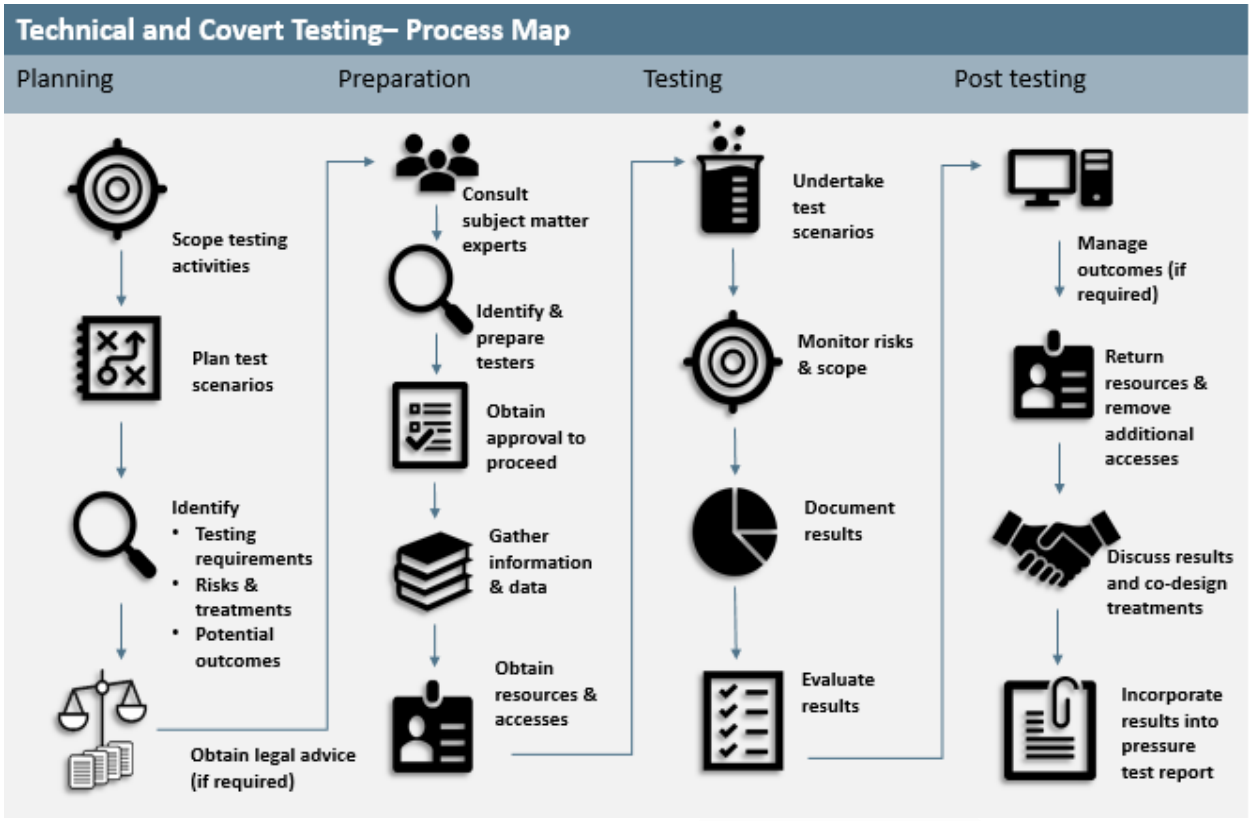
Attachment C – Technical and Covert Testing

Method	Purpose
Technical testing	Practical testing of countermeasures to confirm they exist and observe how they operate. Specific tests would need to be designed for different topics.
Covert testing	Controlled scenario-based testing aimed at finding a way around fraud countermeasures and observing responses.



Note: The above process map outlines the key steps for undertaking technical or covert testing during a pressure test. These steps are an extension to the processes outlined in Attachments A and B of the Commonwealth Pressure Testing Framework (the Framework).

Key principles

The following key principles apply to technical and covert testing performed under the Framework:

1) All technical and covert testing must be undertaken in accordance with the guidance outlined in this framework and the technical and covert testing plan.

2) Detailed technical and covert testing plans must be completed for all pressure tests where technical and covert testing will be undertaken. The plan will specify:
   - who will perform testing
   - the purpose and objectives of testing
   - the scope of testing
   - testing requirements
   - record keeping requirements
   - test scenarios
   - potential risks and counters
   - how anticipated or potential outcomes will be managed.

3) Technical and covert testing plans must be approved by an appropriate senior official within the entity subject to the testing.

4) Additional test scenarios may be developed (if required) based on weaknesses identified during the testing. These are to be included as an appendix to the approved plan. Written approval must be obtained from a designated official before these additional test scenarios are undertaken. This designated official does not need to be the senior official who approved the original plan.

5) Anticipated risks and outcomes must be recorded in technical and covert testing plans. This includes potential risks and outcomes relating to testers, other staff, and external parties such as program participants, Commonwealth assets or Commonwealth finances. Appropriate measures and counters must also be included in technical and covert testing plans to manage identified potential risks and outcomes.

6) Legal advice must be obtained if there is any uncertainty over legal risks for the staff or entity conducting the test.

7) Financial impacts for the Commonwealth, external parties and staff must be minimised or avoided in all circumstances. If applicable, technical and covert testing plans must include potential financial impacts to the Commonwealth, identify how monies will be recovered and require signed agreements as to the method of repayment by those involved in testing.

8) Detailed records must be kept for all testing activity. This will make sure:
   - all the plans, decisions, actions and outcomes related to the testing are identified, captured, managed and retained
   - records can be used as evidence to support the findings and recommendations of the pressure test
   - testers are protected if activity related to the technical and covert testing plan is detected and investigated.

Roles and responsibilities

Roles and responsibilities for senior officials:

(a) Adhere to the key principles outlined above.
(b) Make sure appropriate approvals are received before testing commences.
(c) Manage operational risks associated with technical or covert testing.
(d) Make sure risk management principles are the basis for all planning and decision making.
(e) Make sure all testers understand their responsibilities when undertaking technical or covert testing.
(f) Make sure all testers hold appropriate security clearances.
(g) Make sure all testers have agreed to and signed all declarations and acknowledgments.
(h) Support and protect the testers in the event of an investigation arising from activities included within the scope of the technical and covert testing plan.
(i) Manage the provision and return/removal of resources (including system access) required for technical and covert testing activities.
(j) Manage the repayment of monies acquired by testers through technical or covert testing in accordance with the agreed method of repayment.
(k) Understand confidentiality obligations and the privacy and secrecy provisions of the legislation that the entity administers.
(l) Perform sufficient due diligence in respect of work health and safety, protective security, legal and information security risks.
(m) Understand risks associated with the technical and covert testing.

Roles and responsibilities for testers:

(a) Adhere to the Key Principles outlined above.
(b) Make sure appropriate approvals are received before testing commences.
(c) Understand and acknowledge their responsibilities with undertaking technical or covert testing.
(d) Make sure they have agreed to and signed all declarations and acknowledgments.
(e) Comply with relevant guidelines, instructions and policies as they relate to work health and safety, protective security and information security.[1]
(f) Comply with their confidentiality obligations and the privacy and secrecy provisions of the legislation that the entity administers.
(g) Be aware of the risks associated with the technical and covert testing and recognise, communicate and respond to emerging or changing risks.
(h) Notify the entity when resources (including system access) are no longer required for testing, and make sure the return/removal of resources are finalised.
(i) Comply with the repayment of any monies acquired through the technical and covert testing in accordance with the agreed method of repayment.

[1] Where it is not a direct requirement of the technical or covert testing.

(j) Understand the full sequence of events for all activities, including those not being tested, to minimise unintentional impacts on fraud detection or investigation resources.

Planning and support

As outlined in the key principles above, a technical and covert testing plan must be completed for all pressure tests where technical and covert testing will be undertaken. Pressure testers can use the PTP12 - Plan Template – Technical and Covert Plan to plan and obtain approval for technical or covert testing. The template provides additional guidance on planning requirements.

Testing requirements and support

Testing performed under this framework will involve scenario-based testing to evaluate the effectiveness of countermeasures, detection processes and prevention strategies, and explore options to find a way around them.

Any requirements for support from stakeholders or specialist staff or contractors must be included in the technical and covert testing plan. Supporting staff must only be provided with detail of the pressure test on a need to know basis.

Managers may also be required to support testing activities. For example, they may need to approve access or resource requests for the testers. This may require these managers to complete a declaration of consent to participate in testing.

All testers must complete a declaration and acknowledgement of their understanding of their responsibilities and the risks associated with testing. Pressure testers can use the PTP12a - Declaration and Acknowledgement Form (Technical and Covert Testing).

Technical testing may require support from a range of stakeholders within the entity to provide access to testers and test risks related to specialist functions. For example, pressure testers may require specific building or system access or require specialist support to effectively test countermeasures.

Covert testing is generally performed without the knowledge of other staff or stakeholders. This helps to test the countermeasures in their natural state, making sure the results are not contaminated by any pre-awareness or preparation.

Managing potential or expected outcomes

Testing for financial gain

When undertaking technical or covert testing, pressure testers may attempt to find a way around countermeasures to see if fraud can occur. This can involve performing what would be considered unauthorised activity in normal conditions to try and acquire payments, information or assets.

Technical and covert testing plans should include any potential outcomes from testing and plan for how the potential outcomes will be managed. For example, if there is a possibility of a test scenario resulting in a payment to the tester, the technical and covert testing plan must detail how the money will be returned and require the pressure tester to sign an agreement as to the method of repayment.

It is recommended that the financial impact from testing be minimised. For example, a test could demonstrate a vulnerability by diverting $10 rather than $10,000. Where possible, it is beneficial for payments to be stopped at the final step or reversed immediately to avoid overpayments occurring.

The entity is responsible for making sure all pressure testers have agreed to and signed all declarations and acknowledgments. The entity is also responsible for managing the repayment of monies transferred through technical or covert testing in accordance with the agreed method of repayment.

Pressure testers are equally responsible for complying with the repayment of monies transferred through technical or covert testing in accordance with the agreed method of repayment. Pressure testers can use the PTP12b - Agreement as to method of repayment (Technical and Covert Testing) to obtain agreement from testers regarding the specific methods of repayment.

Return of resources and removing additional access
Any resources or additional access required for technical or covert testing (such as building or system access) must be returned/removed as soon as the need for them expires. This could be before the conclusion of all the technical or covert testing activities.

The entity is responsible for managing the provision and return/removal of resources (including system access) required for technical or covert testing activities.

The pressure testers are equally responsible for notifying the entity when resources (including system access) are no longer required for technical or covert testing and making sure the return/removal of resources occurs.

Detection assurance
Technical or covert testing activities can, where applicable, assess the effectiveness of the entity's detection countermeasures. This adds further value by:

- validating the entity's ability to detect unauthorised activity
- providing assurance that detected unauthorised activity is appropriately referred for investigation.

Keeping records of plans, actions and outcomes

Detailed records must be kept for all testing activity. This will make sure that:

- all the plans, decisions, approvals, actions and outcomes related to the testing are identified, captured, managed and retained
- records can be used as evidence to support the findings and recommendations of the pressure test
- testers are protected if activity related to the technical and covert testing plan is detected and investigated.

What records should be collected during testing?
The type of information collected during technical or covert testing can include but may not be limited to communications, decisions and actions related to the test scenarios outlined in the technical and covert testing plan and the details of any additional test scenarios. This may include:

- documents (e.g. file notes, emails etc.)
- sworn statements (affidavits)

- transcripts
- photographs
- screen captures
- access logs
- transaction reports.

Pressure testers can use the PTP13 - Document Template – Technical and Covert Testing – Methods and Results and/or the PTP14 - Document Template – Technical and Covert Testing – Summary spreadsheet to document the results of each test scenario.

It is beneficial to file all records associated with technical and covert testing with pressure testing records.

The results and conclusions from technical and covert testing can be recorded and communicated in the pressure test report.

Managing risks

Operational risks associated with technical or covert testing can be managed in accordance with the entity's risk management policy. Risk management principles must be the basis for all planning and decision-making.

A risk assessment must always form part of the technical and covert testing plan. Each plan will include a risk register that contains risks specifically related to the technical or covert testing to be undertaken and identify appropriate risk treatments. This risk assessment can consider possible risks beyond the immediate results of testing (e.g. second and third order consequences).

Responsible officials and testers will be responsible for managing identified risks and recognising, communicating and responding to emerging or changing risks.