exposure.
- Considerations that might make fraud more likely, such as characteristics of the customer or supplier base, or the complexity of processes and transactions.
- Relevant business processes and procedures associated with the assessment area.

3.1.2 Task 2 - Identify and Describe Fraud Risks

This task is to identify the fraud risks and describe them for thematic/group level and detailed level fraud risk assessments.

The risks identified can be recorded in the fraud risk assessment template.

Identify Fraud Risks

There are several techniques to identify and define fraud risks faced by the area under assessment. The extent of the techniques will depend on a range of factors, such as the existing knowledge of fraud risks and the scope of the fraud risk assessment. Organisations often use a combination of techniques to achieve the most comprehensive fraud risk identification.

Regardless of the technique used, it is important to identify and engage relevant employees and subject matter experts who can help to identify fraud risks. These should include (but are not limited to) employees who work in the area or activity under assessment.

The following are six common techniques used to identify fraud risks:

- **Workshops:** This involves a group of stakeholders, experts or team members coming together to generate a list of potential risks. Workshops are useful to gather information about the countermeasures that will be used later in the assessment process. They can also provide an opportunity to analyse the risks in consultation with stakeholders. Workshop participants may engage more effectively with the process if they received a pre-workshop pack and have an opportunity to think about potential fraud risks in advance. A pre-workshop pack could state the aims, objectives and methodology of the fraud risk assessment. It could also include the organisation's description of fraud and examples of fraud risks.
- **Process mapping:** This involves creating visual representations of processes to identify fraud risks. Visual representations can include business process mapping, flow charting or operational modelling. This is particularly useful when identifying fraud risks in the design phase of an externally facing government programme. Annex B provides an example of how to combine business process mapping and fraudster personas to identify fraud risks.
- **Surveys and questionnaires:** Involves input from employees, external stakeholders, or experts through surveys or questionnaires to identify fraud risks.
- **Senior executives' interviews:** Conducting interviews with senior executives to understand what they believe the fraud risks are within the organisation or their specific business area. Annex C provides a guide on key points that could be covered in these interviews.
- **Root cause analysis:** Reviewing past incidents or allegations of fraud to understand the underlying causes and potential risk. This could include speaking to people who were involved in the investigation.
- **Environmental scanning:** Examine fraud intelligence, previous fraud risk assessments, results of fraud investigations, or consider case studies from other agencies (this should not necessarily be restricted to New Zealand agencies). The CFC publishes case studies of SFO fraud and corruption investigations which can be used to identify potentially fraudulent activity in an organisation.

When identifying fraud risks it can help to consider the different methods fraudsters might use to target an organisation. The CFC have identified common tried and tested methods fraudsters use to commit financial crimes, referred to as fraudster personas.

There are seven fraudster personas to help think of different ways fraud could be committed against an organisation:

The Fabricator - invents or produces documents or information that is false. This might involve creating false invoices or other types of records for personal gain.

The Corruptor - abuses their position of entrusted power. This might involve negative incentives such as threats or intimidation, or positive incentives such as bribes or kickbacks.

The Impersonator - pretends they are another person or organisation. This might involve using false or stolen identities, attributes, or credentials.

The Deceiver - makes others believe something that is not true. This might involve providing false statements, deliberate misrepresentation or withholding facts or circumstances.

The Enabler - knowingly enables fraudulent activity. This might involve an individual who intentionally keeps themselves unaware of the circumstances to avoid responsibility.

The Exploiter - uses something for a wrongful purpose. This might involve misusing their position or privileges or dishonestly exploiting a vulnerability for personal gain.

The Organised - are groups of people who use a combination of the above methods in a planned and coordinated way. This may involve using trusted professionals or service providers to help or facilitate their criminal activities.

The fraudster persona guide is available at Fraudster Personas - Serious Fraud Office, New Zealand (sfo.govt.nz). This guide provides red flags to look out for, for each persona as well as the countermeasures organisations can use to mitigate the actions of the persona.

Describe Fraud Risks

A well described risk provides clarity, understanding and context, and enables more informed decision making and risk management. An effective method for describing fraud risk is to consider the 'Actor, Action, Outcome' approach.

An example of a poorly defined fraud risk from the invoice payment process would be "fraud in the invoice payment process". As there are often multiple ways that fraud could occur in an invoice payment process, describing a fraud risk in this way does not help to identify where the potential risk lies.

Examples of appropriately described fraud risks:

- A service provider (Actor) submits a falsified invoice (Action) to receive a payment for services not provided (Outcome).
- A service provider (Actor) coerces an official to approve and/or process a falsified invoice (Action) to receive a payment for services not provided (Outcome).
- An official (Actor) manipulates the finance system (Action) to divert an invoice payment to their own bank account (Outcome).

Use your judgement to strike a balance between capturing sufficient detail about fraud risks and documenting a manageable number of fraud risks. This can be achieved by combining similar risks and clearly documenting the various contributing factors (actors and outcomes).

3.2 Step 2, Tasks 3 & 4 - Fraud Risk Analysis

After identifying and describing fraud risks, the next step is to analyse the risks. Risk analysis is the process of understanding the likelihood of a risk happening and the consequences if it did. When analysing a fraud risk, the likelihood is understood as the probability of a risk occurring, while the consequences refer to the impact or the severity of the risk if it were to happen.

A common way to analyse risks is to use a risk matrix to match the combination of likelihood and consequence to give an estimate of the risk rating. An example of a risk matrix is documented in Annex D. This can be used if your organisation does not have a risk matrix or needs to update an existing risk matrix.

Risks are often analysed at both the inherent risk level, which assumes that there are no countermeasures in place as well as at the residual risk level, which is after countermeasures are in place.

Assessing risks at both levels can help to prioritise resources by:

- helping an organisation ensure they are not allocating excessive amounts of time and/or resources mitigating low risks, or
- identifying risks with a higher residual risk rating so that organisations can dedicate more resources to address/manage them.

3.2.1 Task 3 - Analyse the Inherent Risk of Fraud

When this task is completed the likelihood, consequence and overall inherent risk rating should be put into the fraud risk register. These ratings can be recorded in the fraud risk assessment template.

Estimating the Likelihood of Fraud

When determining the likelihood of fraud, consider the probability (chance of fraud happening) and frequency (expected number of incidents).

There are several factors which may influence the likelihood of fraud occurring including, but not limited to:

- **Lack of ethical culture:** Organisations where unethical behaviour is tolerated or not addressed are at higher risk of fraud.
- **Nature of the industry or sector:** Some industries face higher fraud risks because of the nature of their operations. For example, healthcare and government sectors often deal with sensitive data and significant amounts of funding that can be attractive to fraudsters.

- **Complex business processes:** Complex business processes can create opportunities for fraud due to difficulties in monitoring and understanding the flow of transactions.
- **High transaction volumes:** High transaction volumes are more susceptible to fraud as fraudulent activities can be hidden among legitimate transactions.
- **Geographic dispersion:** Organisations with operations in multiple locations or countries may face challenges in maintaining consistent countermeasures and oversight, making them a more attractive target for fraudsters.
- **Legacy systems and/or outdated technology:** Using outdated or unsupported technology can result in vulnerabilities that fraudsters can exploit. An organisation's IT security team will be able to provide insights into cybersecurity.
- **History of past fraud incidents:** Previous instances of fraud against an organisation can be an indicator of higher inherent risk, as this may be an indicator of systemic weaknesses that were not addressed.
- **Unpredictable external events:** Unexpected events, such as a natural disaster or public health crisis, can disrupt operations and create opportunities for fraud.
- **Time criticality:** When programme implementations are rushed, they can often be a target of fraudulent activity.

Estimating the Consequences of Fraud

Estimating the consequences of fraud can help an organisation understand potential negative effects that fraud could have on its operations. When estimating the consequence of fraud, one should consider both the duration (time before fraud is detected) and the impact (the potential severity of the fraud).

The impacts, and therefore consequences can go beyond the financial. Additional ways an organisation might be impacted include human, government outcomes, industry, government systems, security, environmental, reputational and business impacts.

The impacts to fraud guide is available at Impacts of Public Sector Fraud - Serious Fraud Office New Zealand (sfo.govt.nz).

3.2.2 Task 4 - Identify Countermeasures and Analyse the Residual Risk

The next task in the fraud risk assessment process is to identify countermeasures that mitigate identified fraud risks and analyse residual risk levels. Residual risk is the likelihood and impact of the risk occurring after countermeasures are in place. The countermeasures and residual risk rating can be recorded in the fraud risk assessment template.

Identify Countermeasures

You may find that you have already identified existing countermeasures when completing the fraud risk identification task. However, if this is not the case some methods for identifying them include brainstorming, senior executive interviews, process mapping and root cause analysis. For more information about each of these methods refer to task 2.

The CFC countermeasure guides contain a list of commonly used countermeasures. Use this list to identify and list existing countermeasures. The countermeasures guide is available at Fraud Countermeasures Guidance - Serious Fraud Office New Zealand (sfo.govt.nz).

Consider all four categories to identify a comprehensive list of countermeasures for each fraud risk.

Capability countermeasures guide expected behaviours and determine organisational culture around fraud.

Prevention countermeasures are the most common and cost-effective way of limiting the size of fraud risk. These countermeasures aim to stop fraud or reduce the likelihood of it happening.

Detection countermeasures aim to find or identify, disrupt, and reduce the impacts of fraud.

Response countermeasures help organisations respond after fraud has occurred to reduce or disrupt additional impacts.

Residual Risk

Once countermeasures have been identified the next task is to assess the residual risk rating. To do this follow the same process used to estimate the inherent risk rating and estimate the likelihood and consequences of the risk happening. The combination of the likelihood and consequence rating will provide the overall risk rating.

Here are some points to consider when evaluating the residual risk rating:

- Assessing the likelihood and consequences of fraud at residual level typically requires making assumptions about the effectiveness of the countermeasures.
- You will need to assume that countermeasures (e.g. the verifying an individual's identity) are functioning efficiently, even if you do not conduct an audit to confirm effectiveness.
- If there is evidence suggesting a countermeasure is not operating effectively (such as findings in an internal audit report), this information should be considered when estimating the likelihood and consequence of the risk.

The residual risk rating should be lower than the inherent risk rating because of the countermeasures in place to mitigate the risk. How much the residual risk rating decreases will depend on the nature, extent, and effectiveness of the countermeasures as discussed above.

3.3 Step 3, Task 5 – Evaluate Fraud Risks

Now that residual risks have been analysed the next task is to evaluate the risks. Risk evaluation is where the analysed risks are measured against an organisation's risk appetite and tolerance. This information will determine which risks will be continuously reviewed and which will be subject to treatment.

An organisation's risk appetite and tolerance should be defined in its risk management policy and framework. Risk appetite reflects an organisation's willingness to take on risk in pursuit of its objectives. Risk tolerance refers to the maximum level of risk that an organisation is willing to accept.

The nature of an organisation's business functions will influence its tolerance to fraud risks. Large service-delivery agencies may have a greater inherent fraud risk tolerance to their functions and programmes compared to regulatory compliance and law enforcement agencies.

Evaluated risks will fall into one of two categories:

- **Acceptable risks** are within an organisation's fraud risk tolerance and appetite levels. These risks will be reported on and monitored – see section 4.
- **Unacceptable risks** are outside an organisation's fraud risk tolerance and appetite and will move to the risk treatment phase.

3.4 Step 4, Task 6 - Treat Fraud Risks

In this task the most appropriate risk treatment option is applied to the risk(s). Risks that have been identified as unacceptable in relation to the organisations risk appetite and tolerance will require further treatment.

The '4Ts model' for risk treatment is a framework used in risk management to guide organisations in deciding how to address identified risks. The 4Ts stand for treat, terminate, transfer, and tolerate.

The risk treatment can be recorded in the fraud risk assessment template.

3.4.1 Treat (Decrease the Risk)

The treatment of risks with the aim of decreasing the risk is the most common option and includes implementing or strengthening existing countermeasures. Most countermeasures are designed to reduce the likelihood of the fraud, but some can be targeted at reducing consequences of fraud. For example, reducing the maximum amount of an eligibility payment can reduce the financial consequences of a fraudster's actions.

When considering new countermeasures, or addressing gaps and vulnerabilities in existing countermeasures, involving all relevant parties in the design process will achieve greater engagement and buy-in from stakeholders. As with fraud risk evaluation, it is important to get input from fraud risk owners with sufficient seniority to consider the cost of countermeasures against the risk exposure.

When designing countermeasures, consider the following:

- Are the objectives clear?
- Does it achieve what you want it to achieve?
- What assumptions were made about the purpose and effectiveness of the countermeasure(s)?
- Is the countermeasure automated or applied by people?
- Is the countermeasure being applied consistently and correctly?

The CFC have developed countermeasure guides as a useful resource for considering additional countermeasures or enhancing existing countermeasures. The countermeasures guides are available at Fraud Countermeasures Guidance - Serious Fraud Office New Zealand (sfo.govt.nz).

3.4.2 Terminate

An organisation can choose to terminate a fraud risk by deciding not to start or continue with the activity that gives rise to the risk. For example, an organisation may decide to not allow the use of laptops outside an organisation's premises if the risk of unauthorised access to those laptops is too high.

3.4.3 Transfer

Some organisations transfer risk to a third party e.g. taking out insurance. Risk transfer means that an organisation can reduce the potential impact of the risk, as they may be reimbursed for the loss. Risk transfer incurs a cost to an organisation. The cost should be lower than the potential impact of the transferred risk.

3.4.4 Tolerate

Accept the current level of risk. This is the least desirable option, and it means an organisation accepts the risk without doing anything about it. This option should be used only if the mitigation cost would be higher than the damage the incident would incur.

4 Post-Fraud Risk Assessment Activities

After completing a fraud risk assessment several actions typically follow to ensure findings are addressed and acted upon. This includes evaluating countermeasures, reporting and reviewing of fraud risks. Information in this section is not the core focus of this guide and is intended to offer a high-level overview and introduction to the topic.

4.1 Evaluating Countermeasures

Ongoing monitoring of fraud risks includes testing the effectiveness of countermeasures, which will impact the residual fraud rating and the subsequent evaluation and treatment of fraud risks.

Considering the following questions can help assess the effectiveness of countermeasures:

- What is the objective of the countermeasure and its unique role in managing the risk?
- What assumptions were made about the purpose and effectiveness of the countermeasure?
- Does the countermeasure work as designed? How do you know?
- Is the countermeasure relevant and up to date?
- Is the countermeasure automated or applied by people? If applied by people, how do you know they are applying the countermeasure consistently or correctly?
- What are the activities that support or enable the countermeasure?
- Are there backup countermeasures or fail-safes that would apply if the countermeasure did not work?
- Will the countermeasure lead to unintended changes in behaviour?

Pressure testing can help an organisation to test the strength of its countermeasures through a series of controlled testing activities. The CFC guide to pressure testing is available at Pressure Testing Guide - Serious Fraud Office New Zealand (sfo.govt.nz).

Annex E contains a qualitative and quantitative assessment rating table that can help with rating the effectiveness of countermeasures. The traffic light system is a useful way to communicate where countermeasures are effective or where vulnerabilities might require action.

Now that you have completed the fraud risk assessment and recorded the findings in the fraud risk assessment template you can move to the next task of reviewing and reporting the fraud risks.

4.2 Reporting

The design of your fraud risk reporting should be guided by the organisation's enterprise risk management framework. An example of presenting fraud risks in the form of a heat map is provided in Annex D. Fraud reports should include any assumptions you made while assessing the fraud risks and highlight any area(s) that you were unable to assess.

Reporting results to executive committees can be a useful way to influence action and encourage the undertaking and resourcing of counter fraud activities. Business units may be more inclined to take positive action if they know their counter fraud activities are being reported to an executive committee.

4.3 Reviewing

Fraud risks need to be regularly reviewed and monitored. This promotes continual improvement of management processes and systems. Sometimes only small changes to a business process can alter the inherent risk rating of a known fraud risk, resulting in the emergence of new fraud risks or impacting the effectiveness of existing countermeasures.

Fraud risks should be monitored on an ongoing basis, ideally by the business unit who manages the fraud risk. Changes in an organisation's operations could influence risks an organisation is exposed to, and the fraud risk register should be updated to reflect this.

Annex A - Fraud Risk Register Data Points

A fraud risk assessment is typically recorded in a fraud risk register. Here is a list of key data points that can be included in a fraud risk register. We've also created an Excel version of a fraud risk assessment template which you can use to record the fraud risk assessment.

Risk Identification

- Risk number
- Fraud risk description (actor, action, outcome/impact)
- Fraud risk owner
- Applicable fraudster persona.

Risk Analysis

- A short active title/description of each existing countermeasure (e.g. system countermeasures only allow limited authorised users to change bank accounts).
- The following countermeasure attributes:
  - The owner of the countermeasure
  - The type of countermeasure (capability, prevention, detection, response)
  - A description of what the countermeasure does to mitigate the risk
  - An effectiveness rating for the countermeasure
  - If monitoring or assurance is required.
- Countermeasure gaps or enablers (for example, missing countermeasures, barriers to data sharing, prevalence of false identities or perverse incentives).
- An overall assessment of the countermeasure environment.
- A description of the consequences of the fraud risk.
- Likelihood rating (this can include the probability that the fraud risk will occur and/or the frequency the business may expect the fraud risk to occur).
- Consequence rating.
- Inherent fraud risk rating (can include the rationale and/or evidence used for this rating).

Risk Evaluation

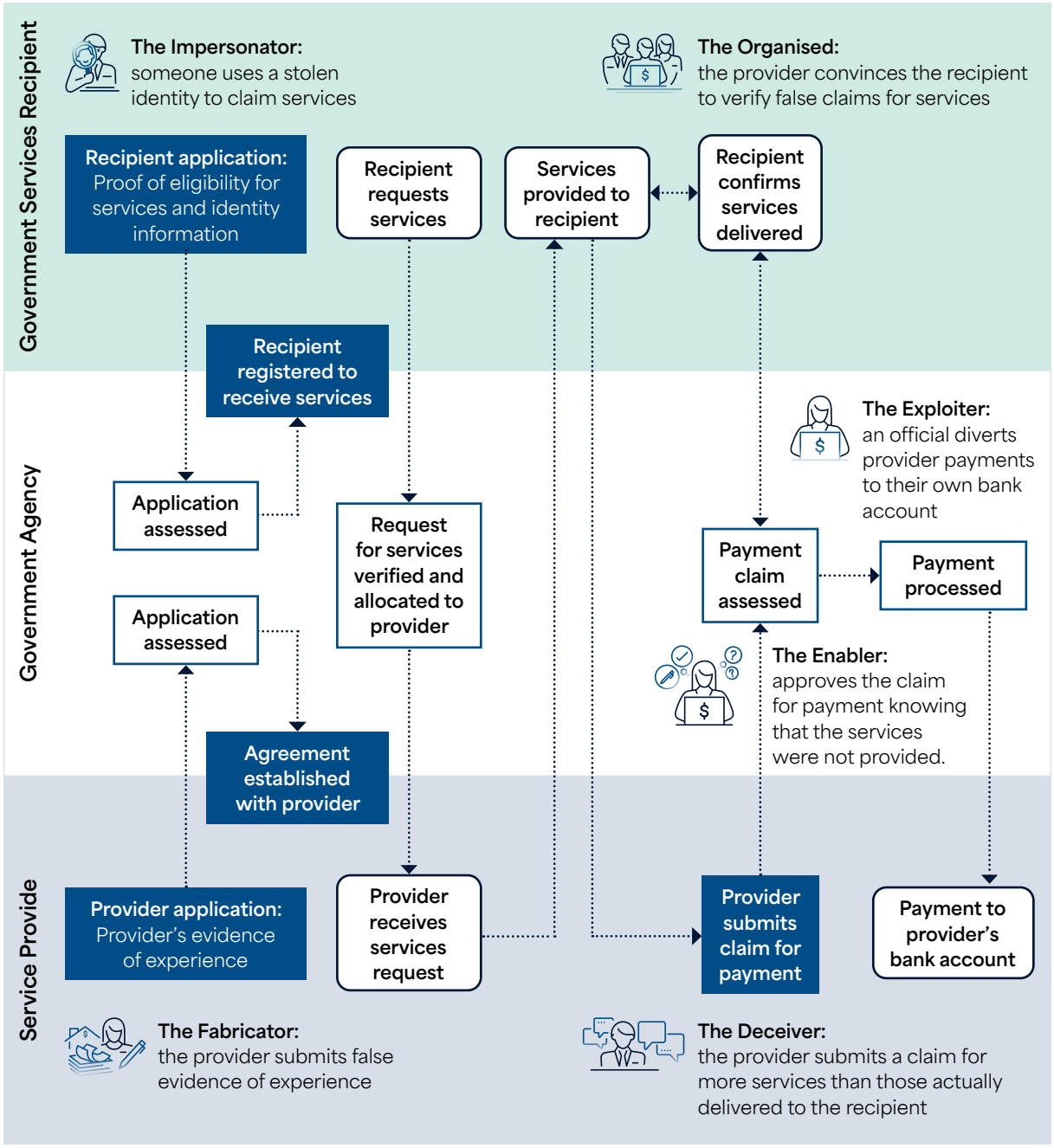
- If a decision is made to maintain existing countermeasures and monitor a risk, record the decision and a future review date.
- If a decision is made to terminate an activity to eliminate a risk, record reasons why (for example, the costs to mitigate the risk were too high).
- If a decision is made to tolerate the risk and not apply treatments, record reasons why (for example, the anticipated benefits of the activity outweigh the consequences of the risk, or the costs of additional treatment, or the timeframes to implement additional treatments, would have a negative impact on the outcomes of the activity).
- If a decision is made to undertake further risk analysis, such as conducting an audit or pressure test of the existing countermeasures, record the action to be taken and when this will be completed.
- If a decision is made to transfer a risk, record the new owner and when it will be transferred as well as how regularly this should be updated or reviewed.

Risk Treatment

- If a decision is to treat a risk, record:
  - The target risk level and the commensurate risk likelihood and/or consequence
  - A short active description of the proposed treatment or countermeasure
  - The type of countermeasure (capability, prevention, detection, response)
  - A description of what the countermeasure will do to mitigate the risk
  - A description of the implementation
  - The treatment owner
  - The implementation timeframe.

Annex B - Fraud Risk Points in a Complex Business Process

This business process map for a hypothetical public service programme illustrates how to use fraudster personas to identify points where someone might commit fraud against the programme. The business mapping process is a way to identify fraud risk (refer to 3.1) and countermeasures (refer to 3.2.2) in a business process to include in a fraud risk register.



Annex C - Senior Executive Interview Topics

These are examples of questions you could pose to senior leaders about their group/division/branch/programme to get a better understanding of the fraud risks and risk management practices of an organisation.

- What is your opinion on opportunities for fraud in your area of responsibility?
- What are the delegations of authority and financial accountabilities in your area of responsibility?
- What monitoring and oversight mechanisms are in place?
- What are the roles and responsibilities of key personnel?
- Can you provide a high-level description of the key financial processes and systems in place?
- What are the monitoring and oversight mechanisms?
- Can you comment on the performance of individual business units?
- Are there any cultural issues or challenges (such as attitude towards mistakes), or morale issues?
- Have there been any recent changes in structure, function, or systems?
- Do any of your business units have high levels of employee turnover?
- Have there been any previous incidents, including suspected and actual fraud/s?
- Are you able to share the results of recent internal or external audits, or third-party assurance reviews?
- Do employees in your area of responsibility have a good awareness of organisation fraud countermeasures, including mechanisms for reporting suspected fraud and misconduct?
- Are there any concerns you have or any other relevant issues you wish to raise?
- What is the process for reporting fraud or suspicious activities? Do your employees know about it?

Annex D - Risk Measurement (Analyse Fraud Risk)

The following risk analysis table is an example of how the likelihood of fraud risks can be measured.

Risk Analysis - Likelihood (Example Only)

Rating	Description	Meaning
5	Almost certain	It is easy for the threat to exploit the vulnerability without any specialist skills or resources, or it is expected to occur within 1-6 months.
4	Highly likely	It is feasible for the threat to exploit the vulnerability with minimal skills or resources, or it is expected to occur within 6-12 months.
3	Possible	It is feasible for the threat to exploit the vulnerability with moderate skills or resources, or it is expected to occur within 12-36 months.
2	Possible but unlikely	It is feasible but would require significant skills or resources for the threat to exploit the vulnerability or it is expected to occur within 3-5 years.
1	Almost never	It is difficult for the threat to exploit the vulnerability, or it is not expected to occur within 5 years.

The following risk analysis table is an example of how the likelihood of fraud risks can be measured.

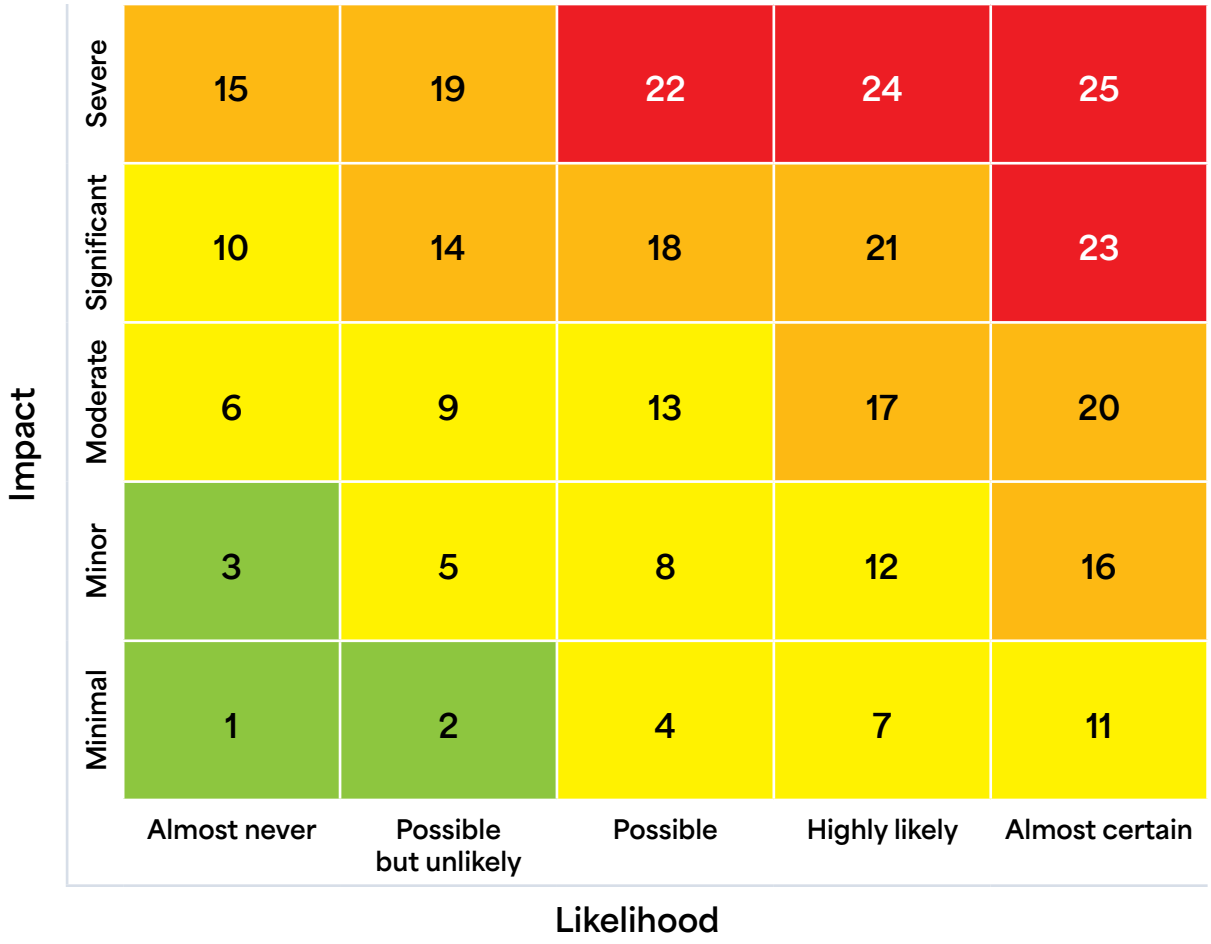
Risk Analysis – Consequences (Example Only)

Rating	Description	Meaning
5	Severe	• Could severely compromise objectives of the agency. • Could severely compromise whole programme or sub-project outcomes or benefits. • Severe on-going impact on service delivery across multiple agencies. • Severe political or reputational damage to NZ Government or multiple agencies. • Impact cannot be managed without significant extra resources (financial or human) and re-prioritisation.
4	Significant	• Could significantly compromise the strategic objectives of the agency. • Could significantly compromise whole programme or sub-project outcomes or benefits. • Significant on-going impact on service delivery across one or more agencies. • Significant political or reputation damage to the NZ Government or one or more agencies. • Chance of breach of laws or litigation against the NZ Government or one or more agency. • Impact cannot be managed without extra resources (financial or human) and re-prioritisation. • Minister is embarrassed.

Rating	Description	Meaning
3	Moderate	• Could compromise a strategic objective of the agency. • Could compromise programme or project outcomes. • Limited impact on work delivery across the NZ Government or border protection agencies. • Limited political or reputation damage to the NZ Government or one or more agencies. • Impact can be managed with some re-planning and modest extra resources (financial or human). • Minister(s) may need to be briefed. • Chance of litigation against one or more government agencies.
2	Minor	• Minor impact on work delivery across the agency. • Minor impact on a strategic objective of the agency. • Impact can be managed within current resources, with some re-planning. • Communication with key stakeholders may be needed.
1	Minimal	• No real effect on the outcomes and/or objectives of the agency. • No real effect on the strategic objectives of the agency. • Any impact on the agency's capacity and/or capability can be absorbed. • No impact to stakeholders.

The following risk analysis table is an example of what a risk management matrix could look like.

Risk Analysis Matrix (Example Only)



Risk Rating	Level of action required
Very High	The risk is beyond an organisation's risk tolerance and appetite and must be immediately mitigated or avoided. Regular review and monitoring of the risk needs to be provided to senior executives and all relevant stakeholders.
High	The risk should be mitigated or avoided unless the anticipated benefits of the activity outweigh the consequences of the risk. Regular review and reporting of the risk need to be provided to relevant stakeholders, and senior executives at their discretion.
Medium	The risk may be acceptable and regular review and reporting of the risk needs to be provided within the relevant business unit and to affected stakeholders.
Low	The risk is generally acceptable but must be monitored to make sure that the risk rating does not change.

Annex E - Countermeasure Assessment Rating Table

The following Countermeasure Assessment Rating Table can help with rating the effectiveness of countermeasures. It uses qualitative and quantitative considerations when determining the countermeasure's effectiveness. The traffic light system is a useful way to communicate where countermeasures are effective or where vulnerabilities require action.

Rating	Quantitative considerations	Qualitative considerations	Action required
Effective	• The countermeasure operates as specified 100% of the time. • The countermeasure operates as specified 90-99% of the time, however there are backup countermeasures (fail-safes) in place.	• The countermeasure is operating as specified. • The countermeasure clearly addresses the risk causes or consequences. • The countermeasure provides a reasonable level of assurance that objectives are being met.	• Continue monitoring the countermeasure.
Partially effective	• The countermeasure operates as specified 90-99% of the time. • The countermeasure operates as specified 60-89% of the time, however there are backup countermeasures (fail-safes) in place.	• The countermeasure is occasionally operating as specified. • The countermeasure partially addresses the risk causes or consequences. • The countermeasure provides little assurance that objectives will be met.	• Review the countermeasure and consider action to improve its design and/or operational effectiveness. • Consider implementing backup countermeasures (fail-safes).
Ineffective	• The countermeasure operates as specified less than 60% of the time. • The countermeasure operates as specified 60-89% of the time, and there are no backup countermeasures (fail-safes) in place.	• The countermeasure does not operate as specified. • The countermeasure does not address the risk causes or consequences. • The countermeasure provides no assurance that objectives will be met.	• Take action to replace the countermeasure or improve its design and/or operational effectiveness. • Implement backup countermeasures (fail-safes).

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

SFO | SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Te Kāwanatanga o Aotearoa
New Zealand Government