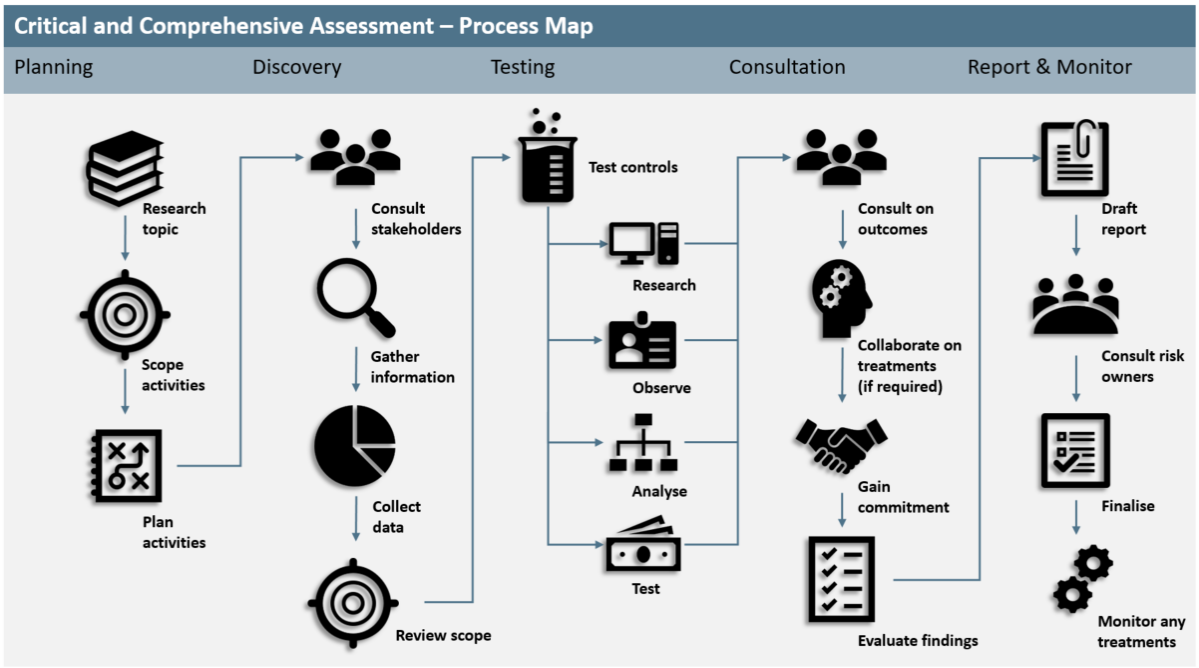
Attachment B – Critical and Comprehensive Assessment Processes

Process	Purpose
Critical assessments Testing only the most critical countermeasures	Critical assessments help identify and test the effectiveness of the most critical countermeasures within a program or function. This process helps make sure resources are focused on entities with more critical countermeasures within a broader control environment.
Comprehensive assessments Testing all known countermeasures across integrated environments	Comprehensive assessments help undertake comprehensive 'deep-dive' reviews that consider multiple current or emerging fraud risks across programs, payments, systems and processes, and assess the effectiveness of the integrated control environment at countering these risks.



How to decide what to pressure test

The pressure test's subject can be informed by a variety of inputs including:

- fraud risk assessments and other pressure tests
- concerns raised by staff or senior officials
- outcomes from fraud detection programs
- outcomes of fraud investigations.

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

This allows entities to maintain a register of potential pressure tests. This register can capture information such as:

- a description of the potential pressure test
- how this potential pressure test was identified
- what stakeholders would be involved
- what type of pressure test would be most suitable (critical or comprehensive).

> **Tip:** You may also want to develop a pressure testing forward work plan (a pool of pre-authorised pressure tests) and have this approved by an appropriate senior official. You can then prioritise these pre-authorised pressure tests using the PTP01 - Guide - Priority Assessment Tool.
>
> Consider recalibrating your work plan every 12-24 months to account for changes to team resources, organisational learning and emerging risks.

Once a pressure test has been allocated, pressure testers can track its progress using the PTP02 - Reporting Template – Pressure Test Tracker.

Planning phase

Research topic

When starting a pressure test, it is beneficial to research the topic and identify the known fraud risks and possible vulnerabilities. Relevant fraud risk assessments may help. However, these might not always be available or helpful. This research is not expected to be exhaustive but can help effectively plan and scope the pressure test.

Scope and plan activities

Following the research, the next step is to meet with colleagues to plan the approach to testing through a planning meeting or workshop. Pressure testers can use the PTP03 - Guide – Pressure Test Planning Workshop to help cover the right questions and capture notes during these meetings or workshops.

Some key questions to consider during planning:

- What is the scope of the pressure test?
- How might fraud be committed within this scope if the countermeasures did not exist or were not fully effective?
- Has this type of fraud been successfully committed in the past or against other entities? If so, how?
- What kind of benefit might be gained from this type of fraud such as what's the incentive - money, entitlements, assets, information or influence?
- What countermeasures are in place that we know about? Are there other countermeasures that need to be considered?
- What assumptions have been made about the impact or effectiveness of the countermeasure?
- Does the countermeasure change any actor's behaviour? If so, how?
- How would we or our stakeholders measure the effectiveness of these countermeasures?
- Who are our key stakeholders for this pressure test?
- Who might we need to engage?

- What evidence or data would be useful to obtain and how would we collect this?
- Could technical or covert testing be applied to test the countermeasures? If so, should a plan be developed now or after the stakeholders have provided more information?
- What are the potential vulnerabilities we might discover?
- What are some possible treatments we might need to co-design with stakeholders?

On completion of the research and planning pressure testers can use the PTP04 - Plan Template – Pressure Testing Plan to seek approval from an appropriate senior official.

> **Tip:** You can also use the PTP17 - Report Template – Detailed Pressure Test Report to start recording your research findings.

Discovery phase

Consult stakeholders

Once the Pressure Test Plan has been approved by the appropriate senior official, consult with other relevant senior officials about the objectives and scope of the pressure test. Pressure testers can use the PTP05 - Email Template – Initial SES engagement to facilitate this consultation.

The plan may need updating following feedback from other relevant senior officials. Pressure testers can use the PTP06 - Email Template – Follow-up SES consultation on updated plan (if required) to share and seek further input on the updated plan.

Gather information and data

Once responses have been received from relevant senior officials pressure testers can begin engaging with their nominated points of contacts (POCs).

Pressure testers can contact POCs by phone or in person to introduce themselves, provide an overview of the process, explain their role in the process and organise an appropriate time to have a meeting with them and other subject matter experts. Pressure testers can then schedule the meeting using the PTP09 - Meeting Template – Preliminary POC engagement meeting.

At the meeting, discuss the purpose of the pressure test and their role in the process and build rapport with the POCs. Objectives for these meetings are:

- using the knowledge and expertise of stakeholders by building trust and inviting them to be part of the process rather than the subject of it
- confirming that the countermeasures exist and operate as described
- understanding how the countermeasures work to counter the fraud risk
- determining how stakeholders know the countermeasures are working (the countermeasures are used, followed, enforced, switched on, monitored and tested)
- identifying any supporting countermeasures (backup countermeasures or fail-safes) that exist? How do the countermeasures work together to counter the fraud risk?
- considering if there was an actively thinking adversary who intends to commit fraud, could they find a way around the countermeasures? If so, how would they do it?
- understanding what the consequences might be if the countermeasures do not work as intended

- identifying any other issues or concerns with the countermeasures
- identifying any fraud risk treatments that could be implemented to address vulnerabilities
- obtaining any other information, documentation, statistics/data or stakeholder contacts that could help with evaluating the countermeasures.

It is beneficial to have a colleague at these meetings to take minutes. The next step is to use the minutes to create a 'record of conversation' (ROC). Pressure testers can use the PTP10 - Document Template – Record of Conversation. Distribute the ROC to all attendees to make sure the content of the ROC is an accurate reflection of the conversation that occurred. Pressure testers can use the PTP11 - Email Template – Verify ROC with POCs to share and seek further input on the ROC. Once verified by the relevant stakeholder, file the ROC with the pressure testing records.

Stakeholders may need to be contacted with some follow up questions. This follow up can occur via email or over the phone. If over the phone, send an 'as discussed' email to the stakeholder to verify the additional information they provided.

Begin cataloguing and categorising countermeasures

On receiving information from different stakeholders pressure testers can start cataloguing the different countermeasures identified. Pressure testers can also start recording information about the design and purpose of each countermeasure. Pressure testers can use the PTP17 - Report Template – Detailed Pressure Test Report to begin recording information about countermeasures.

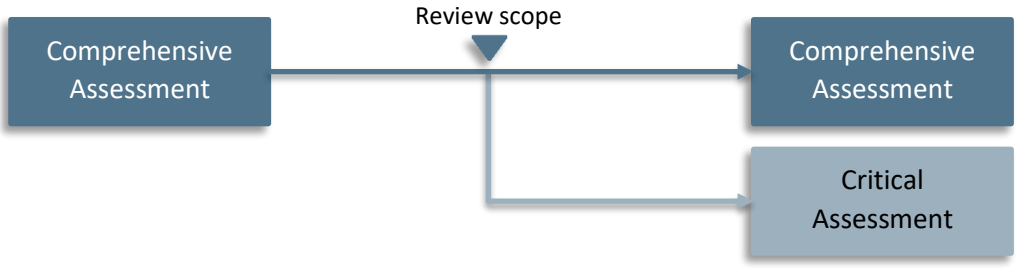
Assigning countermeasures into categories (prevention, detection and response) helps structure the report and will help correctly measure the countermeasures' effectiveness. The PTP15 - Catalogue of Fraud Countermeasures can help identify and correctly categorise different countermeasures. This catalogue also provides guidance on how to measure different types of countermeasures.

Review scope

Not all of the countermeasures identified will have the same impact on the risk. If all the countermeasures are not tested with the same level of detail, more time and effort than necessary is likely to be spent to provide an adequate level of assurance.

It is beneficial to rate each countermeasure from 1-5 based on how critical it is to countering the fraud risks. For example, countermeasures that have little or no impact on the risk can be rated 1, while absolutely critical countermeasures can be rated 5.

Once pressure testers have identified the risks and assessed the criticality of each countermeasure, they can review the scope of the analysis and evaluation. At this stage the scope of a comprehensive assessment could be reduced to a critical assessment if necessary. When determining this, consider the nature of the pressure test, the risk ratings and the information gathered up to that point. For example, where there is a high risk of fraud, it may be appropriate to evaluate the effectiveness of all the countermeasures. However, where there is a medium or low risk of fraud, it may be preferable to evaluate only the most critical countermeasures.



Tip: If you decide to undertake a Critical Assessment, identify the critical countermeasures that will remain in scope for analysis and evaluation. Also keep a record of the other countermeasures you have discovered and include them in any relevant fraud risk assessments.

You may want to designate an appropriate official to approve this decision (an EL2) and file the decision with your pressure testing records. You may also need to note this decision in your final report.

Testing phase

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.

See Chapter 4 of the Commonwealth Pressure Testing Framework for guidance on testing and evaluating the effectiveness of fraud countermeasures.

See **Attachment C** for guidance on technical or covert testing. Pressure testers can use the PTP12 - Plan Template – Technical and Covert Plan to plan and obtain approval for technical or covert testing.

The PTP15 - Catalogue of Fraud Countermeasures provides guidance on how to measure different types of countermeasures. The catalogue gives:

- a summary of each countermeasure
- specific examples of each countermeasure
- an explanation of the purpose of each countermeasure
- suggested ways of measuring the effectiveness of each countermeasure
- vulnerabilities to consider for each countermeasure
- dependencies with links to other countermeasures that can be considered within a broader control environment.

Pressure testers can use the PTP17 - Report Template - Detailed Pressure Test Report to record evaluation results and preliminary findings.

See Chapter 4 of the Commonwealth Pressure Testing Framework for guidance on determining the effectiveness of countermeasures.

> **Tip:** This is a good stage to revisit your narrative. People seek out patterns to help make sense of information. Therefore, order your report in way that tells a logical story. This is your narrative which is a fundamental structure that should remain consistent throughout the report.
>
> Developing a narrative doesn't need to be complicated. For example, your narrative would tend to follow the end-to-end process if your pressure test relates to a specific payment or process.

Consultation phase 

Co-designing treatments for vulnerabilities

Pressure testers can use the table under Appendix 2 of the PTP17 - Report Template – Detailed Pressure Test Report to record treatment ideas for identified vulnerabilities. This table helps testers consult with stakeholders on the following:

- The purpose of the treatment – what fraud risks will the treatment counter, what vulnerabilities will it address and what will it do?
- 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 and how can this be measured?
- The expected timeframe.

> **Tip:** It is crucial that you consult with relevant stakeholders (including treatment implementers) prior to finishing your report. This will help you co-design appropriate and cost-effective treatments and increase the likelihood they will be approved by senior officials. You can use the PTP19 - Meeting Template – POC collaboration on findings and treatments to help this consultation.

Report and monitor phase 

Drafting the Executive Pressure Test Report

At this point in process pressure testers will have drafted the Detailed Pressure Test Report and consulted with relevant stakeholders about the outcomes and treatment ideas.

Pressure testers will now need to present the pressure test findings to relevant senior officials and seek their approval to implement the proposed treatments (if required). Pressure testers can use the PTP23 - Report Template – Executive Pressure Test Report to help:

- communicate this information in a clear and precise way
- document advice and approvals from treatment owners.

The Executive Pressure Test Report is based on the detailed report but is much more concise. If the above template is not used, consider including the following in the report:

- A cover page that includes a summary of the process or function that was assessed, the results of the pressure test, the number of recommended treatments and the residual risk rating.
- A clear subject overview to provide context.
- A summary of key findings.
- A high-level evaluation of fraud risks.
- A high-level assessment of fraud impacts.
- A high-level evaluation of the fraud countermeasures.
- Recommended treatments (if required).
- Advice about the residual risk if the treatments are implemented.

The PTP24 - Guide – Writing an Executive Pressure Test Report can help to draft a clear and compelling report.

> **Tip:** The more you know about a subject, the harder it is to write for an uninformed reader. This is a natural cognitive bias called 'the curse of knowledge bias'. It results in communication that assumes the reader possesses a similar level of knowledge to you which they may not actually possess.
>
> To overcome this, you need to assume the reader knows hardly anything about the subject. This doesn't mean providing even more information. It instead requires only the *necessary* information written in a well-ordered way to support your conclusions.

Report consultation and approvals

Pressure testers can use the PTP25 - Meeting or Email Template – SES results collaboration to facilitate consultation with relevant senior officials. This meeting or email allows the executive pressure test report to be shared with relevant decision-makers, such as risk and treatment owners, and agreement sought on any proposed treatments.

> **Tip:** If you facilitate a meeting, have your detailed pressure test report on hand in case you are asked to provide more detail. Also bring a colleague along to these meetings to take minutes.

Finalising the pressure test

The report may need to be amended following the meeting with relevant senior officials. If so, the PTP26 - Email Template – Finalising Pressure Test can be modified to circulate the amended report.

Monitoring the implementation of treatments

It is recommended develop a process for recording and monitoring the implementation of agreed treatments. The PTP02- Reporting Template – Pressure Test Tracker can help keep track of these and follow up if required.