International Public Sector Fraud Forum
Bringing countries together to fight public sector fraud

International Public Sector Fraud Forum

A Guide to Pressure Testing

February 2022

Cabinet Office

Commonwealth Fraud Prevention Centre

GAO

Produced in collaboration with the UK Cabinet Office, Australia's Commonwealth Fraud Prevention Centre and the US Government Accountability Office.

With case study contributions from:

- The Association of Certified Fraud Examiners (United States of America)
- The Australian Commission for Law Enforcement Integrity (Australia)
- The Department of Agriculture, Water and Environment (Australia)
- The Government Accountability Office (United Sates of America)
- The Queensland Crime and Corruption Commission (Australia)
- The Victorian Auditor-General's Office (Australia)

Crown copyright disclaimer

The information contained in the International Public Sector Fraud Forum documentation and training is subject to Crown Copyright 2021.

You should not without the explicit permission of the International Public Sector Fraud Forum:

- copy, publish, distribute or transmit the Information;
- adapt the information;
- exploit the information commercially or non-commercially for example, by combining it with other information, or by including it in your own product or application.

The information should not be published or distributed in any way that could undermine the values and aims of the International Public Sector Fraud Forum.

This content consists of material which has been developed and approved by the International Public Sector Fraud Forum.

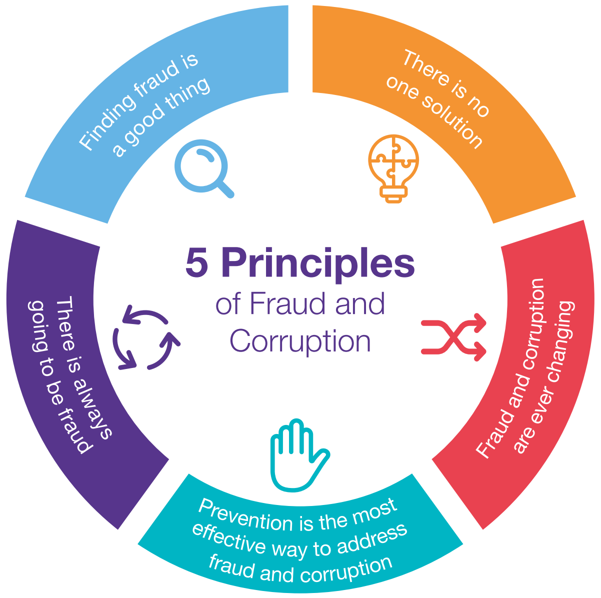
Contents

CASE STUDIES

The International Public Sector Fraud Forum

The International Public Sector Fraud Forum (IPSFF) currently consists of representatives from organisations in the governments of Australia, Canada, New Zealand, the United Kingdom and the United States. The collective aim of the Forum is to come together to share best and leading practice in fraud management and control across public borders.

The Forum has established 5 principles for public sector fraud.


5 Principles
of Fraud and Corruption
Finding fraud is a good thing
There is no one solution
Fraud and corruption are ever changing
Prevention is the most effective way to address fraud and corruption
There is always going to be fraud

1. There is always going to be fraud

It is a fact that some individuals will look to make gains where there is opportunity, and organisations need robust processes in place to prevent, detect and respond to fraud and corruption.

2. Finding fraud is a good thing

If you don't find fraud you can't fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.

3. There is no one solution

Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk. It also requires cooperation between organisations under a spirit of collaboration.

4. Fraud and corruption are ever changing

Fraud, and counter fraud practices, evolve very quickly and organisations must be agile and change their approach to deal with these evolutions.

5. Prevention is the most effective way to address fraud and corruption

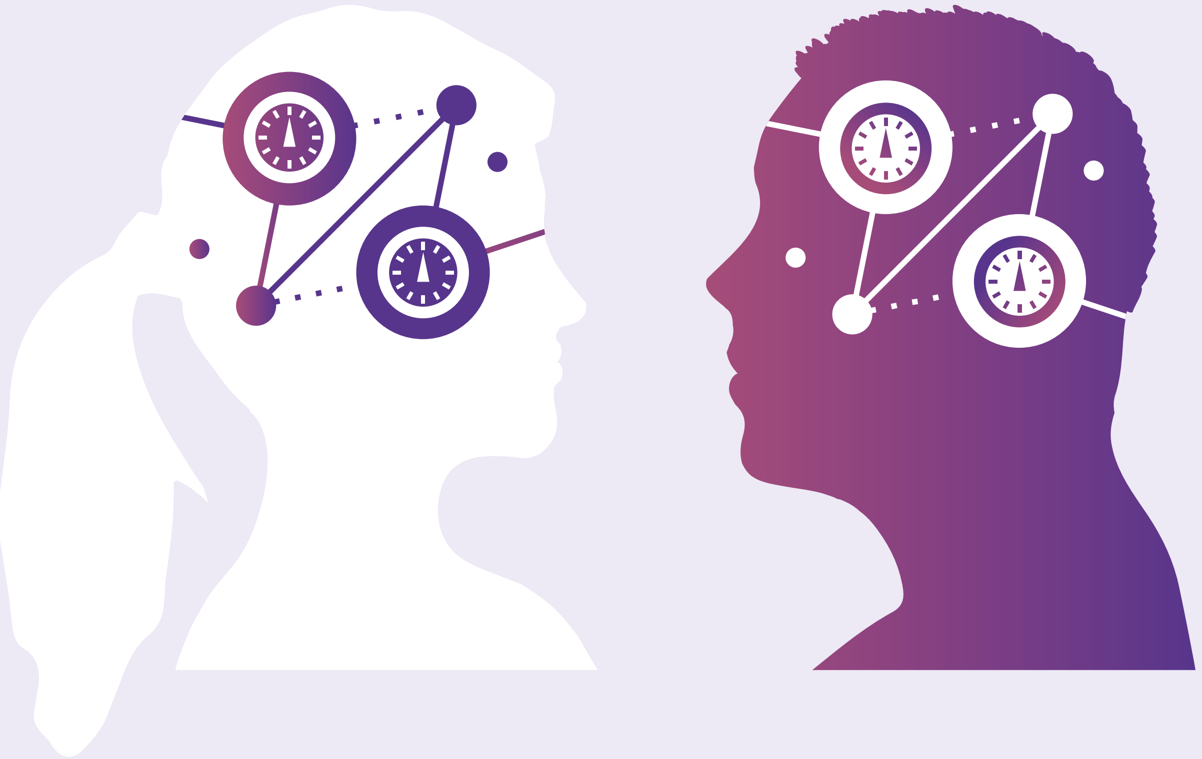
Preventing fraud through effective counter fraud practices reduces the loss and reputational damage. It also requires less resources than an approach focused on detection and recovery.

Introduction: What is Pressure Testing?

Pressure testing[1] refers to the process of examining processes and fraud controls under different conditions (or pressure) to better understand how they operate, measure their effectiveness and proactively identify any control gaps or vulnerabilities.

This involves applying creative and critical thinking and examining processes and systems from the perspective of a fraudster. It also involves employing a range of different testing methods to examine how controls work, eliminate blind spots, uncover vulnerabilities and challenge assumptions about how fraud is managed by public bodies.

In some circumstances this can involve covert testing, where officials simulate methods used by fraudsters to identify how controls respond and how they could be circumvented by malicious actors.



[1] Also often referred to as integrity testing, stress testing, control testing, penetration testing, ethical hacking or white hat hacking.

CASE STUDY

Testing the security of government buildings[2]

The Victorian Auditor-General's Office in Australia undertook covert tests of the physical security measures, access control and security culture at certain government buildings. The objective of this audit was to determine whether the buildings were sufficiently secure to prevent unauthorised access and other criminal or antisocial behaviour that may threaten the safety of staff, visitors and members of the public. The Auditor-General's Office used covert testing in combination with a number of other audit procedures including:

- **Interviewing officials who worked at the buildings.**
- **Observing security controls at selected sites.**
- **Engaging a specialist security consultant to undertake risk assessments.**
- **Physical security testing of selected sites.**

The covert testing found some examples of staff questioning testers and verifying identification. However, in some circumstances auditors could bypass physical security measures. The auditors also identified serious breaches of physical and information security. For example, at one site, they could easily access discarded, sensitive information.

Ultimately the audit found that the security infrastructure at the facilities was adequate, but its effectiveness as a deterrent to unauthorised access was undermined by human error, enabled by a weak security culture.

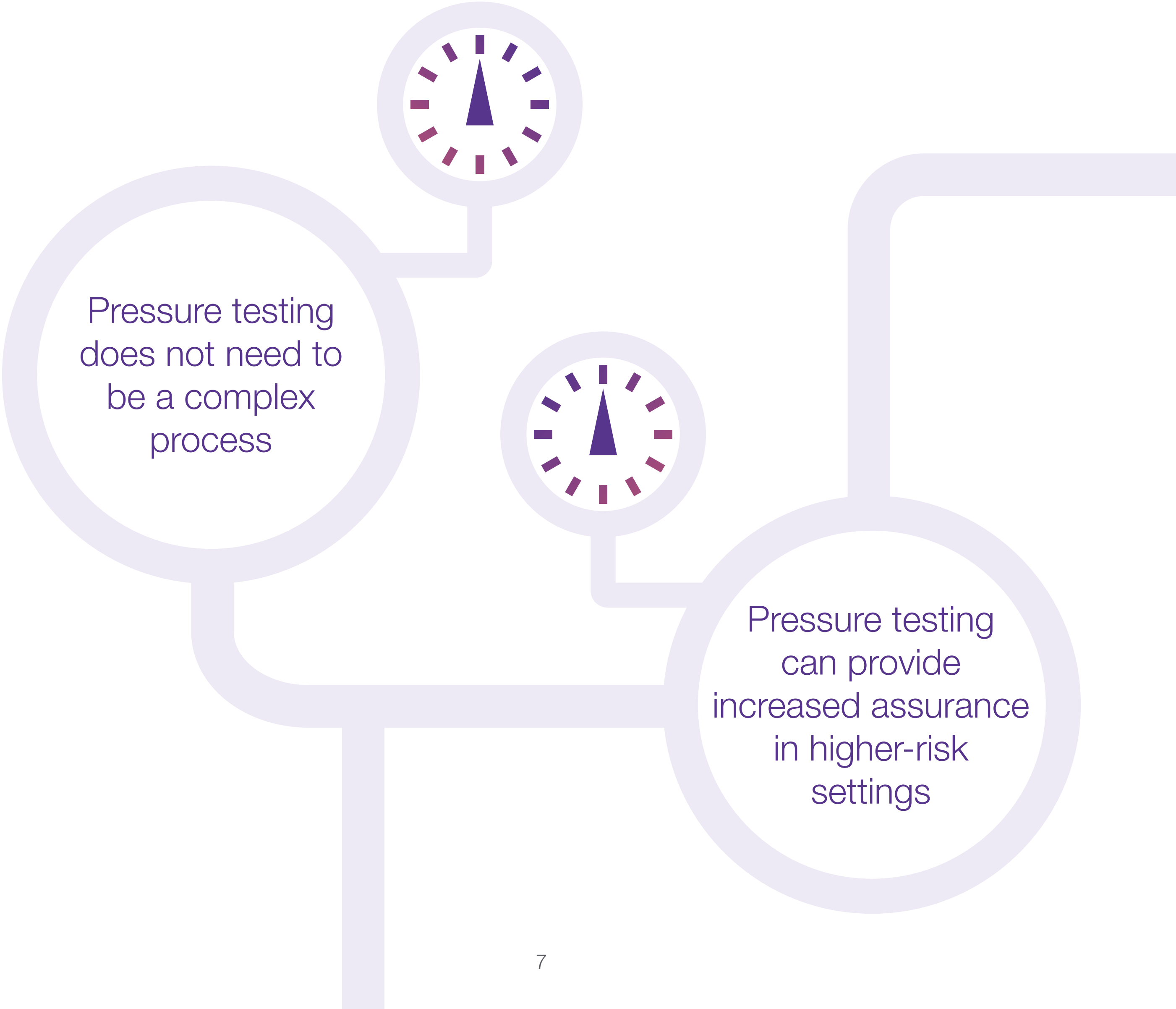
[2] Victorian Auditor-General's Office (2019), Security of Government Buildings

Purpose of this Guide

This guidance is designed to help officials to understand what pressure testing is and how it can benefit public bodies in their efforts to manage fraud and other integrity risks.

Pressure testing does not need to be a complex process. This guide includes basic processes and methods that can be used by any public body to test the effectiveness of fraud controls.

More comprehensive and sophisticated methods for pressure testing outlined in this guide, such as covert testing, can also be employed by public bodies and supreme audit institutions to provide increased assurance in higher-risk settings.



Pressure testing does not need to be a complex process

Pressure testing can provide increased assurance in higher-risk settings

CASE STUDY

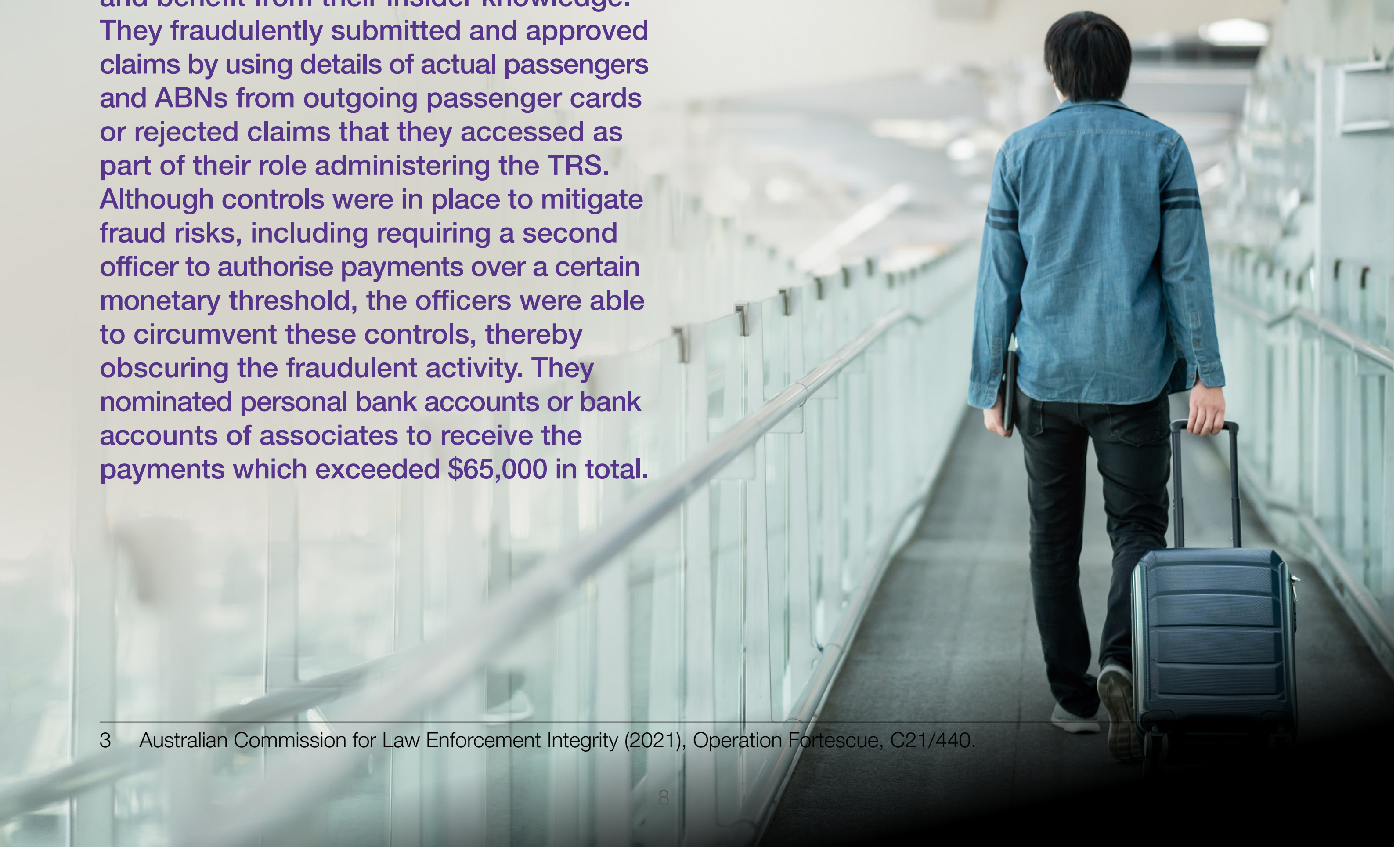
Abuse of office and opportunism: a recipe for fraud and corruption[3]

Between 2017 and 2018, three Australian Border Force (ABF) officers stationed at different international airports across Australia processed fraudulent Tourist Refund Scheme (TRS) claims. The TRS is an Australian Government initiative that allows international travellers departing Australia to claim a tax refund on goods they have purchased in, and are taking out of, Australia. The ABF administers the TRS at Australian international airports and ports on behalf of the Australian Taxation Office.

The officers' role processing TRS claims placed them in an ideal position to circumvent fraud and corruption controls and benefit from their insider knowledge. They fraudulently submitted and approved claims by using details of actual passengers and ABNs from outgoing passenger cards or rejected claims that they accessed as part of their role administering the TRS. Although controls were in place to mitigate fraud risks, including requiring a second officer to authorise payments over a certain monetary threshold, the officers were able to circumvent these controls, thereby obscuring the fraudulent activity. They nominated personal bank accounts or bank accounts of associates to receive the payments which exceeded $65,000 in total.

All three officers were convicted of the criminal offence of obtaining a financial advantage by deception and repaid the amounts they had fraudulently obtained.

This case study highlights the need to regularly test and question assumptions about the effectiveness of fraud controls, particularly when these may be subject to certain monetary thresholds that could be exploited by insiders familiar with the system. This investigation also illustrated the importance of regularly monitoring and auditing the effective implementation of processes to ensure they conform to policy and record-keeping requirements.



[3] Australian Commission for Law Enforcement Integrity (2021), Operation Fortescue, C21/440.

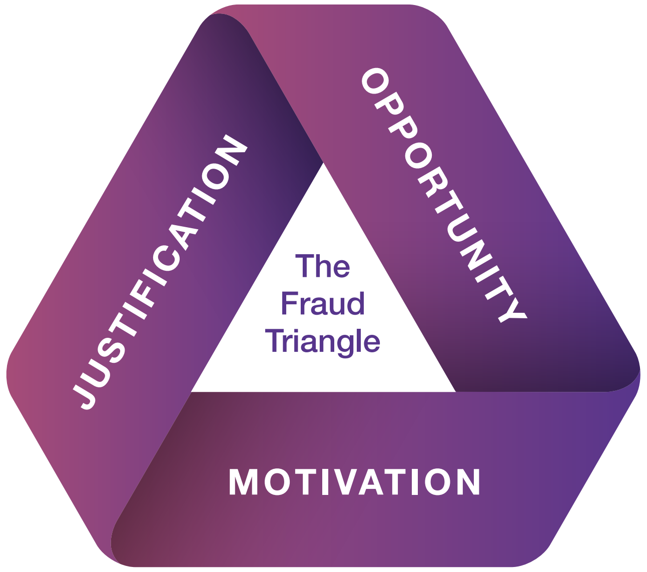
Why is there a need for pressure testing?

Global research shows that gaps or weaknesses in controls lead to more fraud than any other factor.

A 2018 survey by the Association of Certified Fraud Examiners revealed the most prominent weaknesses contributing to fraud is a lack of internal controls (30 per cent) and the ability to override internal controls (19 per cent of cases).[4] In a 2016 study, KPMG found that weak controls were a contributing factor to 61 per cent of frauds.[5]

'Opportunity' is the component of the fraud triangle that public bodies can meaningfully control. And when public bodies neglect this responsibility the impacts can be significant. A 2018 study by PwC found that of all the points in the triangle, 'opportunity' was the leading contributor to the most disruptive fraud.[6]

Public bodies are also particularly vulnerable to losing oversight of risks and weaknesses in control environments during periods of disruption,[7] and when undergoing major restructures or implementing new technologies.[8] This is a common situation for public bodies.



[4] Association of Certified Fraud Examiners (2018), Global Fraud Study.

[5] KPMG (2016), Global Profiles of the Fraudster.

[6] PwC (2018), Global Economic Crime and Fraud Survey.

[7] KPMG Australia (2021), Fraud Risk Survey.

[8] New South Wales Independent Commission Against Corruption (2017), Keeping it together: systems and structures in organisational change.

CASE STUDY

Internal control weaknesses lead to the loss of a princely sum[9]

Reported by the Queensland Crime and Misconduct Commission as potentially the single greatest fraud ever committed in the Queensland public sector, New Zealand man Hohepa Morehu-Barlow (Barlow), defrauded Queensland Health out of AU$16.69 million between 2007 and 2011.

Barlow was employed by Queensland Health and promoted in the organisation based on qualifications from a fake law degree. Throughout his employment, Barlow gained detailed knowledge of the organisation's financial systems and the mechanisms involved in disbursing large amounts of grant funds. He used this knowledge to send public monies to a third-party account before moving the funds into his own bank account.

Barlow successfully camouflaged his criminal activity by creating a smokescreen persona — misrepresenting himself as a wealthy "Tahitian prince" — that appears to have disarmed suspicion and effectively forestalled management action. He also took advantage of relationships with colleagues — in particular, by exploiting the trust of subordinate staff.

The amounts of money Barlow stole increased significantly over time and were used to fund a lavish lifestyle and to give expensive gifts to friends, family and colleagues, including bosses. The fraud continued until November 2011, when Barlow initiated a payment of $11 million in one transaction. The excessively large payment aroused suspicion in a mid-level employee of Queensland Health, where a subsequent investigation revealed that the company receiving the payment was controlled by Barlow. Barlow pleaded guilty at court in 2013 to a string of offences including forgery and aggravated fraud and was sentenced to 14 years in jail.

In this case, a range of internal control weaknesses, such as recruitment checks, compliance to policy and managerial oversight, exposed Queensland Health to long term fraud. Had these controls been working as designed or tested for control effectiveness, Barlow's fraud could have been easily detected sooner or prevented altogether.

[9] Queensland Crime and Corruption Commission (2013), Fraud, financial management and accountability in the Queensland public sector: An examination of how a $16.69 million fraud was committed on Queensland Health.

Benefits of Pressure Testing

Pressure testing is a proven way for public bodies to proactively identify and eliminate blind spots. If public officials know where their programs and functions are vulnerable, they are better equipped and informed to reduce the opportunity for fraud.

Pressure testing will improve how your public body manages fraud. It will help to:

Find weaknesses or gaps in your controls that individuals or criminal groups could exploit

Improve your understanding of different functions, programs and risks within your public body

Provide assurance that your public body's fraud risks are being effectively managed

Develop closer working relationships between counter fraud officials and stakeholders

Increase awareness of fraud across your public body and help officials to acknowledge the risk of fraud and the potential for vulnerabilities

Maintain program integrity during organisational change.

CASE STUDY

A ‘well respected’ colleague exploits internal control vulnerabilities to commit fraud[10]

A long serving and well-respected US Department of Defense employee was able to commit fraud due to “relaxed internal controls” in the Air Force’s payroll system. Michelle Holt began her scheme slowly at first, dishonestly using a co-worker’s credentials to log into the payroll system and retroactively add a few hours of overtime to her paycheck. Once this scheme failed to raise any red flags, Holt grew in confidence and started adding false overtime payments to herself on a regular basis. As her confidence grew, so did her greed; she began adding holiday and sick pay. This scheme continued for over 17 years and ultimately resulted in Holt defrauding the federal government out of $1.4 million.

After pleading guilty to the fraud charges, Holt hugged the federal prosecutor in an expression of remorse and guilt for breaching the trust of her long-time employer and colleagues. Holt was sentenced to four years in prison.

This case shows that even trusted colleagues and friends are capable of committing fraud where there is opportunity and serves as a warning to other public bodies to regularly assess fraud risks and test internal controls. A pressure testing on the Air Force’s payroll system would likely have revealed vulnerabilities in the controls and helped strengthen the system. For example, requirements for employees to regularly update passwords and regular audits would have helped prevent and detect this type of fraud.

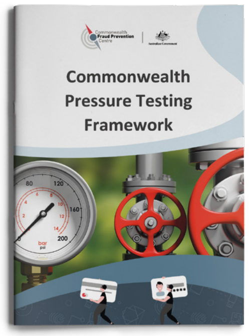
[10] Association of Certified Fraud Examiners (2019), Air Force Secretary Scams Government Out of $1.4 Million Using Simple Fraud Method.

Testing processes

The development of pressure testing in jurisdictions like Australia and the US demonstrate that effective capabilities can be built through iterative improvement. This can be achieved by starting small, delivering consistent wins, and having the patience to continually improve processes and output over time. These outcomes can create an increasing snowball of evidence to invest even more resources into pressure testing.[11]

The Australian Government’s Pressure Testing Framework outlines three pressure testing processes with increasing levels of intensity.

This tiered approach gives public bodies the flexibility to choose the most appropriate type of process to suit their needs. It also helps public bodies to start small and build their capability over time.



Targeted Assessments

These help public bodies quickly test a single control or a small number of closely associated controls.

Example

While performing their regular duties an official identifies a potential flaw in their public body’s credit card acquittal system that creates an opportunity for internal fraud. This flaw might allow someone in certain circumstances to make a purchase, acquit the transaction and reconcile their own spending, with no checks required from another official.

The official alerts the Pressure Testing team of the potential vulnerability. In response, the team conducts a Targeted Assessment on the acquittal process and confirms the flaw. The team then uses its findings to work with business and ICT stakeholders to fix the vulnerability.

[11] Commonwealth Fraud Prevention Centre (2020), Counter Fraud Investment Cases Leading Practice Guide, p. 12.

Critical Assessments

These help public bodies identify and test only the most critical controls within a program or function.

Example

Following a large data breach at another public body, the Pressure Testing team are tasked to review the department's information security controls. The team starts out by identifying existing controls their department has in place. To reduce the size and scope of the exercise, they identify the most critical controls to undertake a Critical Assessment. They work closely with subject matter experts to understand how critical controls are applied in practice. They also review data on access and extraction to ensure only authorised officials are accessing data holdings.

In addition to the internal testing of controls, the team researches data breaches in other organisations, both domestically and globally. This expands the team's understanding of the causes and impacts of data breaches and strengthens their proposals to implement treatments. The team's findings lead to stronger controls that both reduce the likelihood of a breach and improves crisis planning and response if a breach were to occur.

Comprehensive Assessments

Comprehensive Assessments help public bodies test multiple controls across a program or function and assess the effectiveness of a broader control environment.

Example

Prior to a major transformation program, the Pressure Testing team decide to review the public body's procurement practices to determine if they could allow for fraud. Due to large amount of upcoming procurement, the team undertake a Comprehensive Assessment of all relevant controls.

The team starts by reviewing the public body's policies and procedures to confirm they are in line with whole-of-government policies. They also review a sample of recent procurement processes to confirm that correct processes were applied on all occasions. The team then undertakes covert activities to try and work around system access controls, segregation of duties controls and approval workflows. This comprehensive testing helps the team identify a range of vulnerabilities, which helps the procurement team implement timely treatments to mitigate fraud associated with the transformation program.

Testing methods

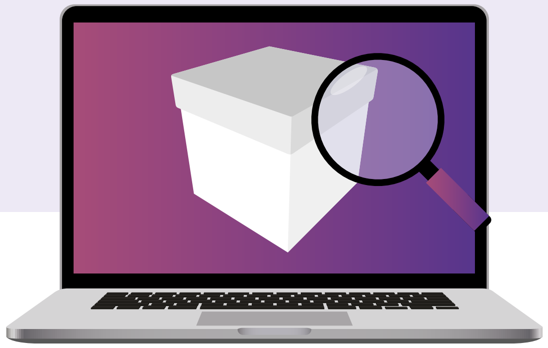
The Australian Government's Framework identifies 8 methods for testing fraud controls. These range from basic methods such as desktop research and observing process walk-throughs, through to more advanced methods such as data analysis and covertly testing processes and controls.

Basic testing methods will always be a necessary part of pressure testing as they provide valuable evidence of how processes, systems and controls operate. These methods are especially useful for public bodies who are building their capability.

Technical and covert testing can detect vulnerabilities that other assessments cannot. Relying on desktop reviews, interviews and system or process walkthroughs to find vulnerabilities can be misleading. Business functions are often overconfident about the strength of their controls, while procedures or system specifications don't always tell the true story of how things operate.

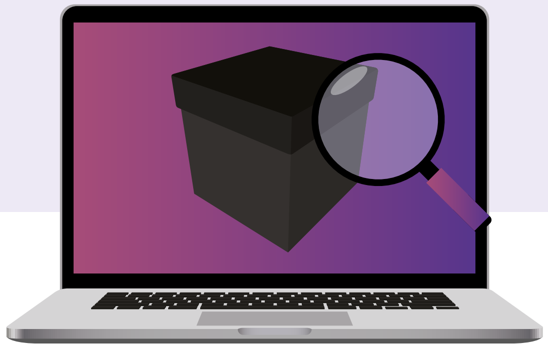
Whitebox Testing

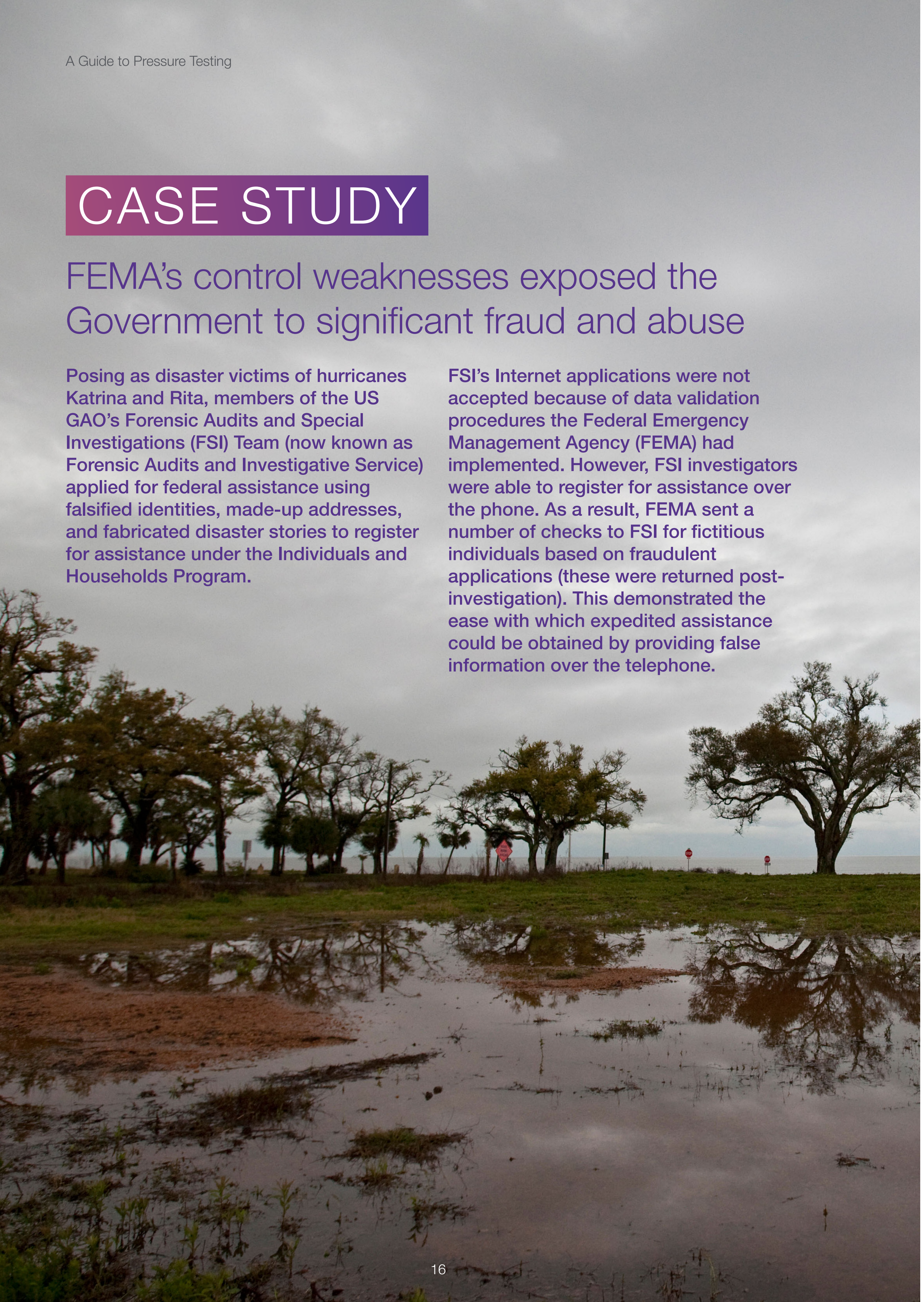
Technical testing (or Whitebox testing) involves practical testing of controls to confirm they exist and observe how they operate. This testing may require support from business functions to provide information and access to testers to help them identify vulnerabilities in systems and processes.



Blackbox Testing

Covert testing (or Blackbox testing) is often performed without the knowledge of the business function and aims to find ways around fraud controls and observing responses. This helps to test controls in their natural state, making sure the results are not contaminated by any pre-awareness or preparation by the business function.





CASE STUDY

FEMA's control weaknesses exposed the Government to significant fraud and abuse

Posing as disaster victims of hurricanes Katrina and Rita, members of the US GAO's Forensic Audits and Special Investigations (FSI) Team (now known as Forensic Audits and Investigative Service) applied for federal assistance using falsified identities, made-up addresses, and fabricated disaster stories to register for assistance under the Individuals and Households Program.

FSI's Internet applications were not accepted because of data validation procedures the Federal Emergency Management Agency (FEMA) had implemented. However, FSI investigators were able to register for assistance over the phone. As a result, FEMA sent a number of checks to FSI for fictitious individuals based on fraudulent applications (these were returned post-investigation). This demonstrated the ease with which expedited assistance could be obtained by providing false information over the telephone.

Pressure testing across the three lines of defence

First line of defence

- Pressure testing can be assimilated with fraud risk assessments to apply a further layer of scrutiny on the effectiveness of fraud controls.
- This enables managers and staff who are responsible for identifying and managing risk to apply their business knowledge or technical expertise to identify and effectively evaluate controls.

Suggested approach: Targeted Assessments using testing methods such as desktop reviews, sample analysis and data analysis. **(Minor level of assurance).**

Second line of defence

- Functions that oversee or specialise in compliance or the management of risk (including fraud risk) can work with the functions that own and manage risks to test the effectiveness of fraud controls.
- This co-delivery approach enables the risk function to apply more specialised and consistent testing methods, while also benefiting from the business function's understanding of complex or discreet processes and procedures, and the environment in which they operate.

Suggested approach: Critical Assessments using testing methods such as case studies, workshops, system and process walk throughs, sample analysis, data analysis and practical testing. **(Medium level of assurance).**

Third line of defence

- Functions that provide independent assurance, such as internal or external audit functions, can undertake field-testing to ensure controls are in place and are operating effectively.
- This field-testing by an independent audit function supports the business function and the risk function to monitor and evaluate control effectiveness in higher-risk settings, including in circumstances where they don't have direct control over certain control activities, and instead rely on external parties, such as other public bodies or contractors.[12]

Suggested approach: Critical or Comprehensive Assessments using testing methods such as unannounced examinations, site visits, covert testing, and surveys of stakeholders responsible for fraud controls. **(High level of assurance).**

[12] US Government Accountability Office (2015), A Framework for Managing Fraud Risks in Federal Programs, GAO-15-593SP.

CASE STUDY

Testing biosecurity controls at Australia's border

Australia's Department of Agriculture Water and Environment works with Australian Government and industry partners to maintain strong import controls to mitigate biosecurity risks to Australian agriculture, the environment and our way of life. In recent years, the department has been monitoring the spread of African Swine Fever in Asia and parts of Europe. African Swine Fever has no vaccine and kills about 80 per cent of pigs it infects, which could have a devastating effect on the Australian livestock industry.

In response, the Profiling & Targeting Section in the department pressure tested the import pathway for synthetic stockfeed additives from source countries with reported African Swine Fever outbreaks. This pathway was identified as being vulnerable to fraudulent practices due to the reliance on one control point, based on documentation from importers.

The pressure test involved intercepting and testing a sample of consignments of stockfeed at Australia's border to identify if prohibited materials were contained in the additive product. The Profiling & Targeting Section worked with industry partners to manage anticipated concerns about increased regulatory impacts from border inspection, testing and delays of consignments. They also liaised with state/territory agriculture agencies to prepare them for the possibility of a control test delivering a positive result for African Swine Fever. The pressure test found the control settings were working as required and provided valuable assurance to the department and industry partners that the import pathway was free from prohibited materials. The presence of sample testing also increases the integrity of the pathway going forward by deterring fraudulent declarations on import documentation.

Choosing the right method to test controls

Controls can be tested in a variety of different ways. The method used to test a control will be highly dependent on the type of control, and may be a quantitative method, qualitative method, or both. Often, controls need to be tested using multiple methods.

The Australian Government's Framework uses the analogy of measuring the value of a gold nugget, which would first require someone to measure both its weight and purity before then looking at the gold market price to estimate its value.

For example, if testing the effectiveness of a business functions' identity authentication procedures, pressure testers may:

Review the information threshold for authenticating an identity. What level of information is publicly available, e.g. could it be found on social media?

Listen to a sample of calls to confirm employees follow correct processes to authenticate identity.

Review data on the number of accounts with strong passwords or that have two-factor authentication enabled.

The Australian Government's Catalogue of Common Countermeasures provides further guidance on measuring different types of fraud controls.

CASE STUDY

Eligibility verification for grant program[13]

Head Start is a grant program for child care centres that provide services to low income families. The US GAO Forensic Audits and Investigative Service Team (FAIS) tested whether grantees followed laws and regulations for verifying applicants' incomes – such as by obtaining documentation of applicant's income.

To ensure the covert testing did not displace actual, eligible applicants, the FAIS investigators used program data to select grantees with high vacancies (LA, NY, Boston, Chicago, Detroit). Investigators performed pre-screening calls to grantees to confirm they had vacancies before applying in-person.

Investigators created fictitious phone, email, address (utility bills), birth certificates, and income documents and applied for the program via phone, email, snail mail, and in-person interviews. They recorded and transcribed the in-person interviews as evidence, and retrieved application documents afterward to verify how application documents were recorded.

In 5 of 15 tests, FAIS found fraud – such as grantees doctoring / fabricating income documents or intentionally dismissing income documents to make over-income applicants appear to be eligible. In 3 of 15 tests, FAIS identified control vulnerabilities – such as being admitted without providing any proof of income. In the remaining 7 of 15, grantees were compliant.

The GAO made six recommendations to mitigate the vulnerabilities identified through the audit.

[13] US Government Accountability Office (2019), Head Start: Action Needed to Enhance Program Oversight and Mitigate Significant Fraud and Improper Payment Risks, GAO-19-519.

Common vulnerabilities you might find

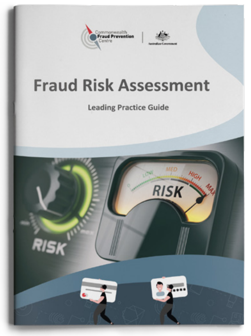
Public bodies can expect to find the following common vulnerabilities through pressure testing:

- ⚠ A lack of fraud awareness.
- ⚠ Inadequate quality assurance.
- ⚠ Staff or processes not verifying information or evidence.
- ⚠ A lack of effective oversight.
- ⚠ Weak technology controls.
- ⚠ Inadequate detection controls.
- ⚠ A lack of reporting or reconciliation.

Treating control vulnerabilities

Pressure tests will uncover gaps and vulnerabilities in controls. A collaborative, co-design approach to treating these gaps and vulnerabilities is encouraged and will help a public body to:

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



Refer to the Australian Government's Leading Practice Guide on fraud risk assessment for practical advice on risk treatment.

Skills and training

The skills and training required for officials will depend largely on the type of pressure testing that public bodies perform.

The requisite skills and training for basic forms of pressure testing would be analogous to those needed to conduct fraud risk assessments. More advanced methods of testing, such as covert testing and complex data analysis, generally require more specialised skills and support (including specialists across the public and private sector).

Introductory skills and experience

- **Fraud Risk Management** – to apply fraud risk management concepts, guiding risk-based thinking and leading conversations on risk mitigation strategies and controls.
- **Planning and Prioritisation** – to manage proactive assignments and effectively planning and prioritising tasks.
- **Stakeholder engagement** – to effectively work in a multidisciplinary environment, consult with subject matter experts and other stakeholders to understand discrete business processes, accurately understand how controls work, and co-design effective treatments for vulnerabilities.
- **Critical analysis** – to break down complex information and processes, apply critical thinking, distinguish between relevant and irrelevant information or evidence, be curious, ask questions, challenge assumptions, think like a fraudster to identify possible fraud schemes.
- **Record keeping** – to collect and document evidence to provide credible and evidence-backed research, analysis, test results and conclusions.
- **Communication** – to prepare well-defined and well written plans, and drafts reports of pressure tests and other documentation to support logical and succinct analysis and recommendations, conforming with relevant standards, policies and procedures.
- **Innovation and creativity** – to apply creative thinking, visualise business processes and concepts, connect different concepts to solve problems, and iteratively improve internal processes based on lessons learned.

Advanced expertise and support

Criminal investigations – to plan and conduct investigations, conduct interviews, decipher evidence and information, perform mobile or fixed surveillance and electronic monitoring, and perform undercover operations.[14]

Visual communication experts – creating fake websites, media, business presence, fake IDs, etc.

Technology experts – conducting data analysis, penetration testing[15], dark web monitoring, etc.

Other consultants – General Counsel, audit staff, methodologists, criminal database experts.

[14] For example, 1811 Criminal Investigator in the US.

[15] The UK's National Cyber Security Centre recommends that public bodies use testers and companies which are part of the CHECK scheme.

CASE STUDY

Testing the security of patients' hospital data[16]

Victorian health services are increasingly using information and communications technology (ICT) to deliver healthcare, and to capture and store patient information. However, while digital records can improve patient care, a cybersecurity breach could have severe consequences for the health sector, resulting in stolen patient information or disabling ICT systems and preventing staff from accessing their patient's information.

The Victorian Auditor-General's Office tested whether health services and supporting ICT services have effective data security practices through penetration testing. The testing was based on the common techniques and tools that cybercriminals or malicious 'insiders' use to attack, such as hospital staff or patients with unsupervised access to hospital systems. The testing identified common weaknesses across all four audited agencies, indicating that hackers could gain access to ICT systems and patient data due to insufficient port security, weak user passwords, limited network segmentation and low staff awareness of data security.

[16] Victorian Auditor-General's Office (2019), Security of Patients' Hospital Data.

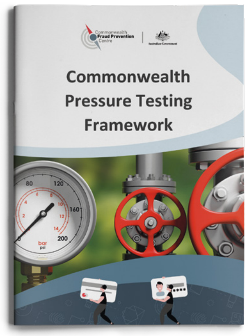
Governance

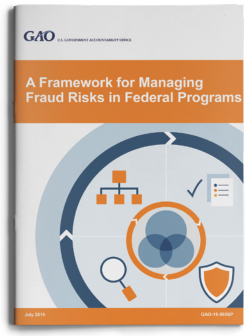
Pressure testing relies on the engagement, support and trust of business functions and senior officials within a public body. The processes and governance arrangements the Australian and US frameworks provide direction to help achieve this, particularly when scoping and approving activities and when managing the outcomes of a pressure test.

Governance arrangements will vary between public bodies based on risk appetite and which pressure testing processes are used. However, there are some things public bodies should put in place before starting, including:

- Receiving appropriate authorisation to undertake pressure testing – this may include a public body incorporating pressure testing into their fraud control plan and strategy
- Identifying which official/s will be responsible for approving individual pressure test plans and covert testing activities
- Developing processes for reporting pressure test outcomes
- Having a mechanism for recording and reporting key actions, decisions and outcomes
- Having a mechanism for recording and monitoring the implementation of treatments.

For further advice on establishing appropriate governance arrangements, refer to the Australian Government Framework and the US GAO Framework for Managing Fraud Risks in Federal Programs.





Managing risks associated with covert pressure testing

The Australian Government Framework includes specific protocols for managing risks, including legal, safety, security and reputational risks associated with technical and covert pressure testing. For example, a risk assessment must always form part of every technical and covert testing plan.

This must identify the inherent risks and possible outcomes of the planned test scenarios and identify appropriate treatments and responses. Officials should also consider potential risks and impacts beyond the immediate results of testing (i.e. second and third order consequences).

The US GAO's Forensic Audits and Investigative Service Team (FAIS) apply strict processes and procedures for planning, executing and reporting on covert operations to minimise risks. This includes the following:

- FAIS investigators protect information from unauthorised disclosure, protect the rights of all individuals involved, and avoid any action that may give the appearance of coercion or intimidation.
- If investigators discover vulnerabilities that pose a significant and immediate threat to public safety, FAIS will immediately discontinue the investigation and alert the appropriate government law enforcement agency.
- When conducting covert testing offsite, FAIS investigators have a cover team to ensure their safety.
- If a covert operation is uncovered during a test, the FAIS investigators and cover team immediately identify themselves and alert the proper law enforcement authorities that a test is being conducted.
- Under no circumstances will FAIS make publicly available any photograph, videotape, or audiotape that could be used as a road map by criminals or terrorist groups.
- FAIS does not usually reveal all details about its covert methodologies in public products. For example, FAIS typically does not reveal the name of any bogus companies that it creates or the fictitious identities that it uses.
- If the findings relate to issues of national or homeland security, FAIS provides a draft product to the public body for a sensitivity review prior to releasing a report.

CASE STUDY

Department of Defense excess property[17]

A US Department of Defense (DOD) Law Enforcement Support Office (LESO) program transfers excess DOD property to thousands of federal, state, and local law enforcement agencies across the US. The US GAO Forensic Audits and Investigative Service Team (FAIS) tested the LESO program's enrolment and application processes through covert testing.

Using publicly available resources, FAIS investigators created a fictitious federal law enforcement agency, including a fictitious website describing that agency's activities. They then completed the application paperwork, submitted it to LESO officials, and corresponded by email to answer follow-up questions, including providing a fictitious statute as a means to legitimize the agency.

Once approved to participate in the program and given access to the LESO program systems, FAIS investigators obtained over 100 controlled items with an estimated value of $1.2 million. This included night-vision goggles, simulated rifles, and simulated pipe bombs, which could be potentially lethal items if modified with commercially available items.

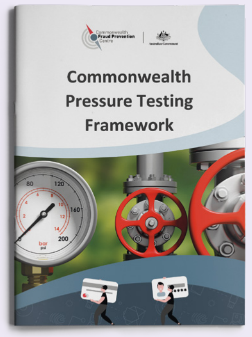
The GAO made four recommendations to the Defense Logistics Agency, including strengthening internal controls over the approval and transfer of DOD excess controlled property to law enforcement agencies, and conducting a fraud risk assessment to institute comprehensive fraud prevention and mitigation measures.

[17] US Government Accountability Office (2017), DOD Excess Property: Enhanced Controls Needed for Access to Excess Controlled Property, GAO-17-532.

Existing guidance and frameworks developed by IPSFF members

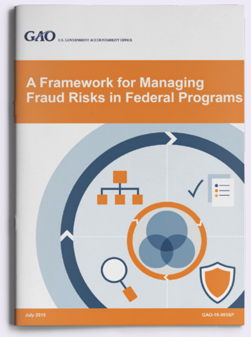
Commonwealth Pressure Testing Framework

This framework sets out key principles and materials for conducting pressure testing within Australian Government entities. The Commonwealth Fraud Prevention Centre also provides guidance to Australian Government officials who want to start applying pressure testing within public bodies.


Commonwealth Pressure Testing Framework

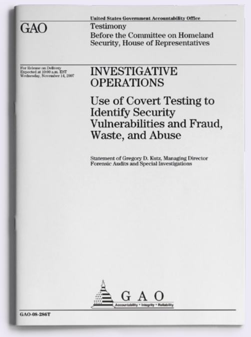
A Framework for Managing Fraud Risks in Federal Programs (GAO-15-593SP)

This framework encompasses control activities in the US Federal Government to prevent, detect, and respond to fraud, with an emphasis on prevention, as well as structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks.


GAO
A Framework for Managing Fraud Risks in Federal Programs

Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse (GAO-08-286T)

This document outlines the US Government Accountability Office's Forensic Audits and Investigative Service Team's processes for undertaking security assessments and special investigations involving covert testing.


GAO
Testimony
Before the Committee on Homeland Security, House of Representatives
INVESTIGATIVE OPERATIONS
Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse
GAO-08-286T

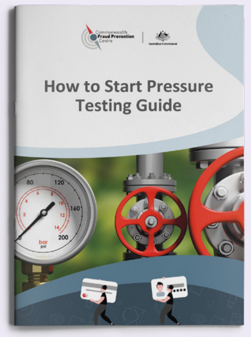
Advice on how to get the most from penetration testing

This guidance from the UK's National Cyber Security Centre (NCSC) provides advice on the proper commissioning and use of penetration tests by UK organisations and cyber security professionals. The NSCS's CHECK scheme provides a list of approved penetration test companies and the method in which they conduct a penetration test.

Additional tools to support pressure testing

How to start pressure testing guide

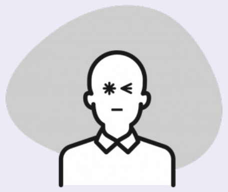
This guide has been developed by the Australian Government for public bodies who want to start applying pressure testing. It contains 10 practical and flexible steps that officials can use to adopt pressure testing. Though it may seem daunting, pressure testing can be a simple process that requires minimal resources and can be conducted by any public body.



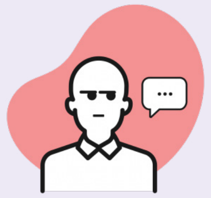
How to Start Pressure Testing Guide

Fraudster Personas

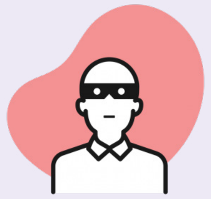
The Fraudster Personas were developed by the Australian Government to help public officials more easily understand the different actions fraudsters use to target government programs and functions. Fraudster Personas can also help pressure testers adopt a fraudster's mindset to identify avenues where fraudsters might exploit a programs or functions and uncover potential vulnerabilities.



The Reckless



The Deceiver

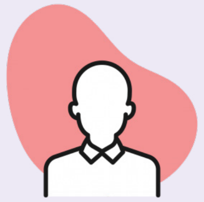


The Impersonator

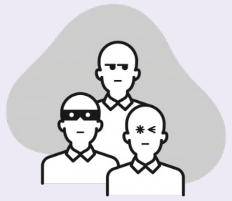
The Fabricator

The Coercer

The Exploiter



The Concealer



The Organised

Catalogue of Common Countermeasures

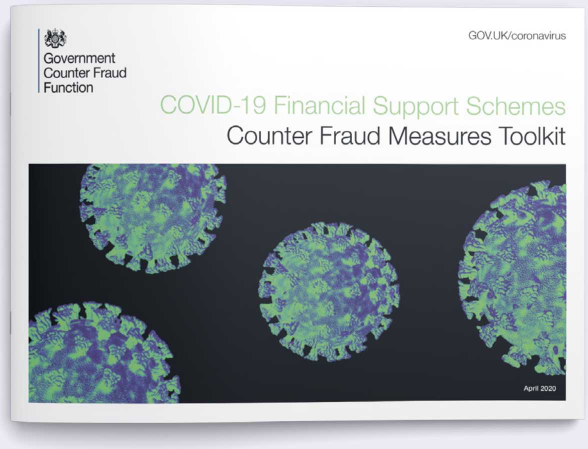
This catalogue was developed by the Australian Government to define and categorise common types of controls and standardise ways to measure their effectiveness. The catalogue provides:

- A summary of each control category
- Specific examples of controls under each category
- An explanation of the purpose of each control category
- Suggested ways of measuring the effectiveness of controls under each category
- Vulnerabilities to consider for each control category
- Dependencies (links to other control categories that help public bodies develop more complete control environments).

Pressure testers can use this catalogue in combination with fraud risk assessments and Fraudster Personas to identify existing controls and gaps across a program or function. The catalogue can help public bodies to improve the quality and consistency of testing and reporting across similar types of controls.

Counter Fraud Toolkits

Policy specific toolkits, such as the UK COVID-19 Counter Fraud Measures Toolkit or those developed by the Australian Government, can help public bodies design and deliver more fraud resilient policies and programs. These toolkits feature advice on different risks to consider in particular policy areas, such as Grants Administration, and provide direction on existing mechanisms and controls public bodies might deploy to reduce fraud. The toolkits can also assist pressure testers to identify key controls to focus their testing efforts.



GOV.UK/coronavirus

Government
Counter Fraud
Function

COVID-19 Financial Support Schemes
Counter Fraud Measures Toolkit

April 2020

Appendix

Overview of the US GAO's approach to covert testing.

The US Government Accountability Office has developed a sophisticated approach to covert testing. The FAIS within the GAO engage in proactive operations to test the security of agencies' systems, controls and property. These operations are carried out by experienced criminal investigators and coordinated with appropriate authorities, such as the Department of Justice. The primary purpose of this testing is to support GAO audits into federal programs.

Planning phase

FAIS develops a written investigative plan containing: a statement regarding the investigation's overall objectives; a description of the legal issues involved; and a summary of the allegations that merit investigation or the processes, systems, and controls that will be tested.

Execution phase

Once an investigative plan has been approved, FAIS begins their covert operation following the steps set out in the investigative plan. In most cases, these steps include the creation of fictitious identities and counterfeit documentation, including items such as birth certificates, driver's licenses, billing records, and social security cards.

All counterfeit documents are manufactured by FAIS using hardware, software, and materials that are available to the general public—this allows FAIS to demonstrate that any security vulnerabilities found could, in reality, be exploited by a criminal or terrorist with moderate means and resources and would not require sophisticated insider knowledge or access to sophisticated equipment.

Reporting phase

Once the operation is complete, FAIS brief relevant Members of Congress. They also brief officials at the tested public body to inform them that they have been the subject of a covert operation, share the results of the testing, and, if necessary, suggest potential remedies for any identified control weaknesses or security vulnerabilities.

After all parties have been briefed, FAIS will issue a report or testimony. Because the covert testing is sometimes part of a broader forensic audit, the result may be reported in the audit report. These contain the GAO's findings, the results of the briefing with the tested public body, and sometimes recommendations.