



**COUNTER FRAUD CENTRE**

Tauārai Hara Tāware






# Pressure Testing

# Assessment Process

APRIL 2023

## Assessment process for carrying out a pressure test

There are three types of pressure testing that can be used to conduct a pressure test. The decision will be dependent on which countermeasure an organisation chooses to test and how comprehensive the testing will be.

| Process  | Purpose   |
|--|---|
| <p><b>Targeted Assessments</b></p> <p>Testing individual countermeasures</p>  <p><b>Targeted assessment</b></p> <p><b>Beginner</b></p>  | <p>Targeted assessments help an organisation to test the effectiveness of a single countermeasure or a small number of closely associated countermeasures.</p> <p>These targeted and agile assessments take minimal effort and allow pressure testers to selectively test key countermeasures across a wide range of systems, processes, and risks.</p> |
| <p><b>Critical Assessments</b></p> <p>Testing only the most critical countermeasures</p>  <p><b>Critical assessments</b></p> <p><b>Intermediate</b></p>                         | <p>Critical assessments help to identify and test the effectiveness of the most critical countermeasures within a programme or function.</p> <p>This process helps to make sure that resources are focused on more critical countermeasures within the broader control environment.</p>   |
| <p><b>Comprehensive Assessments</b></p> <p>Testing all known countermeasures across integrated environments</p>  <p><b>Comprehensive assessments</b></p> <p><b>Advanced</b></p> | <p>Comprehensive assessments enable organisations to undertake ‘deep-dive’ reviews that consider multiple current or emerging fraud risks across programmes, payments, systems, and processes.</p> <p>These assessments measure the ability of the integrated control environment to counter these risks.</p>   |

## How do I decide which countermeasures to target?

Countermeasures selected for tests can be informed by a variety of sources including:

- ▶ Fraud risk assessments and other pressure tests
- ▶ Concerns raised by employees or senior officials
- ▶ Outcomes from fraud detection programmes
- ▶ Outcomes of fraud investigations

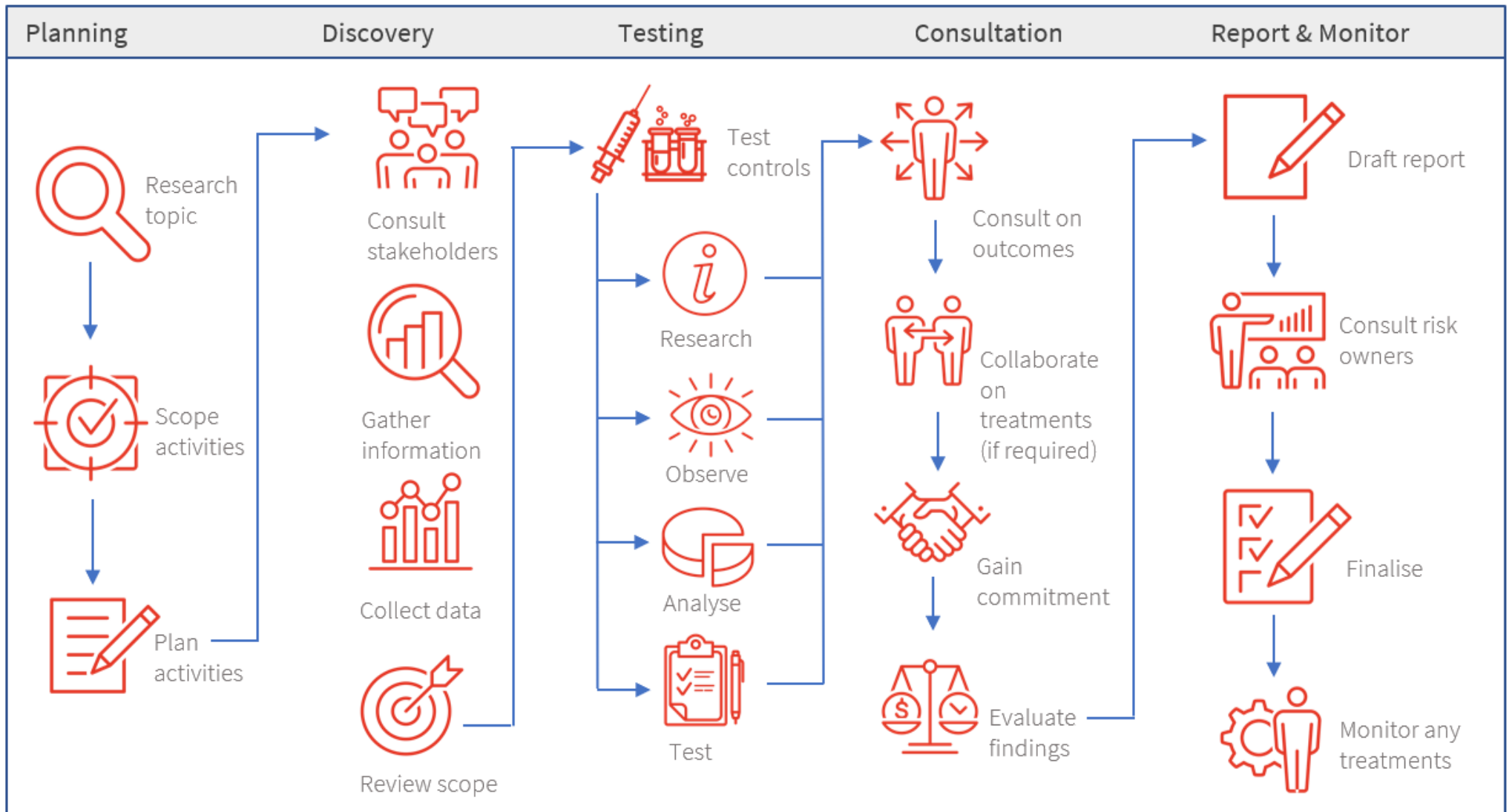
Pressure testers may also want to conduct their own research and monitor the media to remain agile and respond to emerging fraud risks.

Organisations should maintain a register of countermeasures they would like to pressure test. This register can also capture information such as:

- ▶ A description of the countermeasure
- ▶ The relevant fraud risks
- ▶ Why this countermeasure was selected
- ▶ The business area responsible for the countermeasure
- ▶ The likely Point of Contact for the countermeasure.

We recommend that organisations create a 'reporting template – pressure test tracker' in order to track the assessments that have been completed or are in process. Tracking these results will enable an organisation to plan for future pressure tests and observe any emerging fraud risks.

# Pressure Testing Process Map





## Planning Phase

### Research topic

When starting a targeted assessment, it's beneficial to research the countermeasure, the fraud risk, and the possible vulnerabilities.

Relevant fraud risk assessments may help; however, these may not always be available or useful. This research does not need to be exhaustive but can help an organisation to effectively plan and scope the pressure test.

### Plan activities

Following research, the next step is to plan the testing approach through a planning meeting or workshop.

Some key questions to consider during planning include:

- ▶ What fraud risks does the countermeasure counter? How might fraud be committed if the countermeasure did not exist or was not fully effective?
- ▶ What assumptions have been made about the impact or effectiveness of the countermeasure?
- ▶ Has this type of fraud been successfully committed in the past or against other organisations? If so, how?
- ▶ What kind of benefit might be gained from this type of fraud (money, entitlements, assets, information, influence)?
- ▶ Does the countermeasure change any actor's behaviour? If so, how?
- ▶ Are there other countermeasures (e.g. backup countermeasures or fail-safes) that need to be considered?
- ▶ Could technical or covert testing be applied to test the countermeasure? If so, can a plan be developed now or after the stakeholder has provided more information?
- ▶ What other stakeholders might want to engage, beyond the Point of Contact, to evaluate the countermeasure?
- ▶ What evidence or data would be useful to obtain? How would we collect this data?
- ▶ What are the potential vulnerabilities we might discover?

- ▶ What are some possible treatments we might need to co-design with stakeholders?

### Categorise the countermeasure

To help identify and correctly categorise different countermeasures, read [the Fraud Countermeasure Guides](#).

### Identify and contact the owner

It is important to identify the right fraud risk owner to provide the necessary advice and information about the countermeasure. This stakeholder is referred to as the Point of Contact.



## Discovery Phase

### Consult stakeholders

Pressure testers should engage with stakeholders and ask them questions about the countermeasure(s) they are testing.

Gather advice from the Point of Contact about how the countermeasure counters the fraud risk. Some information to gather from relevant stakeholders includes:

- ▶ Confirm the countermeasure examples.
- ▶ Confirm that the countermeasure counters the fraud risk(s) it is recorded against.
- ▶ Describe how the countermeasure works to counter the fraud risk
- ▶ Explain how stakeholders ensure the countermeasure is working (e.g. that the countermeasure is used, followed, enforced, switched on, monitored, and tested).
- ▶ What assumptions exist about the operation and effectiveness of the countermeasure?
- ▶ What supporting countermeasure(s) (back up countermeasures or fail-safes) exist? How do the countermeasures work together to counter the fraud risk?
- ▶ If there was an actively thinking adversary who intended to commit fraud, could they find a way around the countermeasure? If so, how would they do it?
- ▶ What are the consequences if the countermeasure did not work as intended?
- ▶ Are there any other issues that influence the effectiveness of the countermeasure?
- ▶ Are there any ways the fraud countermeasure could be strengthened?
- ▶ Are there additional fraud risk treatments that could be implemented?
- ▶ Any information, documentation, statistics/data, or stakeholder contacts that could help with evaluating the fraud countermeasure.





## Testing Phase

Pressure testers should record evaluation results and preliminary findings.

Some different ways to test countermeasures:

- ▶ 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.

Some examples of what you might like to record include:

### Fraud risk

- ▶ How fraud might occur based on Actor, Action, Outcome
- ▶ Fraud countermeasure
- ▶ Current risk rating

### Countermeasure overview

- ▶ A short outline of the nature of the countermeasure and some information about the risk/control environment it operates within.

### Evaluation of the fraud countermeasure

- ▶ Category
- ▶ Type
- ▶ Criticality
- ▶ Rating
- ▶ How it was measured
- ▶ Evaluation – including evidence to support strengths or weaknesses.

### Assessment of fraud impacts

- ▶ Articulate how the fraud might occur based on Actor, Action, Outcome
- ▶ How might fraud occur within the context of this countermeasure, e.g. what might occur if the countermeasure did not exist.



## Proposed treatment

- ▶ Succinctly describe the treatment
- ▶ Purpose - What vulnerabilities will this treatment address, and what outcomes will it achieve
- ▶ Impacts - Cost benefit analysis, impact on service delivery, any other relevant detail in relation to the treatment
- ▶ Owner
- ▶ Implementer
- ▶ Advice from implementer of treatment
- ▶ Expected completion date



## Consultation Phase

### Further consultation on preliminary findings

On completing the evaluation, pressure testers should engage with the Point of Contact to discuss the preliminary findings.

If the countermeasure is not fully effective, discuss the preliminary findings with the Point of Contact. This will allow the contact to comment on the findings and provide advice or information that might help in the final evaluation. It also gives the opportunity for collaboration with the contact on potential treatments. Pressure testers may also need to consult with other stakeholders about potential treatments.

### Co-designing treatments for vulnerabilities

Pressure testers should work with stakeholders to co-design treatments for any identified vulnerabilities.

When deciding on which treatment to use, consider the following:

- ▶ The purpose of the treatment – what fraud risks will the treatment mitigate, what vulnerabilities will it address, and what is the anticipated outcome
- ▶ Who the treatment owner and implementer will be
- ▶ The implementation process – what steps will be involved
- ▶ The estimated cost of the treatment
- ▶ The expected outcome – will it achieve the purpose, how can this be measured?
- ▶ The expected timeframe.



## Report and Monitor Phase

### Reporting

A final report should be created to present the pressure testing findings and to serve as a record of the relevant results. The report should include all advice and approvals from treatment owners. You can consider including the following in the report:

- ▶ A short summary of the countermeasure
- ▶ A list of key findings
- ▶ An evaluation of the countermeasure's effectiveness
- ▶ Recommended treatments (if required)
- ▶ An evaluation of the fraud risk and a risk assessment table
- ▶ Key stakeholders and their relationship to the countermeasure or treatments.

### Monitoring the implementation of treatments

It is recommended to develop a process for recording and monitoring the implementation of agreed treatments. This can track alongside the preliminary findings, results of the assessments, and the final report.



**COUNTER FRAUD CENTRE**

Tauārai Hara Tāware