



**COUNTER FRAUD CENTRE**

Tauārai Hara Tāware



**Guide to**

**Pressure Testing**

**APRIL 2023**

# Table of Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
	1.1 Purpose	2
	1.2 What is pressure testing	2
	1.3 Common vulnerabilities	2
	1.4 What is a countermeasure?	2
<b>2</b>	<b>Scoping for Pressure Testing</b>	<b>5</b>
	2.1 Where to start	5
	2.2 Thinking like a fraudster	5
	2.3 How to identify different countermeasures	6
	2.4 Pressure test scoping types	7
<b>3</b>	<b>Pressure Testing Methods</b>	<b>8</b>
	3.1 Some ways to test countermeasures	8
	3.2 Testing methods	10
	3.3 Data analysis – Qualitative and quantitative data	12
	3.4 Choosing a process and method	13
	3.5 Determining a countermeasure’s effectiveness	13
<b>4</b>	<b>Treating countermeasure vulnerabilities</b>	<b>14</b>
	4.1 What happens if there are vulnerabilities	15
<b>5</b>	<b>Reporting, monitoring and review</b>	<b>17</b>
	5.1 Tracking the progress of a pressure test	17
	5.2 What to report on	17

# 1 Introduction

Fraud is a serious, underestimated, and often unchecked problem. All public sector organisations are exposed to fraud in some way, and many are an active target for fraudsters, scammers, and criminals. Organisations do not always consider fraud when conducting their activities or know where they are vulnerable.

This guide sets out key principles and contains materials for conducting pressure testing within public sector organisations. Conducting pressure testing enables organisations to identify fraud vulnerabilities and determine if their countermeasures work effectively. In turn, this can help organisations to prevent fraud and the devastating impacts it can have on the governments, people, industries, services, and the environment.

Fraudsters are a capable and committed adversary who actively look for vulnerabilities within government programmes. Research shows that gaps or weaknesses in countermeasures lead to more fraud than any other factor. Organisations do not always consider fraud when conducting their activities or know where they are vulnerable. Organisations are particularly vulnerable to losing oversight of risks or weaknesses in a control environment if there are new programmes being developed, they are undergoing a major restructure, or implementing new technologies.

## 1.1 Purpose

This guide is for fraud practitioners and risk managers who want to start applying pressure testing within a public sector organisation. Though it may seem daunting, pressure testing can be a simple process that requires minimal resources. This guide should be read alongside the [Counter Fraud Centre Pressure Testing Guidance](#).

## 1.2 What is pressure testing?

Pressure testing helps an organisation to measure the effectiveness of their fraud countermeasures by applying different testing methods to assess the operating effectiveness of the countermeasures. This means more than just checking if fraud countermeasures are in place or if processes are being followed. Pressure testing involves considering, and in some instances applying, common methods used by fraudsters to identify how an organisation's countermeasures could be circumvented. Pressure testing helps an organisation to find vulnerabilities and challenge assumptions about how fraud is managed within the organisation.

Pressure testers are those carrying out pressure testing. To do this, they apply creative and critical thinking, and look at processes and systems from the perspective of a fraudster. They do not assume countermeasures work effectively or trust that individuals will follow

processes, rules, and norms. Instead, pressure testers scrutinise processes and countermeasures by considering common methods of fraudsters and applying an understanding of what motivates and enables individuals to commit fraud.

Pressure testing does not need to be a complex process and can be done on a small scale with limited resources. For example, one employee can perform a pressure test, this might be as simple as an employee reviewing an existing fraud policy to determine whether the organisation was following best practice guidelines. However, the value an entity receives from pressure testing increases as it invests more resources and builds its pressure testing capability.

## 1.3 Common vulnerabilities

Organisations and fraud teams may find the following common vulnerabilities through pressure testing:

- ▶ A lack of fraud awareness
- ▶ Inadequate quality assurance
- ▶ Employees or processes not verifying information or evidence
- ▶ A lack of effective oversight
- ▶ Weak technology countermeasures
- ▶ Inadequate detection countermeasures
- ▶ A lack of reporting or reconciliation

## 1.4 What is a countermeasure

Countermeasures are individual measures, processes or functions that help organisations prevent, detect, and respond to fraud. An integrated assembly of countermeasures make up a control environment. Some organisations may also refer to countermeasures as controls.

Countermeasures vary in their purpose and application. For example:

- ▶ Cultural and behavioural factors can play a large role in encouraging or discouraging fraudulent activities. Some countermeasures such as incentives, training, or deterrence measures can:
  - Influence behaviours or decisions to encourage compliance with rules, processes, and expectations.
  - Influence behaviours or decisions to discourage non-compliance with rules, processes, and expectations.
- ▶ Process countermeasures manage risk through a consistent application of designed functions. If designed correctly, countermeasures such as mandatory requirements,

evidence verification, decision making, documentation, and quality assurance checks or audits can:

- Increase the likelihood of compliance with rules, processes, and expectations.
  - Decrease the opportunity for non-compliance with rules, processes, and expectations.
- ▶ Technology countermeasures manage risk through automated application of designed functions. If designed correctly, countermeasures such as guided procedures, data matching, audit logging, and fraud detection programmes can:
- Automatically enforce consistent compliance with rules, processes, and expectations.
  - Automatically safeguard against non-compliance with rules, processes, and expectations.

# 2 Scoping for Pressure Testing

When starting pressure testing, it is beneficial for organisations to start small and focus on a few countermeasures, using simple methods. As organisations develop their maturity and capability, they may wish to conduct more comprehensive testing and utilise more advanced methods.

## 2.1 Where to start

Organisations can scope their testing as described in the three examples in this guide. This enables them to conduct pressure testing at their preferred level of intensity. Having these options can help an organisation to build their capability over time and choose the appropriate testing for the circumstances.

An organisation must manage operational risks associated with pressure testing in accordance with its risk management policy. It can be beneficial to develop a plan to deal with outcomes from the test including communications with relevant stakeholders.

## 2.2 Thinking like a fraudster

Fraud schemes vary in their complexity and creativity. At one end of the scale, they might involve an individual stumbling upon an opportunity, such as a lack of oversight, and then taking advantage of their position and knowledge to exploit it. The other end might involve determined individuals or groups deliberately probing for ways to exploit programmes and services, and creatively using tried and tested fraud methods to mislead or exploit the system. Pressure testing is an equally creative process, and it helps to think like a fraudster when evaluating processes and testing countermeasures.

Pressure testing is more than just looking at whether countermeasures are in place and processes are being followed. Instead of simply trusting employees, providers, and participants to follow processes, rules, and norms a pressure tester must consider the common methods employed by fraudsters and look for common features or vulnerabilities in programmes or functions that motivate and enable them to commit fraud. This requires pressure testers to challenge assumptions and apply creative and critical thinking to find ways around countermeasures just like fraudsters do.

Fraudster personas represent the different types of fraudsters who might target a government programme or service. Understanding these personas will help pressure



testers consider the methods a fraudster might use to target a function or programme, or to get around a countermeasure.

The fraudster personas can be adapted to address the types of fraudsters that are specific to an organisation or programme. Fraudsters often exhibit behaviours from several different personas.

For more information about fraudster personas take a look at the [Counter Fraud Centre guides](#)

## 2.3 How to identify different countermeasures

As with identifying fraud risks, pressure testers may be able to use available fraud risk assessments to identify existing countermeasures. However, pressure testers will also likely discover undocumented countermeasures when they engage with relevant stakeholders.

The CFC have developed countermeasure guides that will be useful for pressure testers when deciding which controls they want to assess. For more information, see the [Counter Fraud Centre Countermeasure Guidance](#).

## 2.4 Pressure test scoping types

The three types of pressure test scoping that an organisation can use are:



### Targeted assessment

Beginner

An organisation can use **targeted assessments** to test individual countermeasures.

This type of assessment can help an organisation to test the effectiveness of a single countermeasure or a small number of closely associated countermeasures. These targeted and agile assessments take minimal effort and allow an organisation to selectively test key countermeasures across a wide range of systems, processes, and risks.



### Critical assessments

Intermediate

An organisation can use **critical assessments** to test only the most critical countermeasures.

This type of assessment can help an organisation to identify and test the effectiveness of the most critical countermeasures within a programme or function. This process would help to make sure an organisation focuses its resources on more critical countermeasures within a broader control environment.



### Comprehensive assessments

Advanced

An organisation can use **comprehensive assessments** to test all known countermeasures across integrated environments.

This type of assessment can help an organisation to carry out comprehensive 'deep-dive' reviews that consider multiple current or emerging fraud risks across programmes, payments, systems, and processes. They can also help an organisation assess the effectiveness of the integrated control environment at mitigating these risks.



# 3 Pressure testing methods

Pressure testers may be able to use existing fraud risk assessments to identify known risks and vulnerabilities. However, these might not always be available or helpful, and may be based on incorrect assumptions. Therefore, during planning, pressure testers may need to complete an independent assessment of risks and vulnerabilities.

## 3.1 Some ways to test countermeasures

Pressure testers can use a variety of techniques to test the effectiveness of different types of fraud countermeasures. The type of method used will most often depend on the type of countermeasure being tested. Pressure testers may also need to test countermeasures in different ways.

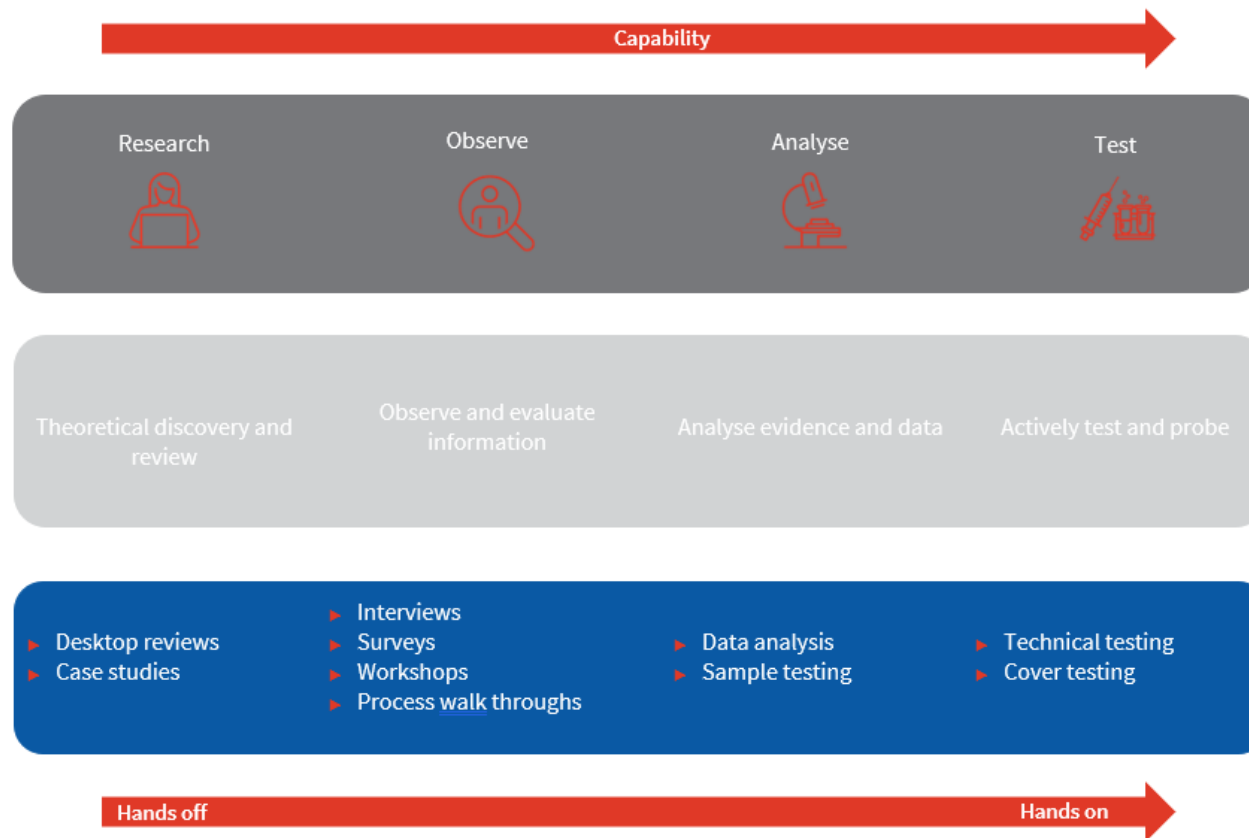
The primary method includes:

- ▶ Research – such as desktop reviews and looking at case studies
- ▶ Observation – such as process walk-throughs or workshops with stakeholders
- ▶ Analysis – such as sample reviews or data analysis
- ▶ Testing – such as technical testing or covert actions to breach countermeasures





The primary testing methods involve research and working collaboratively with stakeholders to understand and observe how countermeasures work. Stakeholder engagement is an essential component of pressure testing. Pressure testing will directly engage employees at all levels of an organisation, from senior leaders and policy experts to frontline employees. Engaged stakeholders are essential for helping pressure testers understand complex or discreet processes and procedures. Pressure testers will also need to collaborate with stakeholders to co-design fraud risk treatments.





As an organisation's capability increases, it may also want to use more advanced 'hands on' methods such as data analysis and covert testing (see figure 1 – methodology spectrum).

Figure 1 - Methodology spectrum



## 3.2 Testing methods

	Testing Method	Example
Research	 <p>Desktop reviews – Research existing documents and compare against better practice and mandatory requirements. This enables the testing officers to confirm that the design of the countermeasure is sound.</p>	Reviewing an organisation’s operational privacy policy to determine if it meets legislative, all-of-government and better practice requirements.
	 <p>Case studies – Review related circumstances where fraud has been perpetrated.</p>	Analyse the outcomes of relevant fraud investigations completed within or outside the organisation.
Observe	 <p>Interviews, workshops, or surveys – Collaborate with those involved in the implementation of a countermeasure. These can be focused on the design and/or implementation of the countermeasure.</p>	Conducting a ‘Black Hat’ workshop with stakeholders or surveying a sample of employees to get their perspective on the effectiveness of countermeasures.
	 <p>System or process walk through – An employee runs pressure testers through the process to demonstrate existing practices and how countermeasures apply.</p>	Employees walking testers through the system/process to demonstrate how a claim is processed and how countermeasures work.

	Testing Method	Example
Analyse	 <p>Sample analysis – To test against a specific policy, process, and/or procedure, this is usually used to determine compliance, but may also be useful in assessing whether something is user friendly.</p>	Checking a sample of procurements for compliance against the department’s procurement policies and processes.
	 <p>Data analysis - Collecting qualitative and quantitative data and interpreting the results to measure the countermeasures effectiveness and fraud impacts.</p>	Collecting data to determine what percentage of employees have completed fraud awareness training within the past 12 months.
Test	 <p>Technical testing – Practical testing of countermeasures to confirm they exist and to observe how they operate. Specific tests would need to be designed for different topics.</p>	Cyber security teams running tests to provide reports that demonstrate countermeasure effectiveness. For example, Penetration testing.
	 <p>Covert testing – Controlled scenario-based testing aimed at finding a way around fraud countermeasures and observing responses.</p>	Attempting to record a fake overtime claim to observe how approval, system, and reporting countermeasures work.

## 3.3 Data analysis – Qualitative and quantitative data

Depending on the assessment process chosen, an organisation may need to adopt a qualitative or quantitative approach to pressure testing.

### Examples of qualitative measurements

- ▶ Obtaining advice from subject matter experts about how countermeasures operate.
- ▶ Comparing processes and work practices against:
  - Organisational or programme policies and procedures
  - Audit New Zealand performance audit reports or guidance
  - New Zealand Standards
  - All-of-Government requirements such as the procurement principles and rules
- ▶ Checking a sample of completed activities to confirm compliance with rules, processes, and expectations
- ▶ Surveying employees to get their feedback on training or processes.
- ▶ Reviewing the results of past internal or external audits.
- ▶ Testing the functionality of system countermeasures to make sure they are operating to design specifications.

### Examples of quantitative measurements

- ▶ Analysing statistical data or comparing results against a benchmark, for example, comparing the number of employees with a privileged system access versus the number of employees who are meant to have access.
- ▶ Identifying the percentage of employees within a work unit who have undertaken fraud awareness training or information security training within the last 12 months.
- ▶ Confirming the percentage of activities that undergo quality assurance checks.
- ▶ Identifying the number of employees in Security Clearance Assessed Positions without a current security clearance.
- ▶ Reviewing detection programme results including the number of unauthorised accesses detected compared to previous periods.
- ▶ Reviewing the number and type of cases referred for investigation compared to previous periods.
- ▶ Identifying the percentage of successful prosecutions for a particular type of fraud matter.

## 3.4 Choosing a process and method

Not all of the above methods need to be applied in a pressure test. The type of process and methods chosen may depend on an organisation's resources and capabilities. For example, a targeted assessment using research and observational methods will require fewer resources and less capability than a comprehensive assessment involving more advanced analytical and testing methods.

## 3.5 Determining a countermeasure's effectiveness

After testing a countermeasure, pressure testers can consider the following questions to inform their conclusions about its effectiveness.

- ▶ What is the objective of the countermeasure and its unique role in managing risk?
- ▶ What assumptions were made about the purpose and effectiveness of the countermeasure?
- ▶ What conclusions can be drawn from the testing results?
- ▶ Does the countermeasure work as designed? How do you know?
- ▶ What else can be checked to verify the countermeasure is working as designed?
- ▶ Is the countermeasure relevant and up to date?
- ▶ Is the countermeasure automated or applied by people? If applied by people, how do you know if 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 does not work?
- ▶ Does the countermeasure lead to any unintended changes in behaviour?

The table on the following page provides guidance on the qualitative and quantitative considerations when determining a countermeasure's effectiveness. The table provides examples that can be adapted to a specific organisation. The traffic light system is a useful way to communicate where countermeasures are effective or where vulnerabilities require action.

Rating	Quantitative considerations	Qualitative considerations	Actions required
Effective	<ul style="list-style-type: none"> <li>▪ The countermeasure operates as specified 100% of the time.</li> <li>▪ The countermeasure operates as specified 90 to 99% of the time, but backup countermeasures (fail-safes) are in place.</li> </ul>	<ul style="list-style-type: none"> <li>▪ The countermeasure is operating as specified.</li> <li>▪ The countermeasure clearly addresses the risk's causes or consequences.</li> <li>▪ The countermeasure provides a reasonable level of assurance that objectives are being met.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Continue monitoring the countermeasure.</li> </ul>
Partially effective	<ul style="list-style-type: none"> <li>▪ The countermeasure operates as specified 90 to 99% of the time.</li> <li>▪ The countermeasure operates as specified 60 to 89% of the time, but backup countermeasures (fail safes) are in place.</li> </ul>	<ul style="list-style-type: none"> <li>▪ The countermeasure is occasionally operating as specified.</li> <li>▪ The countermeasure partially addresses the risk's causes or consequences.</li> <li>▪ The countermeasure provides little assurance that objectives will be met.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Review the countermeasure and consider taking action to improve its design and/or operational effectiveness.</li> <li>▪ Consider implementing backup countermeasures (fail-safes).</li> </ul>
Ineffective	<ul style="list-style-type: none"> <li>▪ The countermeasure operates as specified less than 60% of the time.</li> <li>▪ The countermeasure operates as specified 60 to 89% of the time, but no backup countermeasures (fail-safes) are in place.</li> </ul>	<ul style="list-style-type: none"> <li>▪ The countermeasure does not operate as specified.</li> <li>▪ The countermeasure does not address the risk's causes or consequences.</li> <li>▪ The countermeasure provides no assurance that objectives will be met.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Take action to replace the countermeasure or improve its design and/or operational effectiveness.</li> <li>▪ Implement backup countermeasures (fail-safes).</li> </ul>

**Note:** The measures for assessing the effectiveness of each countermeasure will vary depending on the type of countermeasure. For example, some countermeasures may not even be partially effective if they operate as specified 90% or even 99% of the time.



# 4 Treating countermeasure vulnerabilities

## 4.1 What happens if there are vulnerabilities

Pressure testers will uncover gaps and vulnerabilities in an organisation's countermeasures. The processes outlined in [Pressure Testing Assessment Process](#) encourages a collaborative, co-design approach to treating these gaps and vulnerabilities. A collaborative approach helps an organisation to:

- ▶ Achieve greater engagement and buy-in from stakeholders
- ▶ Cultivate positive and productive relationships with stakeholders
- ▶ Support stakeholders to implement robust treatments.

The **SMART** principle provides a framework of what to consider when co-designing treatments with stakeholders:

<b>Specific</b>	The treatment should have a clear and concise objective, be well-defined and clear to anyone with a basic knowledge of the work. Consider who, what, where, when, and why
<b>Measurable</b>	The treatment and its progress should be measurable. Consider: <ul style="list-style-type: none"><li>▶ What does the completed treatment look like?</li><li>▶ What are the benefits of the treatment and when will they be achieved?</li><li>▶ The cost of the treatment (both financial and employee resourcing)<ul style="list-style-type: none"><li>▪ How do the costs balance against the treatments?</li></ul></li></ul>
<b>Achievable</b>	The treatment should be practical, reasonable, and credible, considering the available resources. Consider: <ul style="list-style-type: none"><li>▶ Is the treatment achievable with available resources?</li><li>▶ Does the treatment comply with policy and legislation?</li></ul>

<b>Relevant</b>	The treatment should be relevant to the risk. Consider: <ul style="list-style-type: none"><li>▶ Does the treatment modify the level of risk (through impacting the causes and consequences)?</li><li>▶ Is the treatment compatible with the organisation's objectives and priorities?</li></ul>
<b>Timed</b>	The treatment should specify timeframes for completion and when benefits are expected to be achieved.

# 5 Reporting, monitoring and review

## 5.1 Tracking the progress of a pressure test

Organisations should create pressure test reporting trackers. These trackers should track the outcomes of pressure tests undertaken; they should be updated on a regular basis. Over time these trackers will provide insight into trends across the fraud risk environment and should be maintained in order for it to be effective. A tracker provides organisations with a holistic view of multiple pressure tests and helps them measure performance and other key metrics.

## 5.2 What to report on

Organisations are encouraged to report the findings from their pressure testing to the executive leadership team at the end of the financial year or upon request. Some suggested ideas of what could be reported on include:

- ▶ The number of pressure tests the organisation has underway, under the following categories
  - Targeted assessments
  - Critical assessments
  - Comprehensive assessments
- ▶ The number of pressure tests the organisation has completed, under the following categories
  - Targeted assessments
  - Critical assessments
  - Comprehensive assessments
- ▶ The total number of countermeasures the organisation has tested
- ▶ The number (and percentage) found to be:
  - Effective
  - Partially effective
  - Ineffective
- ▶ The number of treatments recommended, and the total number agreed to be implemented
- ▶ The number of resources dedicated to pressure testing (FTE at both the beginning and end of the financial year)

Organisations are also encouraged to provide a summary report to their executive leadership team on the countermeasures tested and the vulnerabilities found. Where available this information can also be compared to data and results from previous years

This report will support organisations to continually update and improve the catalogue of common countermeasures, and to share learnings and common vulnerabilities with key stakeholders. This report will also enable senior leaders to share the learnings between teams as well as other organisations in applying pressure testing.



**COUNTER FRAUD CENTRE**

Tauārai Hara Tāware