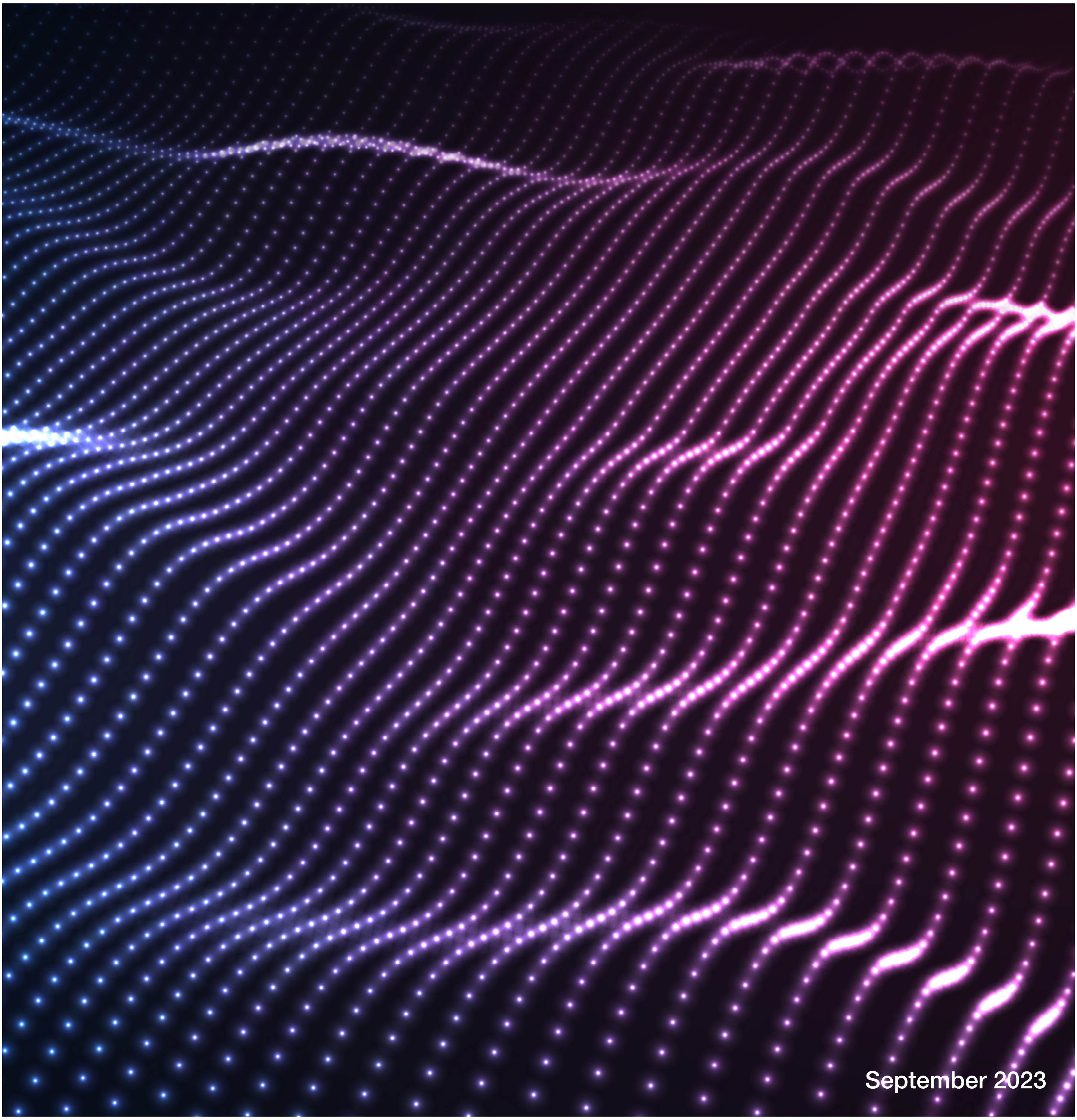
International Public Sector Fraud Forum
*Bringing countries together to fight public sector fraud*

International Public Sector Fraud Forum

# Fraud Control Testing Framework

FCTF-01



September 2023

Public Sector
Fraud Authority

Commonwealth
Fraud Prevention
Centre

Produced in collaboration with the Public Sector Fraud Authority and the Commonwealth Fraud Prevention Centre.

### Crown copyright disclaimer

The information contained in the International Public Sector Fraud Forum documentation and training is subject to Crown Copyright 2023.

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

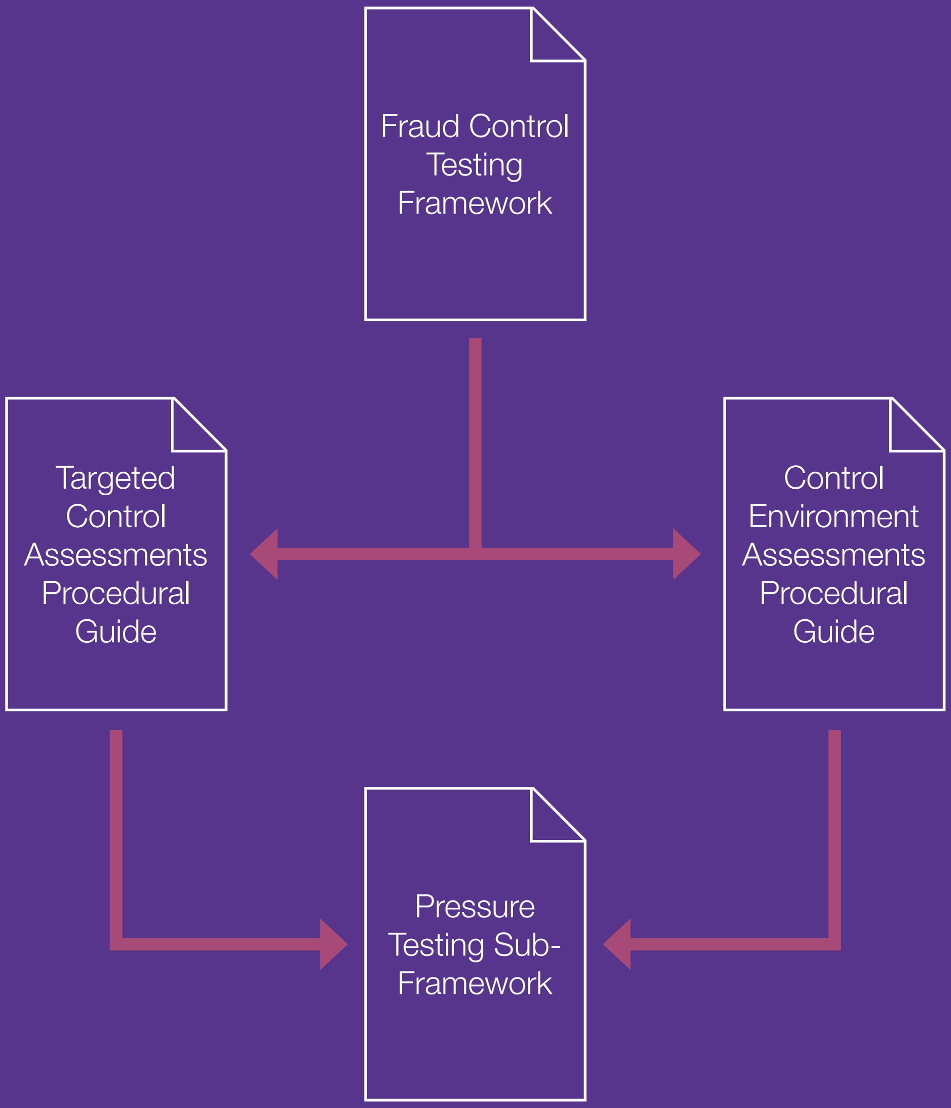
- copy, publish, distribute or transmit the Information;
- adapt the information;
- exploit the information commercially or non-commercially for example, by combining it with other information, or by including it in your own product or application.

The information should not be published or distributed in any way that could undermine the values and aims of the International Public Sector Fraud Forum.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

# Fraud Control Testing Framework – Document Map



Fraud Control Testing Framework

Targeted Control Assessments Procedural Guide

Control Environment Assessments Procedural Guide

Pressure Testing Sub-Framework

## Tools and Templates

Fraud Control Catalogue
Commonwealth Fraud Prevention Centre
OFFICIAL
Handbook of fraud control testing methods

# Purpose

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. International good practice shows the best way to deal with fraud is to prevent it.

This requires capability and focus. However, public bodies do not always consider fraud when conducting their activities or know where they are vulnerable.

This Framework sets out key principles, processes and tools for conducting fraud control testing within public sector organisations. Conducting fraud control testing enables public bodies to:

- better understand their exposure to fraud risk;
- identify previously unknown fraud vulnerabilities in their schemes and business functions;
- gain a better understanding of their fraud controls, their effectiveness and limitations;
- reduce the opportunity for fraud and the harmful impacts it can have on citizens, government services and industry partners;
- provide assurance to their accounting officer and that their fraud risks are being managed appropriately;
- implement ongoing monitoring and assurance of control effectiveness; and
- increase the quality, safety and efficiency of the programs and services they deliver.

This in turn will deliver considerable benefits - trust in the public sector will be enhanced, government programs and services will be more secure and effective, public funds will be better spent, the government will continue to be seen as a trusted partner for industry, and ultimately the economy will be stronger.

International good practice shows the best way to deal with fraud is to prevent it.

## Who this Framework is for

This Framework has been developed for the Counter Fraud Function across all types of public bodies and will help Counter Fraud Professionals better understand fraud risk, recognise prevention opportunities and collaborate with others to design, implement and evaluate controls.[1]

Fraud control testing has been successfully conducted for a number of years in jurisdictions like Australia and the United States. This Framework builds upon their leading practice to give public bodies a choice of processes that can be performed at different scales and levels of complexity to suit their needs and resources. For example, public bodies can apply fraud control testing to:

- an individual control (generally a critical control);
- multiple controls (generally the most critical controls) across a specific scheme or business process.

While designed for those working in Counter Fraud, the flexibility of this Framework enables different elements to be applied across the three lines of defence, which can provide fuller and ongoing assurance on the effectiveness of fraud controls.

The Framework also supports officials with different levels of experience, and helps them to build their understanding and expertise. To enable this, the Framework is underpinned by aids that educate officials on the common methods used by fraudsters (Fraudster Personas) and the common vulnerabilities that enable them to commit fraud. This knowledge can then be applied by both Counter Fraud Professionals and business stakeholders to specific schemes and functions to help identify potential threats and control vulnerabilities.

> This Framework has been developed for the Counter Fraud Function across all types of public bodies.

The Framework also supports officials with different levels of experience, and helps them to build their understanding and expertise.

The Framework is also supported by practical tools and guidance to enable officials to quickly identify and categorise controls (e.g. working closely with stakeholders and using a Fraud Control Catalogue as a guide for discovery) and apply consistent methods to test control effectiveness.

This Framework is issued by the International Public Sector Fraud Forum in conjunction with the UK's Public Sector Fraud Authority (PSFA) and sets out the recommended best practice for fraud control testing. It is a principles-based document and is designed to be flexible and adapted to public bodies' individual circumstances.

[1] UK GCF Professional Standards and Guidance: Fraud Prevention, A2. Introduction

# Introduction

## What is Fraud Control Testing?

Fraud control testing involves the assessment and evaluation of internal controls, processes, and procedures to detect and prevent fraudulent activities. It aims to ensure that public funds are used appropriately and that public bodies maintain high standards of accountability and transparency. It also helps public bodies examine the effectiveness of their fraud controls using different testing methods. It 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.

## Why is there a need for fraud control testing?

Global studies consistently reveal that weak controls lead to more fraud than any other factor. For example:

- **The Association of Certified Fraud Examiners, in their 2022 Global Fraud Study**, highlighted the most common factor underlying frauds in their study was "a lack of internal controls; 29% of victim organisations did not have adequate controls in place to prevent the fraud from occurring. Another 20% of cases involved an override of existing internal controls, meaning the victim organisation had implemented mechanisms to protect against fraud, but the perpetrator was able to circumvent those controls."[2] The study also found that strong fraud controls correlate with "both lower fraud losses and quicker detection."[3]
- **PwC, in their 2018 Global Economic Crime and Fraud Survey**, found that opportunity was the "leading contributor to the most disruptive fraud committed by internal actors." Furthermore, PwC noted, "virtually every significant internal fraud is a result of management circumventing or overriding controls," and concluded that, "it is important to be wary of the false sense of security that internal controls, even well-designed ones, can bring."[4]
- **KPMG's 2016 report, 'Global Profiles of the Fraudster'**, notes that, "weak internal controls were a contributing factor for 61 per cent of fraudsters, compared with 54 per cent in 2013."[5] KPMG also found that while fraud detection methods continue to improve, technology is creating weaknesses as quickly as it is filling gaps.[6]

Occupational Fraud 2022:
A REPORT TO THE NATIONS
ACFE
Pulling fraud out of the shadows
pwc
KPMG
Global profiles of the fraudster
Technology enables and weak controls fuel the fraud
May 2016

[2] Report to the Nations on Occupational Fraud and Abuse, p.42, Association of Certified Fraud Examiners, 2022

[3] Report to the Nations on Occupational Fraud and Abuse, p.35, Association of Certified Fraud Examiners, 2022

[4] Pulling fraud out of the shadows, pp. 25-26, PwC, 2018

[5] Global Profiles of the Fraudster, p. 6, KPMG International, 2016

[6] Global Profiles of the Fraudster, p. 20, KPMG International, 2016

The effectiveness of fraud controls can also degrade over time. For example:

- Fraudsters are a committed adversary, continually developing new and novel ways to beat the controls public bodies put in place to counter them. In some circumstances this can involve professional facilitators who help criminals develop sophisticated fraud schemes.
- New enablers for fraud can emerge which can make traditional controls less effective, e.g. the prevalence of compromised identity information has rendered traditional identity authentication controls ineffective.
- Organisational change and digital transformation can also make public bodies vulnerable to losing oversight of risks and weakened control environments.[7]
- New technology and innovations also create opportunities to replace original controls with new, more cost-effective controls – increasing efficiency and improving user experience.[8]

## What are the benefits of fraud control testing?

Taking proactive action to test controls will greatly benefit public bodies and officials who are accountable for managing fraud risk, helping them make more informed decisions about their risk tolerance. It will also help public bodies take considered and decisive action to reduce the opportunity for fraud and minimise the risk of reputational damage by strengthening their control environments.

Fraud control testing is a proven way for public bodies to proactively identify and eliminate blind spots. If public bodies know where their vulnerabilities are, they are in a better place to prevent attacks or uncover where they are being exploited.

However, the benefits of fraud control testing go well beyond identifying control vulnerabilities. For example, fraud control testing:

- **Enhances operational efficiency** – helping to identify areas of inefficiency, duplication of efforts, or gaps in procedures resulting in operational efficiencies, streamlined workflows, and optimised resource allocations.
- **Enhances operational effectiveness** – through reduced error and waste, improved employee engagement and experience, and improved customer or client satisfaction.
- **Prevents financial loss** – helping to identify vulnerabilities and implement measures to prevent fraud before it occurs and safeguard public funds.
- **Mitigates fraud risk in an efficient and measurable way** – by proactively addressing specific vulnerabilities and reducing fraud in a way that can be measured.
- **Increases fraud awareness** – helping officials acknowledge the risk of fraud and the potential for vulnerabilities, making them more effective agents in preventing fraud.
- **Deters fraud** – knowing that fraud control measures are in place and actively monitored can discourage people from engaging in fraudulent activities.

[7] Keeping it together: systems and structures in organisational change, p. 7, NSW Independent Commission Against Corruption, 2017

[8] Guidelines for Managing the Risk of Fraud in Government, p.5, Office of the Auditor General of British Columbia, 2010

- **Enables fraud measurement and detection activities** - by regularly testing internal controls, public bodies can identify red flags and anomalies that may indicate potential fraud, as well as support fraud and error loss measurement.
- **Reduces cost** – helping to avoid unnecessary expenditures associated with fraud investigations, legal proceedings, and reputational damage.
- **Provides assurance that risks are being adequately managed** – through the development and validation of a robust internal control environment.
- **Preserves public trust** – by demonstrating a commitment to transparency, accountability, and responsible financial management.

Therefore, fraud control testing can accelerate, improve or otherwise enhance business elsewhere in the public body, demonstrating it's wider value. This is because fraud control testing is a part of good governance transparency, and accountability. Fraud control testing activities can also improve efficiency, effectiveness and compliance.[9]

Furthermore, once a counter fraud framework and associated performance measures have been established, fraud control testing can provide evidence that the public body is achieving objectives and meeting standards. As people and communities increasingly expect visible integrity from public services, fraud control testing offers tangible evidence of management action. This can be particularly important in the wake of a serious incident.

Appendix C expands on these benefits for public bodies, which can help public bodies develop a compelling business case to invest resources into fraud control testing.

## HM Government Fraud Risk Management Cycle

Drawing from the UK's Government Counter Fraud Profession standards helps to illustrate the process in relation to fraud risk management. The Fraud Risk Management Cycle (Figure 1)[10] offers an illustration of the end-to-end process, from using research to identify known risks, completing a fraud risk assessment, and using this to actually manage and mitigate those risks by informing controls. The cycle has four component parts:

- Fraud Risk Assessment identification
- Fraud Risk Assessment - evaluation and prioritisation
- Evaluating controls
- Reviewing and reporting.

The first half of the cycle deals with Fraud Risk Assessment. The second half of the risk cycle is where fraud prevention actions should be implemented to mitigate the identified risks. This includes:

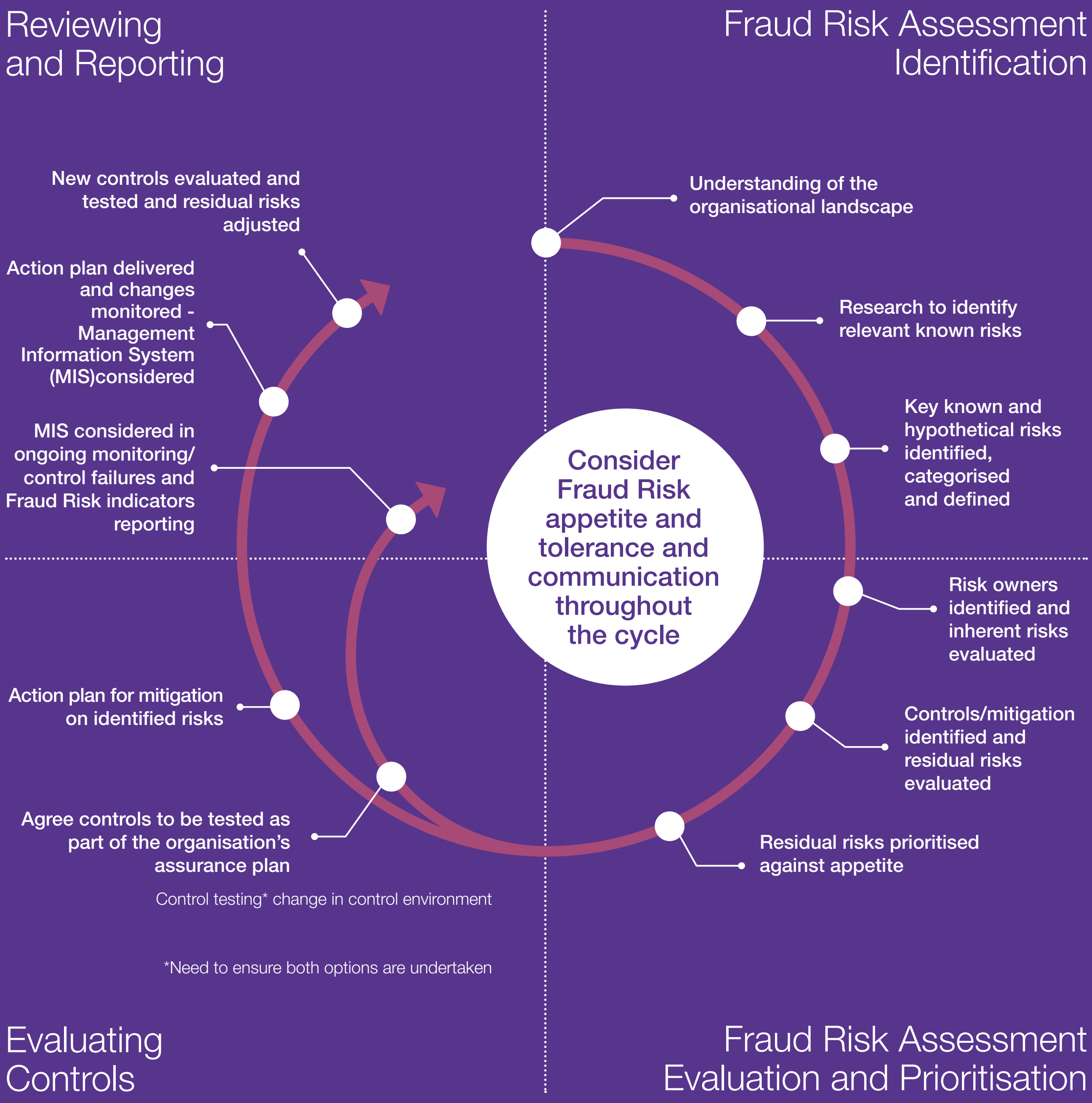
- Agreeing on controls to be tested as part of an organisation's assurance plan
- Putting a Management Information System in place to monitor controls
- Evaluating and testing new controls.

There is a continual need for reporting and then reviewing and re-doing aspects of the cycle. The key to delivering an effective fraud control testing capability, as part of the Fraud Management process, is a thorough understanding of the organisational landscape, undertaking good Fraud Risk Assessments and having mechanisms in place for reviewing and reporting on how fraud risks are being managed.

[9] Adapted from Counter Fraud Investment Cases Leading Practice Guide, Commonwealth Fraud Prevention Centre pp. 25-26

[10] GCF Professional Standards and Guidance: Leadership, Management and Strategy

Figure 1 - Fraud Risk Management Cycle



Reviewing and Reporting

Fraud Risk Assessment Identification

Understanding of the organisational landscape

Research to identify relevant known risks

Key known and hypothetical risks identified, categorised and defined

Risk owners identified and inherent risks evaluated

Controls/mitigation identified and residual risks evaluated

Residual risks prioritised against appetite

Consider Fraud Risk appetite and tolerance and communication throughout the cycle

Agree controls to be tested as part of the organisation's assurance plan

Action plan for mitigation on identified risks

MIS considered in ongoing monitoring/ control failures and Fraud Risk indicators reporting

Action plan delivered and changes monitored - Management Information System (MIS)considered

New controls evaluated and tested and residual risks adjusted

Control testing* change in control environment

*Need to ensure both options are undertaken

Evaluating Controls

Fraud Risk Assessment Evaluation and Prioritisation

# Governance arrangements

Drawing on the UK's Functional Standards, S013[11], we can consider the governance arrangements for fraud control testing within a public body should be an integrated part of their governance and management framework for managing fraud, bribery and corruption. Public bodies may also wish to integrate fraud control testing into their broader risk management framework.

Governance arrangements will vary between public bodies based on risk appetite, who will be delivering the activities, and which fraud control testing processes and methods they intend to use. However, there are some things public bodies should put in place before starting, including:

- Receiving appropriate authorisation to undertake fraud control testing – such as by incorporating fraud control testing into their counter fraud, bribery and corruption policy.
- Identifying an appropriate Board or Committee to provide senior oversight, guidance, and support to ensure that fraud control testing receives appropriate resources, attention, and priority.
- Understanding how fraud control testing may interact with applicable laws, rules, and regulations associated with the public body and its operations.
- Identifying an appropriate senior official who will be responsible for approving individual fraud control testing plans and activities.
- Having secure systems for storing and managing information.
- Developing processes for reporting fraud control testing outcomes.
- Recording and reporting key actions, decisions and outcomes.
- Monitoring the implementation of treatments for identified vulnerabilities.
- Tracking the performance of fraud control testing, including the benefits it delivers.
- Establishing reporting mechanisms, including:
  - Internally to support effective senior management oversight and accountability over agreed outcomes and decisions.
  - Externally to the PSFA (see the chapter on reporting and monitoring).

Effective capability is generally 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 a capability that delivers value to the organisation.[12] Therefore, when starting with fraud control testing, it is beneficial for public bodies to start small and focus on a small number of controls using simple methods. However, the value a public body receives from fraud control testing increases as it invests more resources and builds its capability. Therefore, as public bodies build in maturity and capability, they should aim to conduct more comprehensive testing and utilise more advanced methods.

[11] UK GCF Functional Standard GovS 013: Counter Fraud

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

Fraud control testing relies on the engagement, support and trust of business functions and senior officials within a public body. In some circumstances, fraud control testing also involves risk, such as financial, work health and safety, protective security, legal and information security risks. Therefore, strong and defined governance arrangements are particularly important when planning, scoping and approving activities and when managing the outcomes of fraud control testing activities.

The governance arrangements for fraud control testing should also foster collaboration with business stakeholders rather than making them feel subject to an audit. Officials working within their own scheme or function are best placed to identify controls and help evaluate whether they are working effectively. A collaborative approach invites stakeholders to be actively engaged in the process, leverages their knowledge, expertise and resources, builds trust in the process, and delivers greater credibility behind in testing results and treatment recommendations.

Fraud Control Testing, including pressure testing, is first and foremost an assurance function – it is not intended to test whether individual staff are complying with internal policies and procedures. However, in some circumstances, testing activities may find evidence of staff failing to apply internal policies or controls, or not meeting behavioural standards. Depending on the circumstances, this may warrant a specific response, for example providing feedback to the staff member's manager. Fraud control testing is also not intended to detect fraud or corruption. However, the results from testing may identify indicators of fraud or corruption. Where this occurs, testers should consult with investigators, as it may be necessary to cease testing to avoid the risk of compromising a current or future investigation. Therefore, public bodies should have defined escalation and reporting protocols for circumstances where instances or indicators of serious non-compliance, misbehaviour, fraud or corruption are revealed through testing.

Before commencing a fraud control testing activity, public bodies should also consider potential outcomes that may adversely affect business lines and industry partners. By considering these potential outcomes upfront, and who may be affected, public bodies can proactively manage risks, as well as brief and prepare relevant stakeholders to manage the results.

Public bodies should also put in place assurance mechanisms (e.g. management reviews or the occasional internal audit) to provide confidence that fraud control testing activities are being delivered with due professional care, i.e. in a thorough, legal, appropriate, safe, effective, impartial, objective, ethical and timely way.[13] These mechanisms should also ensure fraud control testing minimises disruption to other work, avoids overlaps and duplication of effort with other assurance functions, such as internal audit, while remaining rigorous and meeting the needs of stakeholders.

[13] Adapted from the Quality Standards for Investigations issued by the US Council of Inspectors General on Integrity and Efficiency, 2011, pp. 8-9

## Fraud control testing across the three lines of defence[14]

The governance arrangements within a public body should identify the functions responsible for fraud control testing, including establishing objectives, roles and responsibilities, guidance on processes and procedures, and a consistent oversight and reporting regime for activities across different business teams and functions.

While this Framework is primarily for those working in Counter Fraud, the following outlines how fraud control testing can be deployed in different ways across the three lines of defence.

### First line of defence

The first line of defence are the business lines who own and manage fraud risks. Fraud control testing can be assimilated with fraud risk assessments to apply a further layer of assurance 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. Basic testing methods such as desktop reviews, sample analysis and data analysis are likely to be more feasible for the first line of defence.

### Second line of defence

The second line of defence often involves a centralised area that oversees or specialises in compliance and/or the management of risk (including fraud risk), e.g. those working in Counter Fraud. These areas can apply their knowledge of fraud risks and enablers to support the first line of defence test the effectiveness of fraud controls in high risk areas.

This co-delivery approach enables the second line of defence to apply more specialised and consistent testing methods, while also benefiting from the business area's understanding of complex or discreet processes and procedures, and the environment in which they operate.

### Third line of defence

The third line of defence are the functions that provide independent assurance, e.g. audit functions. The third line of defence can work in combination with the second line to undertake field-testing to ensure controls are in place and are operating effectively in high risk areas.

This field-testing by an independent audit function supports both 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.[15]

[14] A Guide to Pressure Testing, p. 17, International Public Sector Fraud Forum, 2022

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

# Training, skills and other attributes

The skills, training and other attributes required for fraud control testers will depend largely on the type of processes and testing methods that public bodies intend to use.

## Introductory skills and experience

The requisite skills and training for compliance testing would be similar to those needed to conduct fraud risk assessments, including:

- **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 plan and prioritise 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 fraud 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, and 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 clearly-written plans and drafts reports of fraud control testing activities 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.[16]

## Advanced skills and expertise to support Pressure Testing

Because of the critical and sometimes sensitive nature of Pressure Testing activities, public bodies should ensure all operational leads and designated testers possess the requisite knowledge, skills and abilities summarised below to fulfil their responsibilities:

- Knowledge of theories, principles, practices, and techniques of investigation and the education, ability, and experience to apply such knowledge to Pressure Testing activities.
- Knowledge of government organisations, programs, activities, functions, and, where applicable, their interrelations with the private sector.
- Knowledge of applicable laws, rules, and regulations such as those relating to privacy, freedom of information, whistleblower protection, work health and safety, protective security and information security.

- Ability to exercise tact, initiative, ingenuity, resourcefulness, and judgement in collecting and analysing facts, evidence, and other pertinent data.
- Ability to use computer equipment, software, and related systems effectively in support of the testing process.
- Ability to deliver clear, concise, accurate, and factual summaries of testing results, both orally and in writing.[17]

Public bodies may also need to commission additional support to deliver specialised Pressure Testing techniques, such as covert testing and complex data analysis (including from specialists across the public and private sector). For example:

- **Visual communication experts** – creating fake websites, media, business presence etc.
- **Information technology, data and cyber security experts** – conducting data analysis, penetration testing,[18] dark web monitoring etc.
- **Legal experts and other consultants** – General Counsel, audit staff, methodologists, criminal database experts etc.

## Character

Fraud control testers must possess and maintain the highest standards of conduct and ethics, including unimpeachable honesty and integrity. Every citizen is entitled to have confidence in the integrity of public sector employees, particularly those who routinely access sensitive information and have knowledge of vulnerabilities in processes and controls.

Consequently, public bodies should establish sound hiring policies to adequately screen applicants for fraud control testing positions. Processes to consider include pre-employment checks that meet the relevant security standard for your organisation.

> Fraud control testers must possess and maintain the highest standards of conduct and ethics.

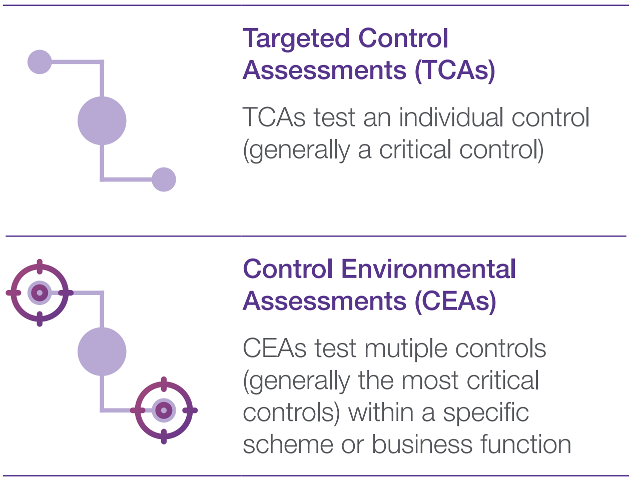
[17] Adapted from the Quality Standards for Investigations issued by the US Council of Inspectors General on Integrity and Efficiency

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

# Fraud control testing processes

This Framework accommodates for the different needs, resources and capabilities of public bodies. The two approaches outlined below (Figure 2) give public bodies the flexibility to choose the most appropriate type of process to suit their needs.[19] It also helps public bodies pilot fraud control testing, start small and build their capability over time.

Figure 2



**Targeted Control Assessments (TCAs)**

TCAs test an individual control (generally a critical control)

**Control Environmental Assessments (CEAs)**

CEAs test mutiple controls (generally the most critical controls) within a specific scheme or business function

The different processes even allow more resourced public bodies to adjust the scope, size and level of complexity of testing activities as needed. Depending on the type of risk or available resources, it may be appropriate for a public body to only evaluate a select number of controls within a scheme or function to determine their effectiveness. In other circumstances, it may be necessary to evaluate all known controls across an entire control environment to provide a higher level of assurance that fraud is being managed effectively.

## Targeted Control Assessments

Targeted Control Assessments (TCAs) help public bodies quickly test the effectiveness of a single control, or a small number of closely associated controls. These targeted and agile assessments can be applied by all types of public bodies and allow them to selectively test critical controls across a range of high-risk processes and systems. This process provides a limited level of assurance to risk owners by ensuring that critical controls are operating effectively.

See the Targeted Control Assessments – Procedural Guide (Ref: FCTF-02) for the process for undertaking a TCA, including a process map, an overview of the different stages, and links to different tools and templates.

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 public body's Counter Fraud Function of the potential vulnerability. In response, the Function quickly plans and conducts a TCA on the acquittal process, which confirms the flaw. The team then uses its findings to work with business and ICT stakeholders to fix the vulnerability.**

[19] Adapted from the Commonwealth Pressure Testing Framework, Commonwealth Fraud Prevention Centre, 2020

## Control Environment Assessments

Control Environment Assessments (CEAs) help public bodies identify and test the effectiveness of multiple controls within a specific scheme or business function. This process provides a high-level of assurance to risk owners and the Board regarding the effectiveness of the control environment.

The scope of CEAs can be adjusted based on the type of risks or available resources. For example, public bodies should follow the Pareto Rule[20] and focus the scope of the CEA on the highest risks, as well as use the Control Criticality Assessment Tool (Ref: FCTF-13) to identify and only test the most critical controls within a control environment. This process helps ensure counter fraud resources are used most efficiently and effectively by targeting the more critical controls within high-risk areas, while still providing a high level of assurance to risk owners on the effectiveness of the control environment.

Understanding the design and purpose of a control is fundamental to determining how, and to what extent, it reduces the risk. Therefore, an assessment of control criticality should be undertaken after the control environment has been mapped out. Collaboration with business areas and subject matter experts will also help achieve a more accurate and objective assessment of which controls are most critical for reducing the risks within the scope of the CEA.

In rare circumstances, public bodies may need to test all known controls across a specific scheme or business function. This process provides the fullest level of assurance to risk owners on the effectiveness in an integrated control environment.

See the Control Environment Assessment – Procedural Guide (Ref: FCTF-03) for the process for undertaking a CEA, including a process map, an overview of the different stages, and links to different tools and templates.

**Example**

**Following a large data breach at another organisation, a Counter Fraud Unit is tasked to review their public body's information security controls. The team develops a plan for a CEA and identifies the systems and databases within the public body that are most susceptible to a large-scale data breach. They also identify the controls in place to mitigate the risk of unauthorised access and disclosure. To reduce the size and scope of the CEA, the team work closely with subject matter experts to understand the design and purpose of the controls and identify the ones most critical for reducing the risk of a large-scale breach. They then test the most critical controls, such as examining data on how the systems and databases are being accessed and how data is being extracted to ensure only authorised officials are accessing data holdings for relevant business purposes.**

**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 large-scale breach and improves crisis planning and response if a breach were to occur.**

[20] This rule in economics, named after economist Vilfredo Pareto, specifies that 80% of consequences come from 20% of the causes, asserting an unequal relationship between inputs and outputs.

# Choosing what areas to focus on

It is impractical for public bodies to test the effectiveness of every fraud control. This expectation would ultimately lead to a "mile wide, inch deep" approach, diminishing the assurance value fraud control testing can deliver. Therefore, public bodies should aim to focus their effort and resources on their highest risk areas and test their most critical controls.

Public bodies should undertake a Strategic Threat Assessment,[21] Strategic Fraud Risk Profiling[22] and data analysis to identify those areas where they are most susceptible to fraud risk, enabling them to focus their control testing in these areas. Other useful sources of data to help identify which controls, processes, programs, functions or systems are suitable for fraud control testing include:

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

Functions that oversee or specialise in compliance or the management of risk (including fraud risk) should also conduct their own research and scan the media to remain agile and respond to emerging fraud risks. They should also create a register of potential control testing activities. This register should capture information such as:

- a description of the potential control testing activity
- how this potential control testing activity was identified
- what stakeholders would be involved
- what type of control testing activity would be most suitable (TCA or CEA).

Public bodies may also want to develop a forward work plan (a pool of pre-authorised fraud control testing activities) and have this approved by an appropriate senior official. Officials responsible for undertaking fraud control testing can then prioritise these pre-authorised activities using the Priority Assessment Tool (Ref: FCTF-05). Public bodies should recalibrate their work plan every 12-24 months to account for changes to team resources, organisational learnings and new risks.

Fraud control testing can also be performed on new policies or programs that are in the design process. When deciding what areas to test fraud controls, it is also important to consider the potential benefit to your public body and whether there have already been other similar audits or tests recently conducted.

If the control testing activity is a proof of concept, public bodies should focus a TCA or CEA on a high-risk scheme or business function to demonstrate benefits, try techniques, provide lessons learned and/or identify future tests.

Another factor to consider is the potential benefits a control testing activity would bring to your public body as well as others across government. All public bodies have common functions and processes such as payroll and procurement. Collaborating with cross-government functions can benefit multiple public bodies. Some public bodies also deliver similar schemes and services. Collaborating or sharing findings with other bodies can also help improve the efficiency of control testing, extend the value delivered and avoid duplication of effort.

[21] UK GCF Professional Standards and Guidance: Fraud Prevention, E.9 Strategic Threat Assessment
[22] Commonwealth Fraud Prevention Centre 2022, Fraud Risk Assessment Guidance and Tools

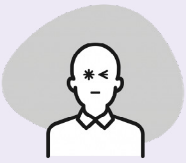
# Adopting a fraudster's mindset

Fraud schemes vary in their complexity and creativity. They range from opportunistic individuals taking advantage of weak controls, such as a lack of oversight, through to determined individuals or organised groups deliberately probing for ways to exploit programs and schemes, and creatively using tried and tested fraud methods to mislead or exploit the system.

Fraud control testers therefore need to be equally creative and think critically about processes and systems from the perspective of a fraudster. They do not assume controls work effectively or trust that people will follow processes, rules and norms.

Instead, fraud control testers challenge assumptions and scrutinise processes and controls by adopting a fraudster's mindset.

The following Fraudster Personas, developed by the Commonwealth Fraud Prevention Centre, give fraud control testers and business stakeholders practical direction to help them adopt a fraudster's mindset.[23] Moreover, as they represent the different actions fraudsters use, they are an effective tool for scrutinising the effectiveness of fraud controls. In particular, they help fraud control testers consider techniques to test, probe and find creative ways to bypass controls – just like fraudsters do.



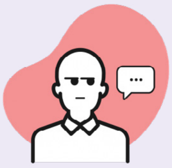
### The Reckless

The Reckless acts recklessly (without care, responsibility or regard to the consequences of their actions) by disregarding requirements, procedures, warnings or directions.

For example, the Reckless might target a scheme of business process by:

- claiming a benefit without checking if they are eligible
- using grant funds for personal use.

The Reckless is countered by measures that support clear and consistent requirements and processes.



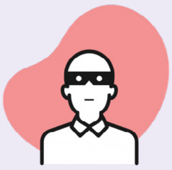
### The Deceiver

The Deceiver dishonestly gains a personal benefit by making others believe something that is not true.

For example, the Deceiver might target a scheme of business process by:

- misrepresenting facts or circumstances to receive a benefit
- withholding pertinent information to get increased payments.

The Deceiver is countered by measures that support honesty, integrity, information sharing and verification.



### The Impersonator

The Impersonator dishonestly gains a personal benefit by pretending they are another person or entity.

For example, the Impersonator might target a scheme of business process by:

- posing as a vendor to hijack a payment
- using stolen identities to receive a fraudulent payment.

The Impersonator is countered by measures that support identity security and authentication.

[23] Commonwealth Fraud Prevention Centre, Discover different types of fraudsters

### The Fabricator

The Fabricator dishonestly gains a personal benefit by inventing or producing something that is false.

For example, the Fabricator might target a scheme of business process by:

- fabricating documents to receive a grant
- fabricating receipts to receive a rebate.

The Fabricator is countered by measures that support information sharing and verification.

### The Coercer

The Coercer dishonestly gains a personal benefit by influencing, manipulating or bribing another person to act in a desired way.

For example, the Coercer might target a scheme of business process by:

- bribing and coercing someone within an organisation
- targeting staff or vulnerable members of the community.

The Coercer is countered by measures that support probity, information security, oversight and deterrence.

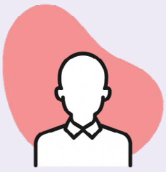
### The Exploiter

The Exploiter dishonestly gains a personal benefit by using something for a wrongful purpose

For example, the Exploiter might target a scheme of business process by:

- embezzling money, equipment, vehicles etc.
- exploiting vulnerabilities in controls, such as a lack of accountability or oversight, to commit fraud.

The Exploiter is countered by measures that support people, process and system integrity, oversight and deterrence.



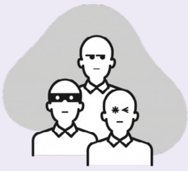
### The Concealer

The Concealer dishonestly gains a personal benefit by preventing their actions from being seen or known about.

For example, the Concealer might target a scheme of business process by:

- deleting records to hide fraudulent activity
- concealing the true nature of their circumstances to receive or increase payments or services.

The Concealer is countered by measures that support oversight and transparency.



### The Organised

The Organised dishonestly gain a benefit by using any combination of the other methods in a planned, coordinated and sophisticated way, ranging from local community groups to transnational syndicates based offshore.

For example, the Organised might target a scheme of business process by:

- creating false websites and pages to legitimise a fraudulent scheme
- working in groups or with professional facilitators to falsify statements or eligibility.

The Organised is countered by measures that support information sharing and strategic collaboration.

**Note:** fraudsters often exhibit behaviours from several different personas. For example, they may deceive a public official, impersonate another individual, fabricate evidence and then conceal their activity.

More information about how to use these Fraudster Personas in a variety of practical ways can be found at counterfraud.gov.au/discover-different-types-fraudsters.

# Mapping business processes

Key to delivering an effective fraud control testing capability, as part of the Fraud Risk Management Cycle, is a thorough understanding of the organisational landscape. Furthermore, the Institute of Internal Auditors Research Foundation (IIARF) has developed a comprehensive methodology for integrated assurance, which notes that control effectiveness is determined based on two distinct areas:

- The architecture or design of the system (control attributes) that encompass the intrinsic characteristics of the process, as well as interrelationships with other processes
- The level of actual performance or functioning of the system, which may range from partial to full execution of the controls as they were designed to be performed
- The overall assessment of an internal control system's effectiveness is based on a combination of these conclusions.[24]

Business process mapping is the visualisation of business processes, allowing for a top-down view of the architecture or design of the system. A process map or flowchart describes the flow of materials and information, displays the tasks associated with a process, shows the decisions that need to be made along the chain and shows the essential relationships between the process steps.[25]

Business process mapping uses charts, flowcharts, and symbols to address the following:

- What triggers the start of a process and what are the subsequent tasks?
- Who performs each task (who are the actors in the process)?
- When does each task occur?
- Why does the step/task exist. e.g. If the step is designed to stop an unintended consequence or fraud, it is a control? This question should be applied at each point of the process.

Fraud control testers need to work collaboratively with stakeholders to gain an informed understanding of the process or system, identify the existing controls in place and understand their design and purpose.

A key way to identify vulnerabilities at different points in a process is to combine the Fraudster Personas with business process mapping.[26] By identifying different threats across the business process, fraud control testers and stakeholders can better understand precisely where and how a scheme or business function might be vulnerable to fraud.[27] This also helps fraud control testers articulate and communicate these threats to decision makers and program designers, and put in place appropriate and effective mitigations at the right point in the process.[28]

[24] Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, p. 19

[25] GCF Professional Standards and Guidance: Fraud Prevention, C15. Business Process Mapping

[26] Fraud Risk Assessment Leading Practice Guide, Commonwealth Fraud Prevention Centre, 2022

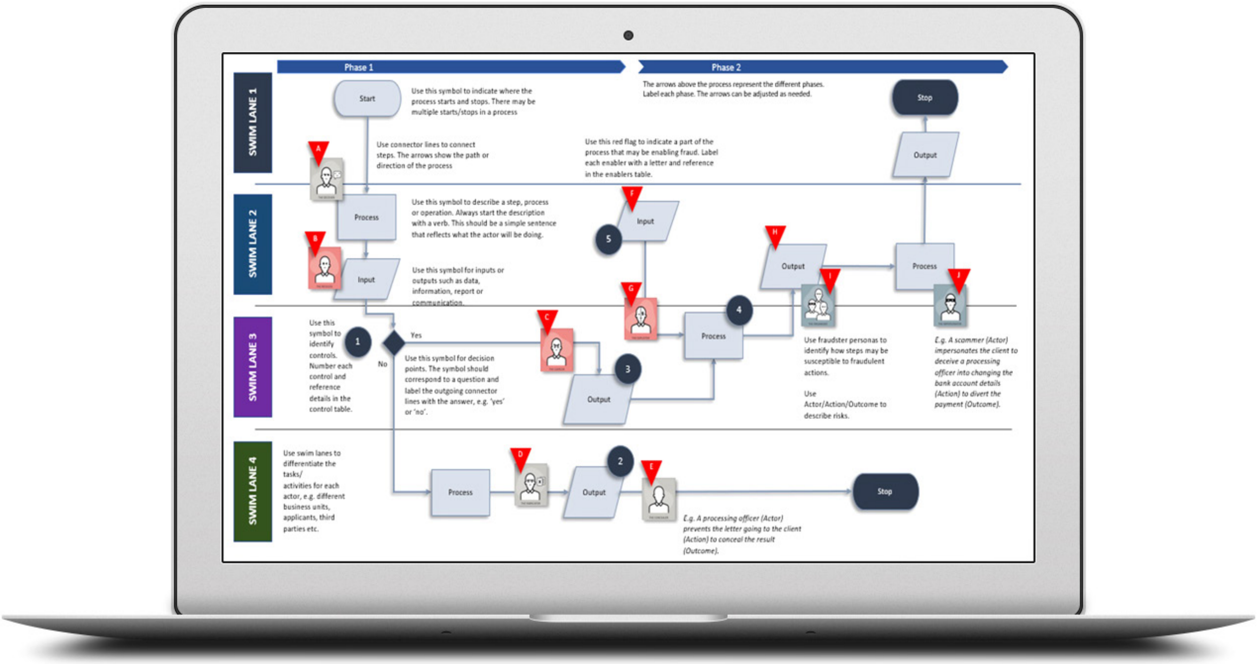
[27] Guide on the Practical Use of Fraudster Personas, Commonwealth Fraud Prevention Centre, 2022 pp. 12-13

[28] GCF Professional Standards and Guidance: Fraud Prevention, D3. Business Process Mapping

Business process mapping can be completed in multiple ways using different tools and software. The tools used to map the process, as well as the level of detail included, will depend on the specific needs of the users and the audience. It may be appropriate to develop multiple types of process maps, for example a detailed process map to examine specific tasks within the control environment and a more simplified version that communicates high-level processes and results to stakeholders and decision-makers.

Business process mapping is the visualisation of business processes, allowing for a top-down view of the architecture or design of the system.

The Business Process Mapping Guide and Template (Ref: FCTF-11) provides a template for communicating a business process in a simplified format.



Use this symbol to indicate where the process starts and stops. There may be multiple starts/stops in a process

The arrows above the process represent the different phases. Label each phase. The arrows can be adjusted as needed.

Use connector lines to connect steps. The arrows show the path or direction of the process

Use this red flag to indicate a part of the process that may be enabling fraud. Label each enabler with a letter and reference in the enablers table.

Use this symbol to describe a step, process or operation. Always start the description with a verb. This should be a simple sentence that reflects what the actor will be doing.

Use this symbol for inputs or outputs such as data, information, report or communication.

Use this symbol to identify controls. Number each control and reference details in the control table.

Use this symbol for decision points. The symbol should correspond to a question and label the outgoing connector lines with the answer, e.g. 'yes' or 'no'.

Use fraudster personas to identify how steps may be susceptible to fraudulent actions.

Use Actor/Action/Outcome to describe risks.

*E.g. A scammer (Actor) impersonates the client to deceive a processing officer into changing the bank account details (Action) to divert the payment (Outcome).*

Use swim lanes to differentiate the tasks/ activities for each actor, e.g. different business units, applicants, third parties etc.

*E.g. A processing officer (Actor) prevents the letter going to the client (Action) to conceal the result (Outcome).*

# Identifying controls

Controls are individual measures, processes or functions that help public bodies prevent, detect and respond to fraud. An integrated assembly of controls make up a control environment.

As with identifying fraud risks, fraud control testers may be able to use available fraud risk assessments to identify existing controls. However, fraud control testers will also likely discover undocumented controls when they engage with relevant stakeholders. Business processes mapping also helps identify the touch point where the controls are triggered and the purpose of each control.

After identifying the controls, the next stage is to assess them by categorising what they do. Controls can be categorised as:

| Prevention | Detection | Response |
|---|---|---|
| These controls are the most common and cost-effective way to reduce fraud. They reduce the likelihood and consequences of fraud by preventing or limiting the extent of the risk occurring. They can include people or process controls to increase transparency and influence behaviours, or processes and technology-based controls to stop or limit fraudulent activity. | These controls help to identify when fraud has occurred. They can help disrupt additional fraud and reduce the consequences. Detection controls are not as cost effective as prevention controls. However, the impacts of fraud can be significantly reduced if detected early. They can include people and process controls such as conducting fraud awareness training and developing tip-off processes or technology-based controls such as fraud detection programs. | These controls respond to fraud after it has occurred. They help to reduce the consequences or disrupt additional consequences. Response controls are not as cost effective as prevention or detection controls. However, if implemented effectively, the present and future impacts of fraud can be significantly reduced. They can include people and process controls such as trained fraud investigators and investigation processes, or technology-based controls such as audit logging and surveillance. |

Each of the 3 categories can then be broken down further to detail the response required:

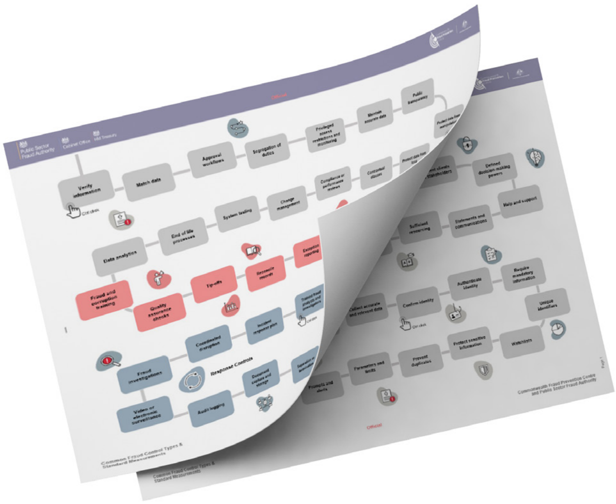
- **Deterrent** - These aim to put people off of fraud. Deterrent controls could include the publication of consequences or investigation sanctions.
- **Directive** - These controls give direction. They include guidance, policies and legislation. Directive controls state the practice to be followed, but do not stop fraud and bad practice occurring - for example, expenses policies.
- **Preventative** - These aim to stop the fraud entering the system or reduce it. Preventative controls could include due diligence checks, multi-factor authentication or segregation of duties for payment approvals.
- **Detective** - These aim to find or identify fraud after it has happened, and can impact on its duration and impact. Detective controls could include audits and financial reports. Detective controls will often lead to corrective actions.
- **Corrective** - These aim to make post-event corrections. Corrective controls could include the recovery of overpaid expenses direct from wages or terminating a process.[29]

[29] GCF Professional Standards and Guidance: Fraud Prevention, C9. Types of Controls

## Business processes mapping ahelps identify the touch point where the controls are triggered and the purpose of each control.

The Fraud Control Catalogue (Ref: FCTF-12) developed by the Commonwealth Fraud Prevention Centre[30], provides an extensive reference of different categories of fraud controls. Fraud control testers can use this catalogue in combination with fraud risk assessments and Fraudster Personas to identify existing controls and gaps across a scheme or business function.

This catalogue also provides guidance on how to measure different types of controls, which can improve the quality and consistency of testing across similar types of controls. Consistent categories and metrics can also improve reporting.



This 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).

The vulnerability indicators in this catalogue acknowledge the inherent limitations in fraud controls that public bodies put in place, such as:

- human error (caused by a lack of awareness, insufficient training, unclear policies, change, workload pressures, carelessness and fatigue)
- an ability for management to override controls, and
- technical or resource limitations, such as insufficient staff to adequately segregate duties.

This provides direction on the types of vulnerabilities public bodies should be testing for.

[30] Commonwealth Fraud Prevention Centre, Discover the different common countermeasures

# Testing methods

The Framework provides different methods to evaluate different types of schemes, functions and controls.[31] These testing methods range from compliance testing such as desktop research and observing process walk-throughs, through to more active testing methods, such as technical system testing and covertly testing processes and controls. The methods are flexible enough to enable departments and public bodies to evaluate control effectiveness at any stage of a program/project lifecycle, including before processes or systems are implemented.

| | | |
|---|---|---|
| Compliance Testing | Review | **Desktop reviews** – Review existing documents and compare against better practice and mandatory requirements. This simple, low cost method enables fraud control testers to confirm that the design of a control is sound.<br>**Case studies** – Review related circumstances where fraud has occurred. Case studies, including those from other organisations, can highlight gaps and vulnerabilities in processes and systems, and provide a strong evidence base to drive continuous improvement. |
| | Observe | **Interviews, workshops or surveys** – Collaborate with those involved in the implementation and/or design of a process, system or specific control to understand its operation and purpose.<br>**System or process walk through** – Step through the process to demonstrate existing practices, how fraud controls apply and known workarounds. This also helps to develop and/or validate a business process map to identify how the system or process works, who is involved, and where different controls apply. |
| | Analyse | **Sample analysis** – Selecting a determined amount or percentage of transactions within a population to test against a specific policy, process and/or procedure. This method is usually used to determine compliance and can be a useful approach when it is impractical to examine every transaction within a population.<br>**Data analysis** - Collecting quantitative and qualitative data and interpreting the results to measure control effectiveness and fraud impacts. Using data to analyse controls also unlocks the potential to put in place ongoing automated assurance monitoring. |
| Pressure Testing | Actively Test | **Technical testing** – Practical testing of fraud controls to confirm they exist and observe how they operate. Exploratory testing gives you the freedom to creatively probe and look for vulnerabilities in a process or system (often a test environment).<br>**Covert testing** – Controlled scenario-based testing aimed at finding a way around fraud controls and observing responses. This complex testing method helps to test controls in their natural state and gather evidence of how they operate under certain conditions. |

[31] Adapted from the Commonwealth Pressure Testing Framework, Commonwealth Fraud Prevention Centre, 2020

## Compliance testing

Compliance testing methods will always be a necessary part of fraud control testing as they provide valuable evidence of how processes, systems and controls operate. These methods also help practitioners critically evaluate controls to ensure they are in place, are being consistently applied and are working effectively. These basic methods are especially useful for public bodies who are building their capability, or those that have less capability and fewer resources. Compliance Testing involves research and working collaboratively with stakeholders to understand and observe how controls work. In fact, stakeholder engagement is the most essential component of fraud control testing. Fraud control testers should directly engage staff at all levels, from senior officials and policy experts to frontline staff. Engaged stakeholders are essential for helping fraud control testers understand complex or discrete processes and procedures. Fraud control testers will also need to collaborate with stakeholders to co-design fraud risk treatments.

Fraud control testing must also go beyond confirming that controls are in place and processes are being followed. Fraudsters are a capable, committed and creative adversary. Therefore, control testing in the counter fraud context must also involve adopting a fraudster's mindset and sometimes applying the common methods used by fraudsters to find ways around controls. Practitioners need to apply creativity, agility and innovation in the development of testing methods. This helps them find vulnerabilities and challenge assumptions about how fraud is being managed within departments and public bodies.

## Pressure Testing

Pressure Testing[32] is an active form of testing that examines 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. In some circumstances, pressure testing 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. This capability is regularly deployed by governments and private sector organisations to identify cyber security vulnerabilities, e.g. ethical hacking. Ethical hackers have the same skills as malicious hackers, and they also learn the lessons from previous attacks to understand how malicious hackers operate and copy their strategies. However, ethical hacking is not limited to testing cyber controls. Simulating the actions and mindset of a fraudster is also a proven way to identify vulnerabilities across a range of fraud controls, including processes controls, physical security controls and asset security controls.

Furthermore, Pressure Testing controls can reveal vulnerabilities that other methods may miss. Sometimes the data obtained from desktop reviews, interviews and system or process walkthroughs can be misleading and provide false assurance on control effectiveness. Business functions are often overconfident in the strength of their controls, while procedures or system specifications do not always tell the true story of how things operate in the real world. Pressure Testing is an effective way to evaluate controls but is not essential nor necessarily the best testing method in every circumstance. Moreover, Pressure Testing (particularly covert testing) carries risk and may impact negatively on stakeholder relationships. It can also take more time to plan and execute due to the additional governance and documentation involved. Therefore, practitioners should always consider if other testing methods can provide similar results.

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

## Guidance on testing methods

The Handbook of Fraud Control Testing Methods (Ref: FCTF-14) provides practical guidance on how to use different methods to test controls, including examples.

OFFICIAL
Commonwealth Fraud Prevention Centre
Handbook of fraud control testing methods

# Choosing the right method to test controls

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. In their comprehensive methodology for integrated assurance, IIARF provide further direction on assessing control effectiveness:

Once the controls are identified across the process, in relation to control objectives, the first step is to understand the components. This will help you:

- Verify the completeness of the control
- Understand the relationships between the various control components

The next step is to assess the adequacy of each control with respect to the control objective(s). The aggregation of these analyses throughout the various activities of a process will allow the overall evaluation of the internal control system.[33]

In summary, understanding the design and purpose of controls is fundamental to identifying the right metrics for control effectiveness. Controls vary in their purpose and application. For example:

**Testing Methods**

**Cultural and behavioural factors** can play a large role in encouraging or discouraging fraudulent activities. Some controls 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 controls** manage risk through a consistent application of designed functions. If designed correctly, controls such as mandatory requirements, evidence verification, decision making - protocols, 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 controls** manage risk through automated application of designed functions. If designed correctly, controls such as guided procedures, data matching, audit logging and fraud detection programs can:

- automatically enforce consistent compliance with rules, processes and expectations
- automatically safeguard against non-compliance with rules, processes and expectations.

[33] Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, p. 20

Identifying metrics to determine that a control is achieving its purpose will help fraud control testers develop appropriate methods for testing control effectiveness. It is also important to consider how controls work alongside other controls, as no single control works in isolation – it is a component of an integrated control environment.

Different testing methods are also often needed to determine the effectiveness of controls, as performing stakeholder interviews, system or process walkthroughs, sample testing and data analysis on their own may not provide a full picture.

A good analogy is how someone might measure the value of a gold nugget. They cannot measure the value of the nugget just by weighing it. Nor can they measure its value just by its purity. They need to first weigh the nugget, then perform an acid test to determine its purity, before finally checking the current market price for gold. Similarly, there may be different measurements needed to determine the true effectiveness of a control.

Different testing methods are also often needed to determine the effectiveness of controls.

For example, if testing the effectiveness of a business functions' identity authentication procedures, fraud control 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.

Covert testing would not be a viable method of testing in this scenario. You may be able to use social engineering to convince an employee to bypass authentication procedures, but this provides little data regarding control effectiveness without performing this test across a representative sample of employees.

The Fraud Control Catalogue (Ref: FCTF-12) provides guidance on measuring different types of fraud controls. Start by identifying what category the control falls into before considering suggested measurements and vulnerability indicators.

# Drawing conclusions on control effectiveness

Understanding the design and purpose of a control is fundamental to determining its effectiveness. The data gathered through testing supports the fraud control tester to draw conclusions on whether the control is functioning in a way that conforms to its purpose and if there are factors that could undermine the control objectives.

## Criteria for assessing control effectiveness

The criteria used to assess control effectiveness will vary depending on the type of control and the data that has been acquired through testing. The following criteria are a helpful reference when assessing the design of fraud controls:[34]

| | | |
|---|---|---|
| Control Effectiveness | **Relevance** | How relevant and up-to-date is the control to the risks being mitigated? For example, a quality assurance process may only check that processes had been completed, not for fraudulent claims. |
| | **Coverage** | To what extent does the control address all significant risks? For example, do fraud detection algorithms cover only some of the risks across a process? |
| | **Timeliness** | How long would it take for the control to respond to negative events and minimise adverse consequences? For example, sending a letter to a vendor about bank account changes may not allow for timely action to stop fraudulent payments. |
| | **Reliability** | To what extent can the control be relied upon to perform its intended function without failure? For example, are employees sufficiently trained to identify fraudulent evidence? |
| | **Discretion** | Is there a level of discretion or subjectivity in the application of the control? For example, can the application proceed without the user uploading mandatory evidence to the online form? |
| | **Segregation** | Is there segregation between the control and those subject to the control? For example, can the same employee or team create a vendor record and process an invoice? |
| | **Independence** | Is the control's execution dependent on resources that might not always be available? For example, does detection software rely on data that might not always be available. |

[34] Adapted from Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, pp. 21-23 and Canada Revenue Agency's Risk Exposure and Tolerance Assessment tool.

| | | |
|---|---|---|
| Control Effectiveness | **Integration** | To what degree and manner is the control integrated with other controls? Does it support other controls? For example, does the automated decision-making workflow ensure decisions are made in line with defined authorisations/delegations? |
| | **Automation** | Is the control automated or applied by people? If applied by people, how do you know they are applying the control consistently or correctly? Are automated controls still reliant on some human input, which might allow for errors? |
| | **Adaptability** | How adaptable is the control to fluctuating volumes of activity or changing environments? For example, are system audit logs turned off during peak periods to enhance system performance? |
| | **Traceability** | To what extent is the control traceable, allowing it to be verified? For example, is data available that would allow you to confirm monthly reconciliations are actually performed? |
| | **Validation** | To what extent has the control been tested and reviewed against the risk? For example, is there documentation showing segregation of duties controls are regularly audited or monitored? |

Public bodies may wish to develop additional processes to increase the objectivity of their assessments. For example, Canada Revenue Agency’s Risk Exposure and Tolerance Assessment tool includes the following criteria for assessing the relevance of a control:

| Values | Indicating |
|---|---|
| **Very low / Unknown** | The control is marginally relevant in directly affecting the likelihood and impact of the materialisation of the risk, or its relevance is unknown. |
| **Low** | The control is slightly relevant in directly affecting the likelihood and impact of the materialisation of the risk. |
| **Moderate** | The control is somewhat relevant in directly affecting the likelihood and impact of the materialisation of the risk. |
| **High** | The control is relevant in directly affecting the likelihood and impact of the materialisation of the risk. |
| **Very high** | The control is completely relevant in directly affecting the likelihood and impact of the materialisation of the risk. |

## Rating control effectiveness

The design and purpose of a control is also fundamental to rating its effectiveness. It may be appropriate to allow for some tolerance in the coverage or operation of certain controls. For example, fraud awareness training may still be effective even if 100% of employees have not received the training. On the other hand, some controls might be ineffective if they fail to perform their intended function only 0.01% of the time.

The following traffic light system is a useful way to communicate where controls are effective or where vulnerabilities may require action.

| Rating | | Indicating | Action Required |
|---|---|---|---|
| 👍 | **Effective** | The control is functioning in a way that conforms to its purpose and there are few factors that could undermine the control objectives. | Identify opportunities to put in place ongoing assurance monitoring. |
| 👌 | **Partially Effective** | The control somewhat functions in a way that conforms to its purpose and/or there are possible factors that could undermine the control objectives. | Review the control and consider action to improve its design and/or operational effectiveness. Consider implementing backup controls (fail-safes). Identify opportunities to put in place ongoing assurance monitoring. |
| 👎 | **Ineffective** | The control does not function in a way that conforms to its purpose and/or there are likely or existing factors that could undermine the control objectives. | Replace the control, improve its design and/or operational effectiveness, or implement backup controls (fail-safes)<br>Alternatively, remove the control. |

# Assessing and measuring residual risk

An important consideration when analysing a fraud risk is the nature, extent and effectiveness of fraud controls. Residual risk is the risk remaining once the risk response has been successfully applied.[35] The effectiveness of the control environment can have a direct influence on residual risk, i.e. the likelihood of occurrence, the frequency of fraud occurring, the duration of fraud and the materiality of its impact.[36]

The results of the fraud control testing activity provide additional business insights to more accurately assess and measure the residual risks.[37] See the UK's Government Counter Fraud Professional Standards and Guidance: Fraud Risk Assessment for more guidance on evaluating residual risk.

The results also help public bodies put in place ongoing monitoring and assurance mechanisms, to help Boards and risk owners stay informed about changes to control effectiveness, and ultimately the risk ratings.

## Measuring residual risk

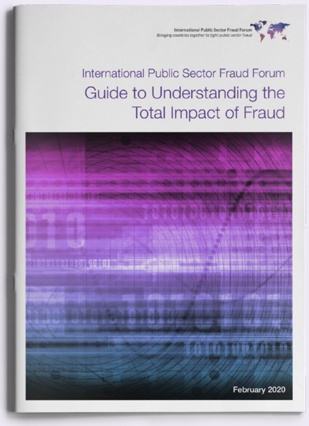
The financial impact of fraud is commonly measured by the level of financial loss that might occur as the result of a single incident, or through cumulative losses from several incidents over a period of time.

An estimate of the potential cost of residual fraud risk can be measured by multiplying the probable frequency of the risk occurring with an estimate of the following impacts:

- Victim impact - Losses, damages or penalties, and/or lost income arising from risk events
- Business impact - Cost of the resolution of risk events, which varies in relation to the actions needed to limit the impact of negative events that occur. These include internal costs to restore a situation (for example, reprocessing costs and advertisement investments to recover from reputational damage).[38]

It is also important to consider the non-financial impacts of fraud when measuring residual risk. The International Public Sector Fraud Forum's Guide to Understanding the Total Impact of Fraud discusses the different impacts of fraud against the public sector, including human impacts, reputational damage and industry impacts.

This more accurate assessment and measurement of residual fraud risk will help risk owners make better informed decisions about their fraud risk tolerance. This in turn will help fraud control testers work with stakeholders to draw a conclusion on whether the control environment is mitigating the risk of fraud to a level within tolerance.[39]


International Public Sector Fraud Forum
International Public Sector Fraud Forum
Guide to Understanding the
Total Impact of Fraud
February 2020

[35] GCF Professional Standards and Guidance: Fraud Risk Assessment, p. 68
[36] GCF Professional Standards and Guidance: Fraud Risk Assessment, p. 58
[37] GCF Professional Standards and Guidance: Fraud Risk Assessment, pp.33-34
[38] Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, p. 44
[39] Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, p. 43

# Evaluating the effectiveness of the control environment

CEAs involve testing multiple controls within an integrated control environment. In evaluating the control environment, the fraud control tester should consider the following questions:

- Does the control environment provide ‘defence in depth’ through a good balance of different categories of controls?
- Are there any critical gaps in the control environment?
- How do the controls operate collectively?
- What parts of the process are susceptible to control weaknesses?
- How critical are the controls that are not fully effective?

It is important to note that a control environment can still be effective even if some controls have been assessed as ineffective or partially effective. Also, a control environment can be ineffective even where the vast majority of controls are effective. This is because not all controls are equal in the effect they have on the risk.

Furthermore, a control environment can have different levels of effectiveness for different types of risk and risk tolerances. For example, a control environment may be effective in mitigating fraud by a lone actor but ineffective in mitigating fraud by colluding actors. Also, the objective of a control environment is to mitigate risks to within tolerable levels, not eliminate risk completely (unless the tolerance is zero).

Fraud control testers should also use a traffic light system to communicate how effective the overall control environment is in mitigating different types of risks to a level within tolerance:

| Rating | | Indicating |
|---|---|---|
| 👍 | **Effective** | The control environment is effective at mitigating the risk of fraud to a level within tolerance. |
| 👌 | **Partially Effective** | The control environment needs some strengthening and improvement to bring fraud risk to a level within tolerance. |
| 👎 | **Ineffective** | The control environment needs substantial strengthening and improvement to bring fraud risk to a level within tolerance.40 |

[40] Adapted from Managing the Business Risk of Fraud: A Practical Guide, Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners, Annex F

## Root Cause Analysis

Root Cause Analysis is the use of a clearly defined methodology to investigate the primary causes of a problem. It can be conducted in a variety of ways. One approach is the "5 whys method".

For example:

Root Cause Analysis can uncover the factors underlying a problem, help to identify other related issues and suggest appropriate solutions. It can be used to highlight the cause of any policy, programme, system, process or control failures, identify the reasons for failure and focus on the necessary remedial actions - including the design and implementation of new controls.[41]

5 whys method

Question

**Why is the process vulnerable to fraud?**

Information is not being verified

Question

**Why is information not verified?**

The system does ask for verification

Question

**Why is verification not requested?**

It is not a built-in requirement

Question

**Why was it not built into the system?**

That wasn't in the design criteria for the scheme

Question

**Why was it not in the design criteria?**

Because there was insufficient understanding of scheme fraud risks at the design stage

# Treating control vulnerabilities

Fraud control 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:

- cultivate positive and productive relationships between counter fraud teams and business stakeholders, leading to more informed, better designed and more cost-effective treatments[42]
- encourage greater buy-in, sense of ownership and follow-through from stakeholders in addressing the identified vulnerabilities in their schemes and business processes.

## Developing SMART treatments

The SMART principle[43] is an example of what to consider when co-designing treatments with stakeholders:

| | |
|---|---|
| **Specific** | 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. |
| **Measurable** | The treatment and its progress should be measurable. Consider:<br>• What does the completed treatment look like?<br>• What are the benefits of the treatment and when they will be achieved?<br>• The cost of the treatment (both financial and staffing resources)<br>• How do the costs balance against the treatments? |
| **Achievable** | The treatment should be practical, reasonable and credible considering the available resources. Consider:<br>• Is the treatment achievable with available resources?<br>• Does the treatment comply with policy and legislation? |
| **Relevant** | The treatment should be relevant to the risk. Consider:<br>• Does the treatment modify the level of risk (through impacting the causes and consequences)?<br>• Is the treatment compatible with organisational objectives and priorities? |
| **Timed** | The treatment should specify timeframes for completion and when benefits are expected to be achieved. |

[42] GCF Professional Standards and Guidance: Fraud Prevention, C17. Stakeholders

[43] GCF Professional Standards and Guidance: Fraud Prevention, C21. Measure, Monitor and Evaluate Effectiveness

The SMART approach will help public bodies describe what each treatment actually does to mitigate the vulnerability and how it will operate. They should also be able to describe what the control does not do in relation to mitigating the vulnerability. By being specific about the effect, public bodies will be able to design treatments that are:

- Easier to explain and negotiate – there will be a clear and specific purpose (relevant to the risk)
- More relevant – it will be clearer how the treatment modifies the risk
- Better designed – there will be clearer requirements and therefore it will be easier to implement
- More targeted – it will be clearer where, when and to whom the treatment should apply
- Proportionate – there will be a specific intent to the treatment, and therefore it will more likely stay compatible with the public body's objectives and priorities
- Easier to measure if they are working effectively – it will be clearer how the treatment is designed to work
- Easier to measure their value – it will be clearer what affect/change the treatment is expected to deliver and when the benefits are expected to be achieved.

## Developing cost-effective treatments

In their comprehensive methodology for integrated assurance, IIARF provide direction on striking the right balance between the cost and effectiveness of controls:

The overall adequacy of internal controls is determined by:

- Effectiveness, which is the capacity to guarantee the minimization of the probability and impact of any risk event, within determined limits
- Cost-benefit factor, which is the capacity to guarantee that the overall cost of the control does not exceed the cost that will incur if the risk event takes place.

Ample analysis can be conducted to seek maximum efficiency, which is intended as the optimal balance between the effectiveness and cost-benefit factors of the controls. In general, the greater the effectiveness of a control, the greater the cost; alternative control solutions can be deployed in search of a positive marginal benefit (possibility to improve the effectiveness/cost-benefit factor ratio).[44]

The cost of control is measured based on fixed and nonfixed costs (e.g., dedicated resources, operational costs, costs of maintaining the information system, etc.) as well as external costs through partners of insurers. This cost should be compared to that of managing residual risk.

The UK's Government Counter Profession Fraud Prevention Standard provides guidance on cost benefit analysis,[45] proportionality,[46] and calculating prevented fraud.[47]

See Appendix D for example formulas for estimating the return on investment for implementing new risk treatments or enhancing existing controls.

[44] Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, p. 20
[45] GCF Professional Standards and Guidance: Fraud Prevention, D7, Cost Benefit Analysis
[46] GCF Professional Standards and Guidance: Fraud Prevention, C3. Proportionality
[47] GCF Professional Standards and Guidance: Fraud Prevention, C14. Prevention Methodologies

# Reporting and monitoring

Each jurisdiction will have local requirements in relation to reporting and monitoring. It requires public bodies to define and establish a governance and management framework that includes:

- requirements for fraud, bribery and corruption risk reporting, incident management, and
- the arrangements for obtaining organisational assurance.

Therefore, in the UK, public bodies should regularly report internally on the results of fraud control testing activities, including trends and lessons learned, through their governance committees to support effective fraud risk oversight and management. This approach may be equally relevant or adaptable beyond the UK.

## Reporting results to the PSFA

The UK also requires a governance and management framework including requirements for tracking and reporting performance in organisations.

To support those working in Counter Fraud to adhere to this standard, public bodies who undertake fraud control testing should maintain records and report onwards as is relevant in their jurisdiction, the following at the end of each financial year or upon request:

- The number of TCAs and the number of CEAs currently underway.
- The number of TCAs and the number of CEAs completed.
- The total number of controls tested via both TCAs and CEAs.
- The number (and percentage) of controls found to be Effective, Partially Effective and Ineffective.
- The number of treatments recommended and the total number agreed to be implemented.
- The total estimated value of risk treatments.
- The number of resources dedicated to fraud control testing (Full Time Equivalent at both the beginning and end of the financial year).

## Lessons learnt reviews

Public bodies should embrace the philosophy of continuous improvement and undertake lessons learnt reviews upon the completion of fraud control testing activities. These reviews should consider:

- The objectives set
- The outcomes achieved
- The successes
- The areas for further work
- Recommendations for change or matters that require executive level discussion.[48]

The review report should contain explicit recommendations, with clearly defined responsibilities and timelines, for action and a process for escalation to executive level within the organisation. Review findings should be shared with stakeholders, including across Government functions and agencies, if appropriate.

See the GCF Professional Standards and Guidance: Fraud Prevention for more guidance on undertaking lessons learnt reviews.

[48] GCF Professional Standards and Guidance: Fraud Prevention, D8. Lessons Learnt reviews

# Appendices

# **Appendix A** – Supporting procedural guides and tools

The following procedural guidance and tools can support public bodies to apply consistent and leading practice approaches to fraud control testing. These are available on request from PSFA@cabinetoffice.gov.uk

### Targeted Control Assessments - Procedural Guide

This outlines the process for undertaking a TCA, including a process map, an overview of the different stages, and links to different tools and templates.

### Control Environment Assessments - Procedural Guide

This outlines the process for undertaking a CEA, including a process map, an overview of the different stages, and links to different tools and templates.

### Pressure Testing Sub-framework

This outlines the process for undertaking Pressure Testing (i.e. technical and covert testing), including a process map, key principles, roles and responsibilities, additional governance requirements, and links to different tools and templates.

### Strategic Fraud Risk Profiling tool

Conducting fraud control testing across multiple schemes and functions delivered by a public body can be complex, time consuming and difficult to prioritise. Strategic-level fraud risk profiling can assist public bodies to identify those areas of the organisation that are more susceptible to fraud risk. This will enable them to formulate a 'heat-map' for fraud risk across the public body and implement fraud control testing activities on a prioritised basis.

### Priority Assessment tool

This tool is designed to assess potential risks and used to determine the priority order of upcoming fraud control testing activities. The tool compares various risks to guide the prioritisation of fraud control testing activities. Each proposal should be assessed and scored against the four components, and the scores combined to provide a total score.

### Business Process Mapping template

This template provides the tools to help fraud control testers work with stakeholders to visualise the business processes. It also provides instructions on how to map business processes and apply a fraud lens to identify vulnerabilities in the process, expanding on information in Chapter 8 of this Framework.

### 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 fraud control testers adopt a fraudster's mindset to identify avenues where fraudsters might exploit programs or functions and uncover potential vulnerabilities.

### Fraud Control Catalogue

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

### Control Criticality Assessment Tool

Not all fraud controls have the same impact on the management and reduction of the risk. Some fraud controls may be absolutely critical to the management of the risk, while other fraud controls may only have a minor impact on the risk. This tool can help public bodies identify their most critical fraud controls in countering particular risks and determine where to invest their time and resources.[49] Understanding the design and purpose of a control is fundamental to determining how, and to what extent, it reduces the risk. Therefore, collaboration with business areas and subject matter experts will help achieve a more accurate and objective assessment.

### Handbook of Fraud Control Testing Methods

This handbook provides practical advice on the variety of methods available to test the effectiveness of fraud controls. It provides examples across the spectrum of testing methods, expanding on information in Chapter 10 of this Framework.

### Red Team vs Blue Team Activity Planner

This Activity Planner provides an outline of how to run a Red Team vs Blue Team exercise with stakeholders. These gaming exercises are an effective way to help stakeholders analyse a business process from different perspectives, including by adopting a fraudster's mindset (Red Team) to try to find ways around controls.

[49] GCF Professional Standards and Guidance: Fraud Prevention, D5. Control Assessment Tool

# Appendix B – Other frameworks and guides

### Commonwealth Pressure Testing Framework

This framework sets out key principles, processes and materials for conducting fraud control testing within Australian Government entities.

### How to start Pressure Testing guide

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

### 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.

### Undercover policing – Authorised Professional Practice

This guidance on covert-related activity, including undercover policing, helps law enforcement agencies undertake undercover activities in a lawful, proportionate, ethical, safe and consistent way.

### 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.

### 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.

### Evaluating Internal Control Systems

This research report published by The Institute of Internal Auditors Research Foundation sets out a comprehensive methodology for integrated assurance for enterprise risk management. This assurance is based on the evaluation of control and risk management processes, considering all pertinent business and governance objectives, through a unified and unique assessment approach.

# **Appendix C** – The benefits of fraud control testing

The benefits of fraud control testing go well beyond identifying control vulnerabilities and accelerates, improves or otherwise enhances business elsewhere in the public body, delivering wider value. For example, fraud control testing:

### Enhances operational efficiency

Fraud control testing often involves reviewing existing processes and controls. This evaluation can help identify areas of inefficiency, duplication of efforts, or gaps in procedures resulting in operational efficiencies, streamlined workflows, and optimised resource allocations.

### Enhances operational effectiveness

Fraud control testing enhances controls and processes which improves the effectiveness of service delivery and supports the achievement of organisational objectives through reduced error and waste, improved employee engagement and experience, and improved customer or client satisfaction.

### Prevents financial loss

Fraud can result in significant financial losses for public bodies, impacting their ability to deliver services and fulfil their mandates. By implementing fraud control testing, public bodies can identify vulnerabilities and implement measures to prevent fraud before it occurs and safeguard public funds.

### Mitigates fraud risk in an efficient and measurable way

Fraud control testing helps public bodies mitigate fraud risks in a more targeted and effective way. By evaluating internal controls, processes, and procedures, public bodies can proactively address specific vulnerabilities and reduce them in a way that can be measured.

### Increases fraud awareness

Fraud control testing increases awareness of fraud across public bodies, helping officials acknowledge the risk of fraud and the potential for vulnerabilities, making them more effective agents in preventing fraud.

### Deters fraud

The presence of a robust fraud control testing program acts as a deterrent to potential fraudsters. Knowing that fraud control measures are in place and actively monitored can discourage individuals from engaging in fraudulent activities.

### Enables fraud measurement and detection activities

Fraud control testing helps identify specific vulnerabilities within schemes and business functions, which can support the detection of fraudulent activities, allowing timely intervention and appropriate actions to mitigate the impact. By regularly testing internal controls, public bodies can identify red flags and anomalies that may indicate potential fraud, as well as support fraud and error loss measurement.

### Reduces costs

By identifying fraudulent activities early on, public bodies can minimise financial losses and avoid unnecessary expenditures associated with fraud investigations, legal proceedings, and reputational damage.

### Provides assurance that risks are being adequately managed

Fraud control testing contributes to the development of a robust internal control environment, providing assurance that it is adequate and operating efficiently and effectively. It also helps public bodies maintain the integrity of their internal control frameworks during organisational change.

### Preserves public trust

Public bodies have a duty to maintain the trust and confidence of the citizens they serve. By actively conducting fraud control testing, public bodies demonstrate their commitment to transparency, accountability, and responsible financial management; helping to preserve public trust.

# **Appendix D** – Examples of estimating ROI for new treatments

### Example 1 – Estimating the financial value of preventing an irregular type of fraud

Here is an example of how you might estimate the future loss prevented for an irregular type of fraud over a 5-year time horizon. This example estimates the financial benefits of reducing the risk of vendor payments being diverted through mandate fraud. The average vendor payment is $650,000 and the highest value vendor payment is $4 million.

The investment is to licence software to verify bank accounts prior to payment at a cost of $20,000 per year with an initial capital investment of $50,000 in year 1.

| Formula | Example calculations |
|---|---|
| **Amount at risk**<br>Calculate or estimate the amount at risk | $650,000 average value ($4 million maximum value) at risk |
| **Probability of risk**<br>Estimate the probability for compromise to occur with current controls | The risk is expected to occur once every 5 years |
| **Current annual risk** | Annual business impact: $130,000 ($800,000 maximum annual impact) |
| **Impact of investment**<br>Determine the impact of the investment | The probability of risk is halved (expected to occur once every 10 years) |
| **Impact value**<br>Calculate the impact of the investment on the current annual risk | $65,000 impact reduction per year ($400,000 maximum per year) |
| **Total cost over 5 years:** | $150,000 |
| **Impact value over 5 years:** | $325,000 in estimated business impact savings |
| **ROI ratio:** | 2.17 |

### Example 2 – Estimating the financial value of preventing ongoing identity compromise

Here is an example of how you might calculate the future loss prevented through ongoing identity compromise over a 5-year time horizon. To mitigate the threats to client identity information through phishing and social engineering, the department proposes to put service delivery staff through training twice per year and implement regular fraud control testing at a cost of $50,000 per year.

| Formula | Example calculations |
|---|---|
| **Amount at risk**<br>Calculate or estimate the amount at risk | Business impact: $1,500 per victim to remediate identities (notify, issue new identifiers and implement ongoing safeguards)<br>Victim impact: $1,076 per victim[50] and 34 hours per victim to repair the damage[51] |
| **Probability of risk**<br>Estimate the probability for compromise to occur with current controls | The risk currently occurs once every 5 days (73 identity compromises in the previous year) |
| **Current annual risk** | Total annual business impact: $109,500<br>• $146,000 annual impact for victims<br>• 2,482 hours of remediation $38,533 of productive time)[52]<br>Total annual victim impact: $184,533 |
| **Impact of investment**<br>Determine the impact of the investment | The probability of risk is reduced by 10% per year over 5 years |
| **Impact value**<br>Calculate the impact of the investment on the current annual risk | Year 1 - $10,950 business impact savings<br>Year 2 - $21,900 business impact savings<br>Year 3 - $32,850 business impact savings<br>Year 4 - $43,800 business impact savings<br>Year 5 - $54,750 business impact savings<br>Year 1 - $18,453 victim impact savings<br>Year 2 - $36,906 victim impact savings<br>Year 3 - $55,359 victim impact savings<br>Year 4 - $73,812 victim impact savings<br>Year 5 - $92,265 victim impact savings |
| **Total cost over 5 years:** | $250,000 |
| **Impact value over 5 years:** | • $164,250 in estimated business impact savings (0.66 ROI)<br>• $276,795 in estimated victim impact savings (1.11 ROI) |
| **ROI ratio:** | 1.77 |

[50] actionfraud.police.uk/news/identity-fraud-continues-to-rise-with-4-million-victims-in-uk-alone
[51] Australian Institute of Criminology, Statistical Report 27, Identity crime and misuse in Australia: Results of the 2019 online survey.
[52] Office for National Statistics: Average weekly earnings in Great Britain: November 2022