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

International Public Sector Fraud Forum

Fraud Prevention Savings Framework

Public Sector Fraud Authority

Commonwealth Fraud Prevention Centre

Produced in collaboration with the UK Public Sector Fraud Authority and Australia's Commonwealth Fraud Prevention Centre.

Crown copyright disclaimer

Contents

Purpose

This Fraud Prevention Savings Framework sets out key principles and credible approaches to estimating and quantifying the financial and non-financial benefits of fraud prevention and compliance activities, as well as how to confirm and communicate the results.

> Enhancing our ability to measure and prove savings is key to shifting the focus and investment from reactive responses to preventing fraud at the earliest possible stage.

This is a new, developing, yet vital capability in the fight against public sector fraud. Fraud is a hidden and often underestimated problem, causing significant unmeasured harm. The very nature of this problem also leads to a lack of investment to deal with it. Enhancing our ability to measure and prove savings is key to shifting the focus and investment from reactive responses to preventing fraud at the earliest possible stage.

Measuring prevention savings in a credible way depends on preliminary activities being undertaken, such as collecting and analysing relevant data, conducting a fraud risk assessment (FRA) or control testing exercise, or undertaking a fraud loss measurement (FLM) exercise. Good governance arrangements also ensure methods used to determine prevention savings are reasonable, robust, consistent and credible.

Specifically, this Framework:

- outlines the key aspects of Fraud Prevention Savings Measurement (Savings Measurement);
- sets out distinct types of preliminary activities that can help with measuring fraud prevention savings;
- shows the types of savings that can be attributed to distinct types of fraud prevention and compliance activities;
- provides methods and approaches for:

    1. developing counterfactuals
    2. estimating the effect of an intervention
    3. quantifying the resultant savings

- provides advice on how to communicate results to key decision-makers;
- outlines governance arrangements to provide a level of assurance that approaches are robust and consistent; and
- explains when and why to undertake a retrospective measurement and review.

The Framework also offers a range of case studies and links to other core material that support fraud prevention and wider fraud control approaches.

Who this Framework is for

This Framework is developed as organisational guidance for counter-fraud functions across the public sector, supporting them to show the impact and return on investment (ROI) of fraud prevention in existing schemes or when designing new schemes and functions.

It sets out the recommended best practice for Savings Measurement. It is a principles-based document designed to be flexible and adapted to an organisation's individual circumstances.

This Framework is issued by the International Public Sector Fraud Forum (IPSFF) in conjunction with the United Kingdom's Public Sector Fraud Authority (PSFA) and Australia's Commonwealth Fraud Prevention Centre (CFPC).

How to use the Framework

The Framework is designed to guide you through the process of Savings Measurement within your organisation. It is organised in clear sections starting with foundational preliminary activities, moving into measurement methods and concluding with implementation guidance and case studies.

To support your understanding, definitions of the key terms discussed in the Framework are provided upfront in **Table 1**. A complete list of terms used throughout the Framework can be found in the Glossary. Use these to clarify any unfamiliar terminology as you progress.

Where applicable, use the tools and templates in the appendices to aid in applying the Framework to your own fraud measurement activities. For example, Appendix D outlines the skills, training and other important attributes needed to conduct fraud prevention saving measurement.

Table 1 - Definition of key terms

Preliminary activities	These can involve a range of activities to establish a baseline of fraud and error, as well as find their causes and potential interventions.
Baseline	The benchmark for measuring the effect of any type of intervention. This is usually the known or estimated rate of fraud and error; however it can be broader, e.g. total transactions within a specific program, activity or function.
Intervention	Any activity undertaken with the aim of reducing the likelihood (probability and frequency) or consequence (duration and impact) of fraud and error. For example, implementing a new control or compliance program.
Method	The technique by which expected or actual savings are figured out – this may include financial calculations as well as evidence of expected non-financial benefits.
Counterfactual	A key part of the method that looks to show "what would have been" had the intervention not occurred.
Estimating the effect of the intervention	An informed and evidence-based assumption of how the intervention will reduce fraud and error levels (or has reduced fraud and error levels) in comparison to the counterfactual.

	**Quantifying approximate savings**	Calculating the amount expected to be saved based on the difference between the predicted reduced rate of fraud and error and the counterfactual over a defined period.
	**Return on investment (ROI)**	The ratio between the savings expected or achieved by the intervention against the cost of implementing the intervention.

Case studies

A simple case study (the Green Homes Subsidy Scheme) will be used throughout the Framework to help illustrate how the Framework can be applied in practice.

More hypothetical case studies are also provided within the Framework. As you progress through the Framework, you are encouraged to keep your own example in mind – this could be a hypothetical scenario, or a program, function, or activity your organisation is currently managing or planning to implement – to help you relate the concepts and methods to your own context.

Introduction

What is Fraud Prevention Savings Measurement?

Savings Measurement involves applying consistent and credible approaches to estimate and quantify the impact and ROI of fraud prevention and compliance activities in public sector organisations. Our ability to measure prevention savings is a key component of the wider Fraud Control discipline for managing fraud and error risk, and is part of the wider discipline of Fraud Measurement, which also includes Fraud Management Information, Fraud Estimation and Fraud Loss Measurement.

> Savings Measurement is a consistent and credible approach to estimating and quantifying the impact of our interventions to prevent fraud and error.

What are the benefits of measuring prevention savings?

Fraud prevention is widely regarded as the most cost-effective and efficient means of mitigating fraud risk, yet its value and impact have historically been difficult to quantify. However, with improvements in capabilities such as fraud risk assessment, measurement, analytics and reporting, the potential to measure prevention savings and therefore the ROI of counter-fraud activities has become increasingly viable.

For example, analysis of fraud loss and workforce reporting data by the UK PSFA[1] indicates that preventative counter-fraud activities delivered a ROI of approximately three times the rate of reactive approaches. However, this figure does not include costs such as court proceedings or broader societal impacts of fraud that go unchecked until detection. This is consistent with the growing body of research, mainly relating to preventative health, that supports the premise that the earlier we intervene to prevent risk and harm, the higher the ROI will be (see identifying interventions to reduce fraud and error).

From an investment perspective, the benefits that can be realised by measuring the ROI from fraud prevention are significant. Moreover, the wider, longer-term benefits are even more compelling. Greater investment in fraud prevention will also help avoid the less-quantifiable harms caused by fraud (see identifying indirect and non-financial benefits).

Adopting Savings Measurement exercises to quantify the savings delivered from fraud prevention can help public organisations:

- demonstrate benefits achieved through counter-fraud investment;
- provide evidence to support investment in further counter-fraud activities;
- show how benefits of fraud prevention and compliance activities outweigh the cost and regulation associated with countering fraud; and[2]
- achieve a cost-effective fraud management approach through developing an optimal balance between fraud prevention and enforcement (reactive) activities.

The lessons learned from these exercises can also enhance business processes in organisations, delivering wider value. For example, Savings Measurement exercises:

---

[1] PSFA fraud loss and workforce reporting data review showed an ROI of 21:1 for pro-active counter fraud activity. In contrast, the same analysis found reactive measures yielded a lower, yet still notable, ROI of around 5:1

[2] Counter Fraud Investment Cases – Leading Practice Guide. Commonwealth Fraud Prevention Centre. www.counterfraud.gov.au/library/counter-fraud-investment-cases-leading-practice-guide

- support new counter-fraud investment cases and/or an expansion of fraud prevention and compliance activities to other programs, activities or functions of the organisation;
- improve understanding of the impact of fraud prevention and compliance measures in different programs, activities or functions;
- inform the effectiveness of fraud controls; and
- inform evidence-based decisions on how to manage fraud.

Measuring and proving the value and overall effectiveness of fraud prevention is therefore fundamental to assuring senior leaders, the Parliament and the wider public that public money is being used effectively.

Business drivers

There are two distinct business drivers for why Savings Measurement might be undertaken, which inform the purpose and goals of the exercise, and the approach that should be taken.

Business Drivers

Prospective forecasting

Prospective forecasting is the process of using available information to predict future outcomes. This type of exercise would generally be undertaken to approximate the savings that can be achieved from a proposed intervention, in support of a business case or policy proposal.

Retrospective measurement

Retrospective measurement involves collecting data about events that have already occurred, looking back in time to examine past outcomes. This type of exercise would generally be undertaken to measure the savings achieved by an existing intervention, showing the value delivered.

Retrospective measurement can also be used to later confirm predictions that were made as part of prospective forecasting.

The reasons why Savings Measurement is undertaken may vary over time, for example, an organisation may initially plan to perform prospective forecasting to support a business case, and later, when suitable opportunities arise, evolve into retrospective measurement and become an ongoing evaluation and assurance program. The methods may remain the same (simply adjusting for new data), or the approach may evolve considering added information as it progresses from prospective to retrospective and the analysis matures.

Retrospective measurement in a UK government grant scheme

A UK Government grant scheme was reporting minimal fraud and error levels in its first year of operation compared to similar grant schemes.

In the second year a range of prevention and detection controls were initiated and included:

- Verifying eligibility criteria such as being in receipt of qualifying welfare support
- Data matching against previous awards and other schemes for duplicate claims
- Enforcing price limits on suppliers
- Verifying identity
- Verifying installations
- Verifying property ownership.

The retrospective detection rate from these new interventions showed that there was a baseline fraud and error level of 55% within the scheme before implementation. After a year of operation, the fraud and error level had fallen to 2% and delivered a cash savings across prevented and detected fraud and error of £422m.

Why do we talk about fraud and error in Savings Measurement?

Concluding whether a particular transaction is fraud, rather than error or non-compliance, often requires more information than can reasonably be obtained in a broad measurement exercise. Additionally, the business actions taken to address fraud and error are typically the same: the aim is to fix the process to reduce the risk exposure and losses to the taxpayer. Therefore, compliance activities are also included when measuring fraud prevention savings.

Outline of key features

This Framework sets out three key features that an organisation should apply when developing an approach for estimating and quantifying fraud prevention savings. These are summarised below and explored in more detail in the following chapters.

1

Preliminary activities

This involves scoping and collecting the initial data/evidence that will:

- define the parameters of the program, activity or function the Savings Measurement relates to
- find and assess the types and causes of fraud and error
- find any pre-existing controls, post-award checks and control weaknesses
- define the baseline rate of fraud and error from which the impact of the intervention can be assessed
- identify possible interventions to reduce the causes of fraud and error.

2

Methods to estimate and quantify savings

This is the overall method to measure savings, which includes three key steps:

1. **Developing a counterfactual**, which involves:
    - predicting fraud or error losses over a defined period where hypothetically the intervention does not or had not taken place
2. **Estimating the expected effect of the intervention on fraud and error levels**, which involves:
    - explaining the impact of an identified risk on fraud and error level
    - outlining and explaining the impact of the intervention
3. **Quantifying approximate savings**, which involves:
    - outlining and explaining the savings period
    - deciding how and when to quantify the changes
    - calculating the return on investment.

3

Governance, approval, assurance and review

This involves setting up governance arrangements to independently review and approve savings methods, providing a level of assurance that approaches are robust and consistent.

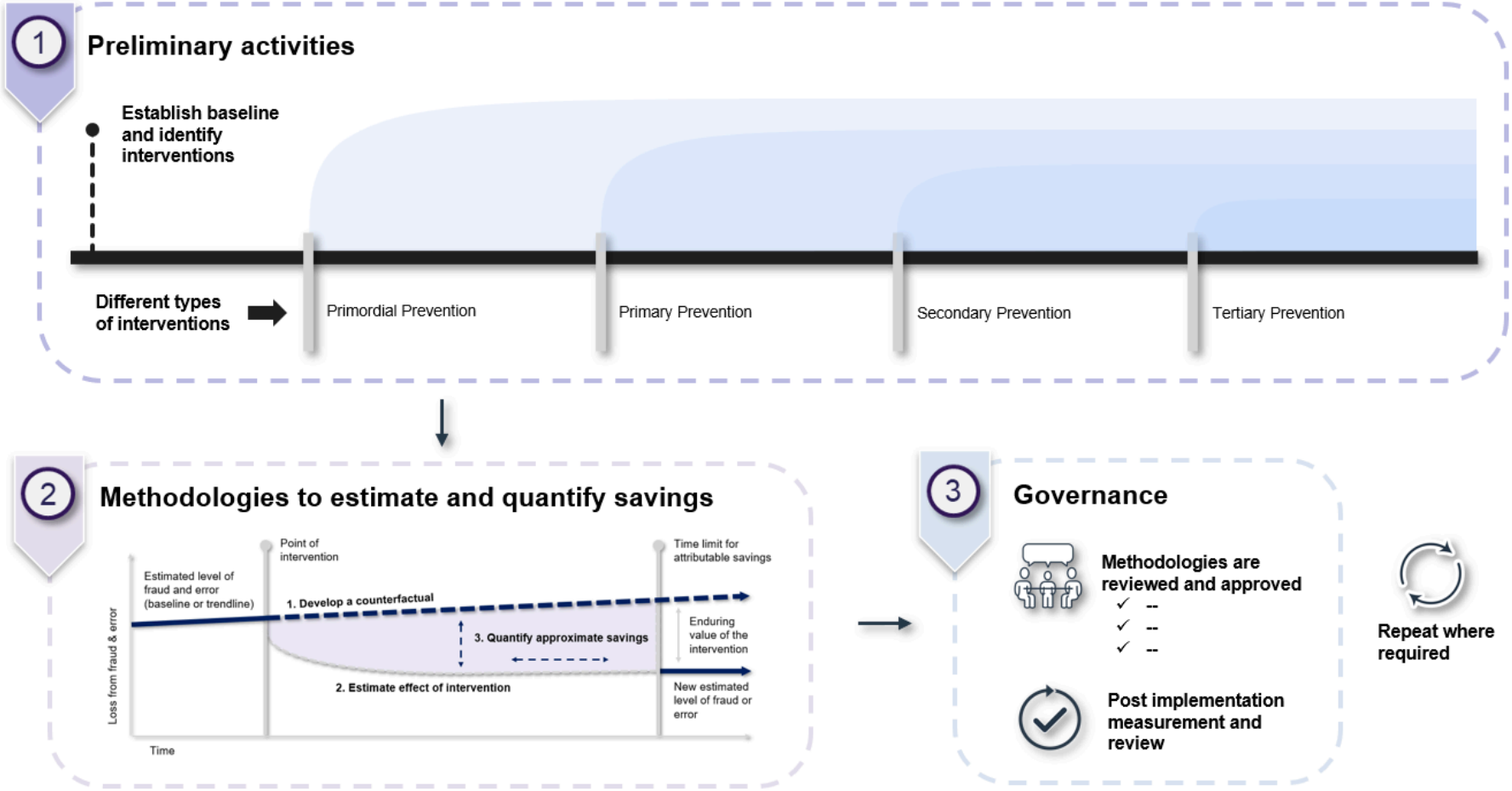
Post-implementation activities should also be reported back through the same governance process. This may include:

- evaluating the effectiveness of the intervention
- testing the assumptions made as part of the method
- figuring out the actual savings delivered by the intervention
- figuring out the enduring value of the intervention.

Organisations may continually repeat the cycle to build on earlier interventions and show further savings.

Figure 1 visually represents how these features interact in a linear or cyclical way, from the preliminary activities helping to establish a baseline of fraud and error and identify causes and interventions, developing a method to measure prevention savings, having the method reviewed and approved through established governance arrangements, and undertaking post implementation measurement or review, repeating the process where required.

Figure 1 - Key features of Fraud Prevention Savings Measurement



1

Preliminary activities

It is important to undertake preliminary activities as a first step of any Savings Measurement activity.
Preliminary activities help:

- define the scope and parameters of the program, activity or function the Savings Measurement applies to
- informing the total amount of payments or revenue at risk of fraud and error
- find the types and causes of fraud or error within the program, activity or function
- find any pre-existing controls and control weaknesses
- define the baseline rate of fraud and error or other metric to use as a benchmark for measuring savings, and
- identify the interventions needed to reduce the causes of fraud and error.

Preliminary activities are critical to establishing the benchmark for measuring the effect of any type of intervention.

Undertaking these preliminary activities in a robust way relies on other fraud control capabilities including fraud risk assessment, fraud control testing, data sharing, data analytics, fraud prevention and detection activities, and fraud measurement. The fundamentals of these capabilities are covered in other standards, frameworks and guidance, such as the IPSFF Fraud Control Testing Framework and IPSFF Fraud Loss Measurement Framework. Building organisational maturity in these areas is critical for developing a detailed and credible understanding of the existing fraud risks and the baseline rate of fraud and error.

Distinct types of preliminary activities

There are distinct types of preliminary activities that can be undertaken. Which preliminary activity is used will depend on a range of factors and will determine the type of baseline used for Savings Measurement.

Type of preliminary activity	Type of baseline this can establish
A. Reviewing comparable programs, activities or functions	This can provide data/modelling to inform the potential level of fraud and error in a new program, activity or function.
B. Collecting and analysing relevant data	This can inform the known amount of fraud or error, or the total amount of payments or revenue at risk of fraud and error, in a new or existing program, activity or function.

	**C.** Conducting a fraud risk assessment (FRA) or control testing exercise	This can inform the level of residual fraud and error risk in a new or existing program, activity or function.
	**D.** Undertaking a fraud loss measurement (FLM) exercise.	This can provide an accurate estimate of the levels of fraud and error in an existing program, activity or function.

A. Reviewing comparable programs, activities, functions or interventions

Reviewing comparable programs, activities, functions or interventions can help with measuring fraud prevention savings by:

- providing insights on the potential types and causes of fraud and error in a new program, function or activity
- providing data/modelling to inform the potential level of fraud and error in a new program, activity or function., which can be used as the baseline
- informing targeted and measurable interventions based on known causes of fraud and error, as well as effective controls, in other programs, activities or functions.

Organisations can review the types of fraud and error affecting comparable programs, functions and activities. Comparable programs may include programs with similar characteristics, including their objectives, operational processes, target population, transaction scale and volume, or technology and systems.

This can be particularly useful when designing new programs, functions, activities or interventions where no existing data is available. Fraud management information, such as historical detection rates (frequency), the average lifetime of the fraud (duration) and the average cost (impact) can provide insights on the type and extent to which fraud and error may affect a new or existing program, function or activity. Organisations can also study the lessons learnt in earlier case studies to be better informed on interventions to implement, and the potential impact of the intervention.

Using data indicators/modelling, comparative studies and/or fraud management information enables organisations to develop broad estimates of potential fraud and error loss for the new program, function or activity to figure out the baseline rate of fraud and error. For further information on using comparative studies to estimate potential levels of fraud and error losses, see Developing a counterfactual below.

Care should be taken to assure the accuracy of data and information being drawn from and to consider any limitations with this approach. Consulting staff from other public bodies or central counter fraud functions can help with figuring out if another program, function, activity or intervention can be reliably used as a standard for comparison.

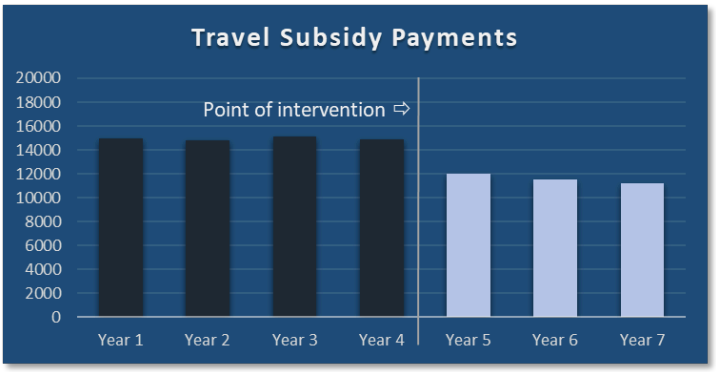
B. Collecting and analysing relevant data

Collecting and analysing relevant data relating to the specific program, activity or function can help with measuring fraud prevention savings by:

- finding known types and causes of fraud or error relating to the program, activity or function
- informing the known amount of fraud or error, or the total amount of payments or revenue at risk of fraud and error, in a new or existing program, activity or function, which can be used as the baseline
- informing targeted and measurable interventions based on known causes of fraud and error relating to a program, activity or function.

Organisations can collect and analyse information and data to develop a simple baseline, such as the total amount of payments made or revenue collected from a target population or the known amount of detected and investigated fraud and non-compliance in a program, function or activity. Predictive analytics could also be a useful tool in analysing the likelihood of fraud or error occurring based on the historical data.

This is a common approach used to measure deterrence, e.g. by comparing an estimate of what the overall spending would have been in the absence of an enforcement action (i.e., pre-period) to actual spending following an enforcement action (i.e., post-period).[3] However, it can be used to measure a range of interventions. For example, an organisation could use historical data on a travel subsidy scheme as a simple baseline for measuring the effect of the new verification requirements.



If the level/value of travel subsidies reduces and no other changes (except the added verification) occur at the same time, it is reasonable to conclude that the reduction in claims is a result of the new intervention.

While not as robust as a fraud risk assessment or fraud loss measurement exercise, using a simple baseline based on scheme or program data is time efficient and provides sufficient evidence for Savings Measurement when limited to a specific area of spend or revenue.

C. Conducting a fraud risk assessment or control testing exercise

Conducting fraud risk assessments (FRA) and control testing exercises can help with measuring fraud prevention savings by:

- finding known and new types and causes of fraud or error relating to a program, activity or function
- informing the level of residual fraud and error risk in a new or existing program, activity or function, which can be used as the baseline

[3] Measuring the value of healthcare anti-fraud efforts. Healthcare Fraud Prevention Partnership. 2024. HFPP Measuring Value White Paper

- informing targeted and measurable interventions to address the types and causes of fraud or error found.

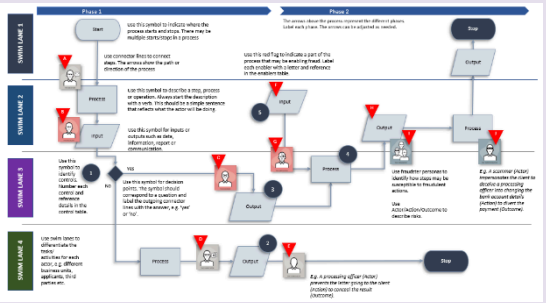
FRAs allow an organisation to effectively and comprehensively identify, describe and assess individual fraud risks. They also help assess and measure residual risks[4] (i.e. the level of risk that remains after applying the fraud and error controls)[5], by assessing the likelihood and frequency of the fraud occurring, its duration and materiality of its impact.[6]

Control testing involves employing different testing methods to examine how controls work, eliminate blind spots, uncover vulnerabilities and challenge assumptions about how fraud is managed by public bodies. The results of control testing offer further business insights to more accurately assess and measure residual risks.[7]

Risks found and prioritised by either of these processes may then lead to more or improved interventions that look to reduce future losses. These can also provide the baseline fraud and error rate from an informed assessment of the likelihood and consequences of the identified risks.

Tips for conducting FRAs and control testing

Fraud risks found in an FRA should be communicated in a way a non-expert can understand, and include detail on who could commit the fraud, how the fraud could take place, and the consequences (i.e. actor, action, outcome).



Business process mapping can be used to visualise the process of the relevant program, function or activity, show processes that may be vulnerable to fraud, and inform interventions that could deliver savings.

Guidance on FRAs and control testing can be found in Fraud Risk Assessment Standards (2022-03-25) and International Public Sector Fraud Forum - Fraud Control Testing Framework FCTF-01.

D. Undertaking fraud loss measurement activities

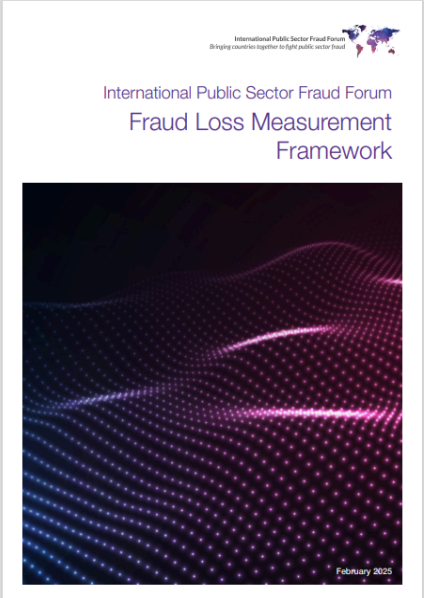
Fraud loss measurement exercises can help with measuring fraud prevention savings by:

- finding known and new types and causes of fraud or error relating to a program, activity or function
- providing provide an accurate estimate of the levels of fraud and error in an existing program, activity or function, which can be used as the baseline

[4] GCF Professional Standards and Guidance: Fraud Risk Assessment, pp.33-34. www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government
[5] GCF Professional Standards and Guidance: Fraud Risk Assessment, p. 68
[6] GCF Professional Standards and Guidance: Fraud Risk Assessment, p. 58
[7] Fraud Control Testing Framework, p. 34. International Public Sector Fraud Forum. www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance

- informing targeted and measurable interventions to address the types and causes of fraud or error found.

Fraud loss measurement (FLM) offers the most robust method for establishing baselines. FLM exercises test and find non-compliant, fraudulent or irregular transactions against external data, within a sample that is statistically valid and significant. This also offers more insights on why fraud and error are occurring within a program, function or activity.



This knowledge allows organisations to:

- estimate the actual rate of fraud and error
- develop more informed and targeted interventions to tackle previously hidden fraud and error, and
- more accurately measure the effects of an intervention.

The IPSFF Fraud Loss Measurement Framework sets out key principles and processes for conducting Fraud Loss Measurement (FLM) exercises within public sector organisations.

Deciding what preliminary activities are needed

The overall goal of the preliminary activities is to establish a benchmark for measuring the effect of any type of intervention as well as inform what targeted interventions are needed to reduce fraud and error. Which combination of preliminary activities you undertake will depend on a range of factors, including the complexity of the relevant program, function or activity, nature of the fraud risks found, type and characteristics of the intervention being measured, and availability of data and resources.

For example, it may be possible to use a simple baseline as a benchmark, such as the current spend, income or service levels across an entire population. Additionally, measuring the effect of compliance or enforcement activities may only require a simple analysis of detected/investigated fraud or non-compliance and recovery rates.

Other circumstances may require a fraud risk assessment (to understand the residual risk) and ideally a fraud loss measurement exercise (although not always viable). While fraud loss measurement exercises provide the most robust baseline of fraud and error losses, they are often costly and time consuming. Their use would most likely allow an organisation to show the full extent, or collative impact, of new interventions across an entire service or spend area. In comparison, fraud risk assessments can be completed with less resources and still provide an informed understanding of the types and causes of fraud or error and a reliable approximation of baseline levels of fraud or error.

While availability of resources may also be a factor, it should not deter organisations from undertaking preliminary activities or measuring fraud prevention savings. Instead, organisations can conduct Savings Measurement on a smaller scale or use less costly methods (e.g. estimating baseline levels of fraud and error using data from comparable

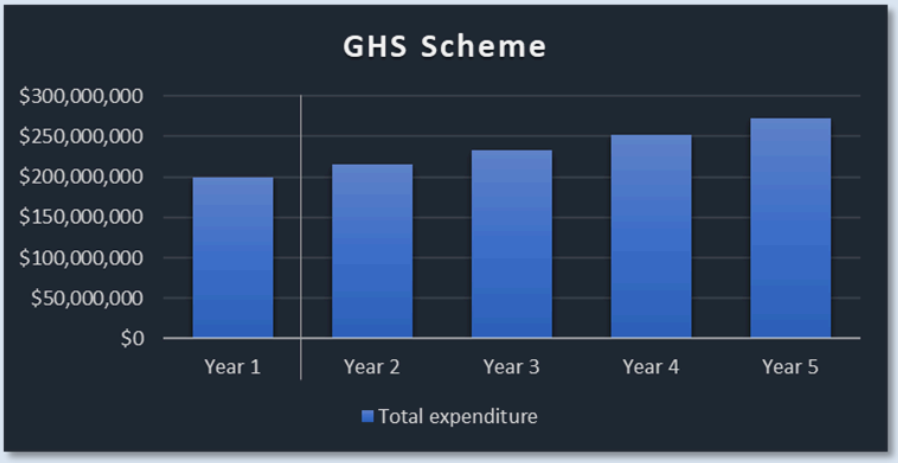
programs, functions and activities). Being able to prove savings can support an investment case for more resources on fraud prevention and the wider capability of the organisation.

It is important to acknowledge the limitations in any approach taken and how this affects the type of baseline, the level of confidence in its accuracy, and the understanding of specific causes of fraud and error. Organisations are also encouraged to conduct multiple preliminary activities to support Savings Measurement.

Case Study – Green Homes Subsidy Scheme

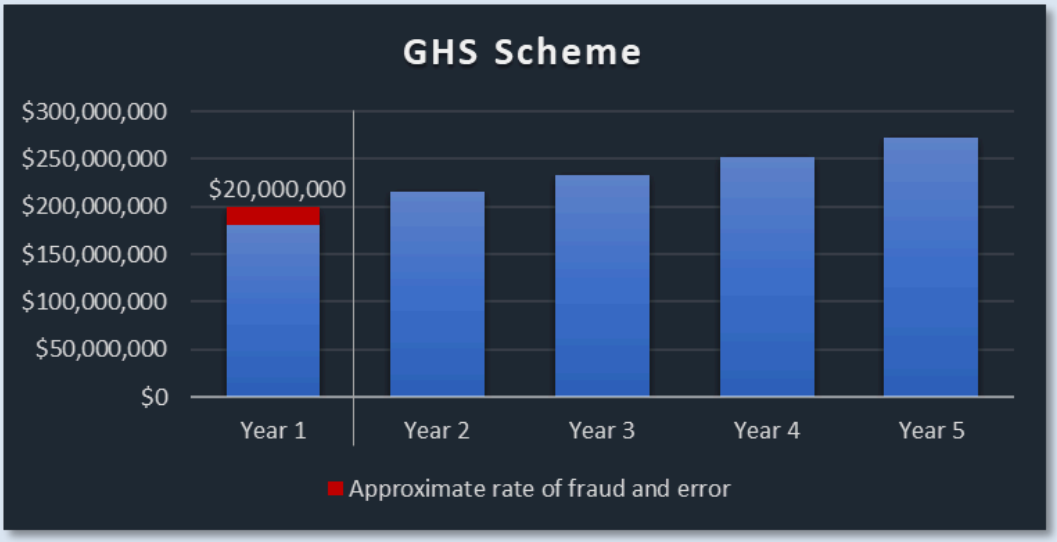
Scheme overview

The government has implemented a Green Homes Subsidy Scheme (GHS Scheme) that will run for 5 years, where the uptake of the scheme is increasing by 8% each year ($200m, $216m, $233m, $252m, $272m). The scheme has already been in place for one year.



Preliminary activities and baseline

At the end of the first year of the GHS Scheme, a fraud risk assessment was undertaken. Combined with other compliance and fraud detection data analysis, this found that in the first year the approximate rate of fraud and error in the scheme was 10% ($20.0m).



Checkpoint

Now you have completed the preliminary activities, you will have:

- defined the parameters of the program, activity or function the Savings Measurement relates to
- found and assessed the types and causes of fraud and error
- found pre-existing controls, post-award checks and control weaknesses
- defined the baseline rate of fraud and error or other metric to use as a benchmark for measuring savings.

Identifying interventions to reduce fraud and error

Undertaking preliminary activities will help identify targeted and measurable interventions to address the types and causes of fraud or error found. Interventions could be any activity undertaken with the aim of reducing the likelihood (probability and frequency) or consequence (duration and impact) of fraud and error in a program, activity or function.

Distinct types of measurable interventions can be developed based on the preliminary activities.

For savings measurement, we use the following four categories of prevention:

Different forms of prevention

Primordial Prevention – designing an optimal control environment before implementing a new program, activity or function, preventing losses to fraud and error from the outset

Primary Prevention – controls that reduce the likelihood of fraud or error occurring, preventing immediate loss

Secondary Prevention – detection mechanisms that find fraud and error early, preventing future loss

Tertiary Prevention – recoveries made from responding to fraud that has been committed, preventing permanent loss

Figure 2 provides examples of activities involved in each type of intervention, ranging from assessing risks and designing an optimal control environment during program design, through to investigations and recovering losses.

Figure 2 - activities involved in each type of intervention

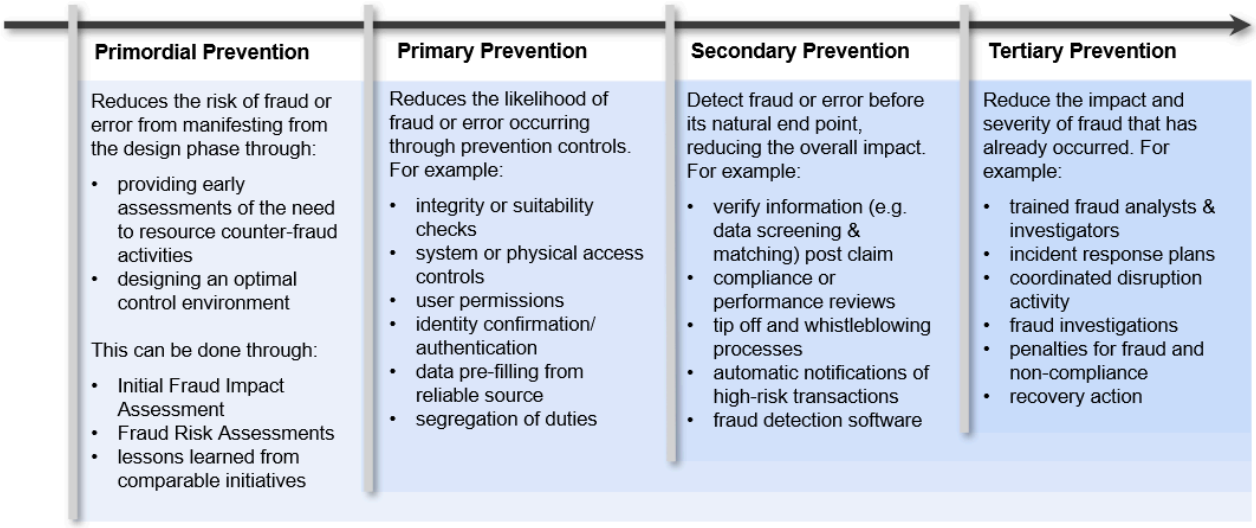
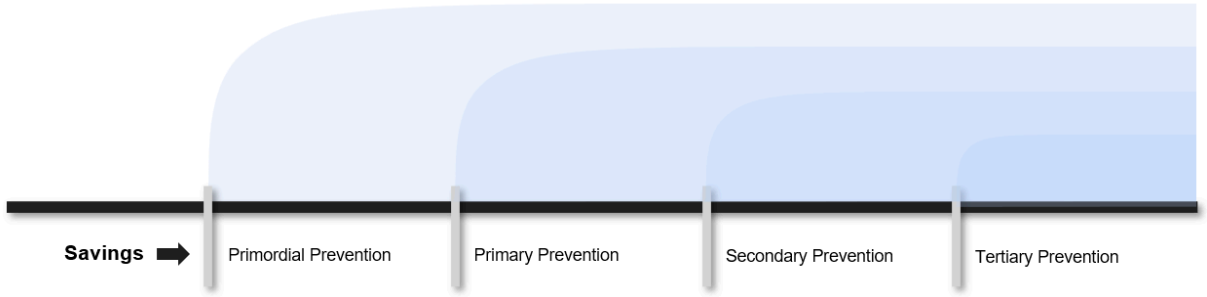


Figure 3 illustrates how these types of interventions work together to provide defence-in-depth through layers of control, delivering distinct types of savings and benefits by reducing the probability, frequency, duration and impacts of fraud and error.[8]

Figure 3 – Different types of interventions that can be developed from the preliminary activities



These interventions may also show the need for further interventions, creating a measurable cycle of improvement. For example, detection and investigations (Secondary and Tertiary Prevention) can find the causes of fraud and error, which inform what added controls can help reduce the ongoing likelihood of fraud or error occurring (Primary Prevention). Lessons learned can then inform how to design effective control environments, helping to prevent losses to fraud and error from the outset when implementing new programs, activities or functions (Primordial Prevention).

Case Study – Green Homes Subsidy Scheme

The preliminary activities have identified the following interventions aimed at reducing losses from fraud and error in the GHS Scheme:

- **Intervention 1: Digital claiming process**

[8]Controlling Fraud and Corruption Risk – Leading Practice Guide. Commonwealth Fraud Prevention Centre. www.counterfraud.gov.au/library/controlling-fraud-and-corruption-risk-leading-practice-guide

    - Intervention 1 is an investment into a new digital claiming process with more rigorous identity authentication for installers, mandatory fields, including product codes, and a need to upload geotagged images of completed installations (primary prevention).

- **Intervention 2: Compliance actions**
    - Intervention 2 is an investment into more compliance resources to recover funds paid due to error or fraud (tertiary prevention).

Checkpoint

Now that you have identified interventions, you are ready to develop a method for estimating or measuring financial savings as well as other indirect and non-financial benefits.

2 Methods to estimate and quantify financial savings

A method is the overall method by which expected or actual savings are figured out – this may include financial calculations as well as evidence of other non-financial benefits.

Methods for figuring out prevention savings include three common aspects.

To measure or estimate any financial savings in a robust and reliable manner, and to extrapolate any resultant ROI calculations, all savings calculations feature three common aspects.

Three aspects to a prevention savings method

1. Developing a counterfactual

This involves predicting fraud or error losses over a defined period if the intervention does not take place (predictive forecasting) or has not taken place (retrospective measurement). This is projecting 'what would have been,' usually derived from a baseline developed through the preliminary activities.

2. Estimating the effect of the intervention

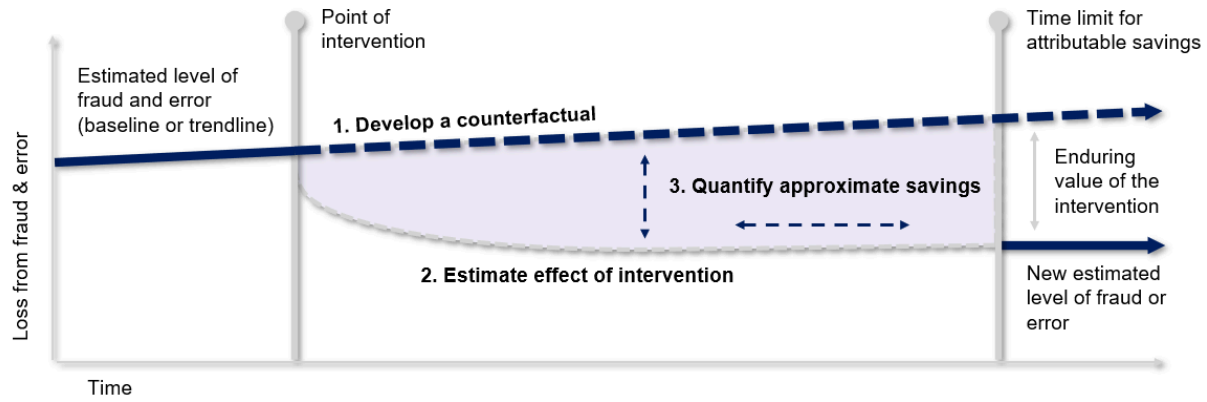
This is an informed and evidence-based assumption of how the intervention will reduce fraud and error levels (or has reduced fraud and error levels) or other direct or indirect harms in comparison to the counterfactual.

3. Quantifying approximate savings

This involves calculating the amount expected to be saved based on the difference between the predicted reduced rate of fraud and error and the counterfactual over a defined period. These will later be validated and communicated as part of governance arrangements (see Communicating prevention savings below).

Figure 4 is a diagram showing how these key features come together as part of a method for Savings Measurement. The counterfactual is used both to estimate the effect of the intervention (by comparing what would have happened if no intervention occurred) and to quantify the approximate savings (by comparing the effect of the intervention to the counterfactual).

Figure 4 - Key features of a prevention savings measurement method

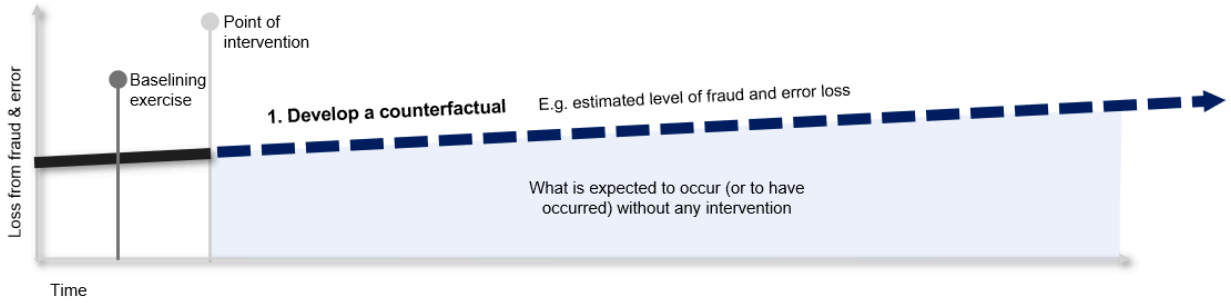


The following sections discuss these 3 key features in more detail, with practical advice and examples on how to apply them.

1. Developing a counterfactual

Developing a counterfactual involves a prediction of fraud or error losses over a defined period if the intervention does not take place (predictive forecasting) or has not taken place (retrospective measurement). See ***Figure 5*** for an illustration.

Figure 5 – Developing a counterfactual



Counterfactuals are key to savings measurement and will usually be drawn from evidence or data gathered through the preliminary activities (e.g. known levels/rates of fraud or error in a specific program, activity or function or another key metric). A counterfactual looks to show 'what would have been' had the change not occurred. For example, in the pharmaceutical sector, counterfactuals are used to measure the impact of a new treatment by comparing treatment outcomes against what would likely have occurred had the treatment not been administered (the counterfactual scenario).

The counterfactual is also the benchmark for measurement as it defines the specific metric you are trying to affect through the interventions. For example, an actual monetary loss forecasted into the future (e.g. $6.3 million in detected fraud and error per annum), or a fraud or error rate applied against future transaction values (e.g. $120m in subsidies over the next 12 months x 4.8% loss rate).

There are different methods for developing counterfactuals, including experimental methods (i.e. using a control group or sample), quasi-experimental methods, and non-experimental methods.[9] Table 2 outlines the most relevant methods for Savings Measurement.

Table 2 - Relevant methods for developing a counterfactual

Non-experimental methods		**Key informant** – This involves asking experts to predict what would happen (prospective forecasting) or would have happened (retrospective measurement) in the absence of the intervention.
		**Logically constructed** – This involves using a baseline as an estimate of the counterfactual where it is reasonable to assume this would remain the same without the intervention or correcting for other variables.

[9] www.betterevaluation.org/frameworks-guides/rainbow-framework/understand-causes/compare-results-counterfactual

Quasi-experimental methods		**Difference-in-difference** – This assesses the impact of the intervention between two separate groups which do not need to be randomly assigned.
		**Statistically created** – A statistical model, such as regression analysis, is used to develop an estimate of what would happen or would have happened in the absence of an intervention.

For an existing program, activity or function, the baseline of historical/current fraud and error loss can be used to forecast the level/rate of fraud and error as if it would continue unaltered into the future ('logically constructed' counterfactual), provided this baseline can be confidently estimated or measured. In particular:

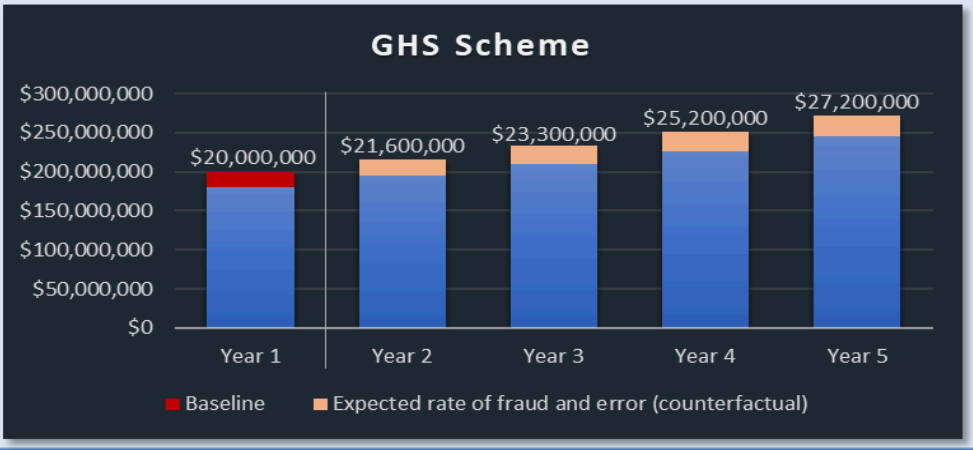
- the results of fraud loss measurement exercises can be used to estimate the rate of fraud and error in the program, activity or function
- the results of fraud risk assessments and control testing can be used to estimate expected losses from residual risk, i.e. the likelihood (probability and frequency) and consequence (duration and impact) of fraud and error in the program, activity or function
- known levels/rates of detected fraud in the program, activity or function, including frequency (e.g. percentage of claims or transactions), duration (current average time to detect and respond) and impact (current average losses), can also be used as metrics.

In the case of a new program, activity or function, there is unlikely a level/rate of fraud and error loss to develop a baseline or counterfactual. These circumstances may require the use of fraud or error levels/rates in a comparable program, activity or function with an evaluation of the characteristics and interventions in the new program, activity or function to predict the level/rate of fraud and error we can expect. In this circumstance, the 'Key Informant' and 'Logically Constructed" counterfactual both play a role. When there is no comparable program, the insights of 'key informants' drawing on common themes of effective fraud control becomes even more important.

Case Study – Green Homes Subsidy Scheme

The baseline rate of fraud and error in the GHS Scheme's first year of operation (10%) is used to develop a counterfactual into the future (logically constructed counterfactual), with the expected rate over the remaining 4 years to be:

- $21.6m in year 2
- $23.3m in year 3
- $25.2m in year 4
- $27.2m in year 5



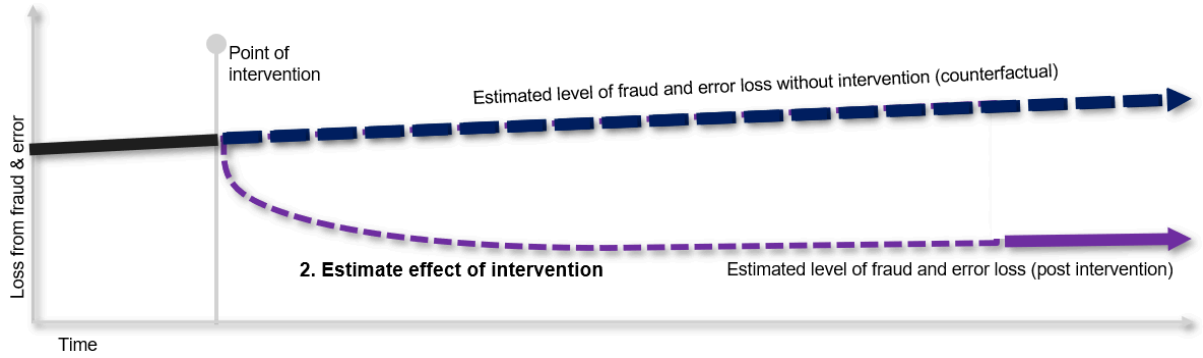
Checkpoint

Now you have developed the counterfactual, you will have a benchmark for measuring and quantifying the effect of your interventions.

2. Estimating the effect of the intervention

Estimating the effect of the intervention involves making informed and evidence-based assumptions about how it will reduce losses to fraud and error (or has reduced losses) in comparison to the counterfactual. See Figure 6 for an illustration.

Figure 6 - Estimating the effect of the intervention



These informed and evidence-based assumptions can be derived from answering two key questions:

- What are the causes that influence the metric you are trying to affect?
- How will the intervention/s impact the causes?

What are the causes that influence the metric you are trying to affect?

Multiple factors and causes contribute to the fraud and error loss in a program, function or activity, which could be individually and specifically found in preliminary activities. To ensure accuracy of the measurement, separate savings methods should be developed for each cause of fraud and error. In other words, if there are multiple identifiable factors leading to fraud and error loss, organisations will need to attribute a specific weighting and value to each cause that will be affected by the intervention/s. Data analysis, such as multinomial analysis, could also be used for a more sophisticated assessment to analyse the relationship between the metric and one or more independent variables (e.g. causes or attributes).

For example, you might find a specific percentage (e.g. 40%) of the fraud and error loss rate in the program, activity or function is caused by a single factor or vulnerability. This value will often depend on expert judgment, supported by evidence, or, if enough data is available, the value could be based on data analysis.

Case Study – Green Homes Subsidy Scheme

The preliminary activities have found that approximately 80% of the fraud and error in the scheme is caused by the manual form submitted by installers, which regularly includes claims for ineligible products (error), and in some circumstances, fabricated claims (fraud).

How will the intervention/s impact the causes?

To estimate the effect of an intervention, first figure out if the intervention will likely impact (prospective forecasting) or has impacted (retrospective measurement) the specific causes that lead to fraud and error in the program, activity or function. For example, a new intervention that prevents a particular type of fraud (e.g. identity misuse) might have minimal or no effect on other types of fraud in the program, activity or function (e.g. duplicate claiming).

This also involves making informed assumptions about the extent the interventions will reduce the causes of fraud and error within the program, function or activity. These assumptions will depend on the specific nature of the causes, as well as the timeliness and effectiveness of the interventions. Like developing a counterfactual, these assumptions will also often rely on the judgement of experts.

To make informed assumptions, experts may draw from available data on quantified savings and impacts of common counter-fraud interventions or evaluations/audits of similar or historic systems where those interventions did not exist to further support the predictions of the impact of the interventions. You should also consider the relevance and coverage of the intervention, the time it takes for the intervention to respond, the adaptability of the intervention etc. It may also be possible for the effectiveness of interventions to increase or decrease over time.

For further guidance on how to determine the effectiveness of an intervention, see pages ***31-33 of the IPSFF Fraud Control Testing Framework***.

Case Study – Green Homes Subsidy Scheme

Expected impact of Intervention 1
Intervention 1 (the digital claiming process) targets incorrect manual forms, which is the cause of 80% of fraud and error in the GHS Scheme. However, the intervention is only expected to be 90% effective at addressing this cause as residual vulnerabilities will exist in the process.

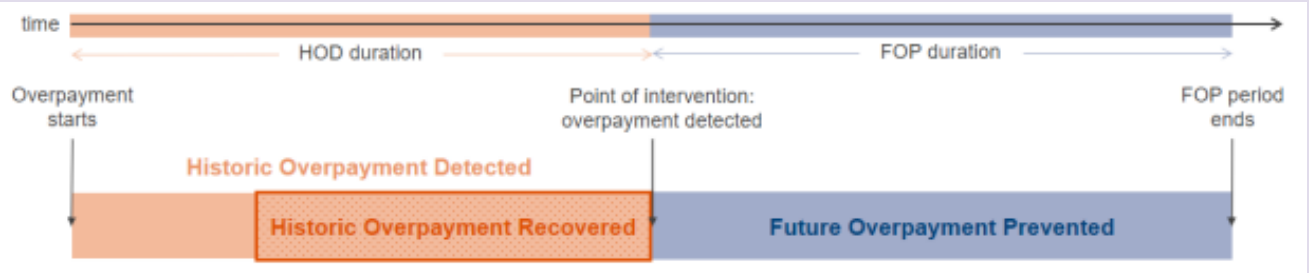
Expected impact of Intervention 2
Intervention 2 (the compliance actions) will apply to all debts raised under the scheme. However, it is only expected to be 50% effective in recovering funds paid due to error or fraud, as some installers will be expected to go out of business and some fraudulent payments will be difficult to recover.

UK Department of Work and Pensions (DWP) Case Study

The DWP has a well-established method for estimating the future impact on expenditure from their counter-fraud activities. This includes detection and recovery of all historic overpayments (HODs), and savings associated with the prevention of the future duration of that overpayment. As part of any fraud and error decision-making activity, they seek to confirm any overpayment to be recovered, and if so send them for recovery action.

They also figure out whether that overpayment would have continued had DWP not identified and intervened, by calculating the weekly or monthly 'Monetary Value of Adjustment' (MVA) (i.e. value of the change to entitlement) and apply an assumed duration depending on the benefit in error (i.e. future loss prevented).

These averages have been worked out based on the hundreds of thousands of real-world overpayments that provide robust evidence, from which they estimate average claims lengths, and resulting losses from fraud and error, had interventions not occurred.



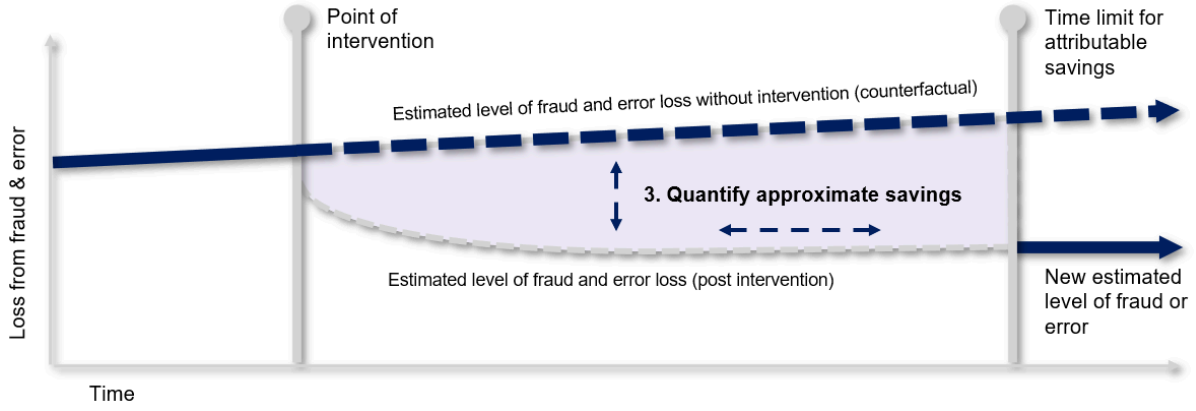
Checkpoint

Now you have approximated the impact of the causes of fraud and error, as well as estimated the effect the intervention/s will have on these causes, you are now able to identify and quantify the savings and other benefits from the intervention/s.

3. Quantifying approximate savings

Quantifying approximate savings from an intervention involves calculating the amount expected to be saved based on the difference between the counterfactual and the predicted reduced rate of fraud and error over a defined period of time. See ***Figure 7*** for an illustration. This can also involve approximating other types of savings, such as administrative costs avoided (see what savings are expected or achieved by the intervention below).

Figure 7 - Quantifying approximate savings



In addition to the counterfactual (to benchmark for calculating savings) and estimating effect of the intervention (to approximate the deviation from the counterfactual), key aspects of quantifying prevention savings include determining:

- What is the quantifiable period?
- What savings are expected or achieved by the intervention?
- What is the return on investment?

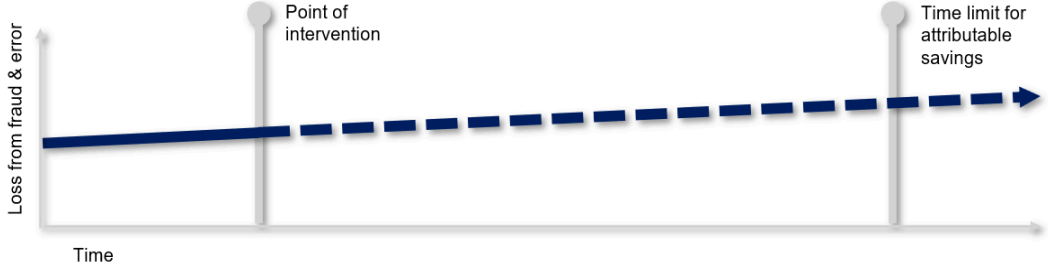
All methods of quantifying approximate savings should be reasonable, logical and clearly linked to the intervention. They should be evidence-based and, where possible, data-driven, either directly or from other comparable areas. See Appendix C for more information on data governance.

What is the quantifiable period?

The quantifiable period (or 'savings period') is the duration of time that savings can be attributed. This is generally defined by:

a. the point at which you start to realise savings, and
b. the time limit for attributing savings – ***see Figure 8***.

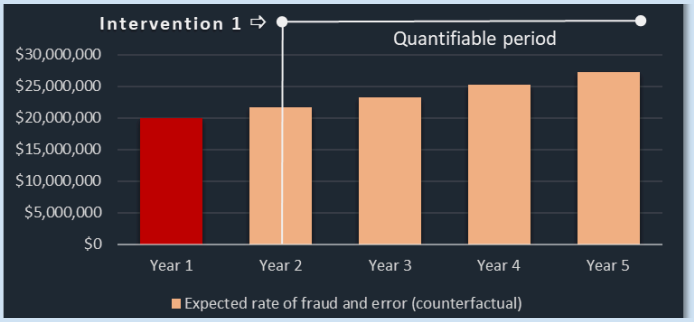
Figure 8 - duration of time that savings can be attributed



A method for Savings Measurement must specify the starting point of an intervention and evidence this. For example, the date a new prevention intervention was implemented or the point in which a payment or service was stopped due to fraud or error being detected.

The boundaries, limits, or other parameters of the program, activity or function, e.g. entitlement periods, may play a role in determining the end of the quantifiable period. For example, a grants program may have pre-defined boundaries or limits (e.g. program end date) which would determine the quantifiable period. See illustrations at Figures 12 and 13 below.

Case Study – Green Homes Subsidy Scheme



As it will take six months to design and implement Intervention 1 (the digital claiming process), the point of intervention will be halfway through year 2 of the GHS Scheme. Therefore, the quantifiable period for Intervention 1 is the 3.5 years from the expected date of implementation to the end of the scheme (end of year 5).

Although Intervention 2 (compliance actions) will take three months to ramp up, its effect will be retrospective (it will apply to all debts raised under the GHS Scheme). Therefore, the quantifiable period for Intervention 2 is the entire life of the scheme (5 years).

What types of savings are expected or achieved by the intervention?

Approximating the financial value of the intervention involves calculating the difference between the counterfactual and the estimated effect over the quantifiable period.

The boundaries, limits, or other parameters of the program, activity or function (e.g. payment caps) are all relevant to determining the types of savings that can be attributed and quantified. ***Figure 11*** below provides examples of the types of savings that may be attributed to each type of intervention. These savings can include both reduced losses and collateral costs avoided (e.g. less reliance on costly and inefficient debt recovery).

The types of savings achieved broadly fall into two categories:

1. Reduced losses from fraud and error; and
2. Collateral costs avoided.

Reduced losses from fraud and error

Once the types of savings and the quantifiable period have been determined, the next step is to assign a monetary value to the effect of the intervention (the deviation from the counterfactual). Reduced losses may be the summation of:

Primary Loss Prevented - stopping the immediate and direct loss stemming from fraud or error (primordial and primary prevention)

Future Loss Prevented - stopping further losses though early intervention (secondary prevention)

Permanent Loss Prevented - recovering losses that have already occurred (tertiary prevention)

Collateral costs avoided

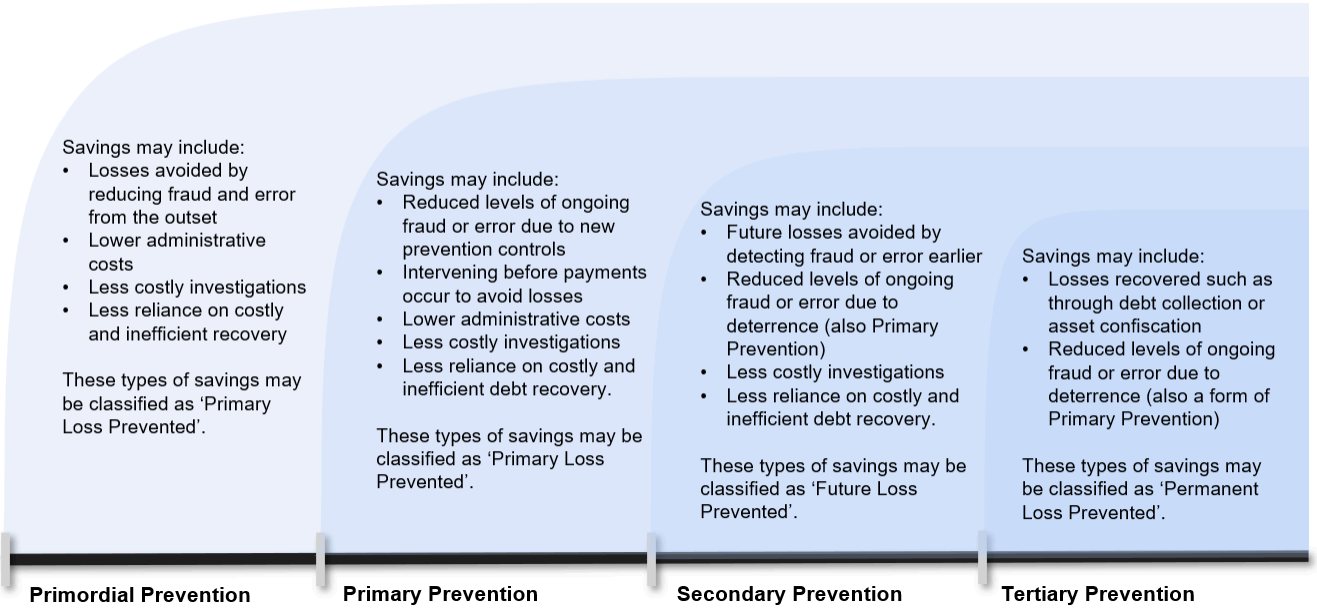
Calculating the effect of the intervention may include a reduction in collateral costs, such as:

- reduced costs to administer the relevant program, activity or function (e.g. through more streamlined or automated checks and controls)
- avoiding costs involved in compliance and investigations, or to pursue post-payment recovery actions.

Attributing savings to different types of interventions

The earlier the point of intervention, the more types of savings can be attributed to that intervention - ***see Figure 9***. This is because earlier interventions, such as primordial prevention, also reduces the costs involved in later interventions (e.g. costs of investigations and recovery action). Correspondingly, later interventions, such as tertiary prevention, only yield limited types of savings. It is therefore key to understand the stage of the intervention as part of the overall assessment of the likely savings that can be realised.

Figure 9 – Types of savings delivered by different types of interventions



Where there are multiple interventions being implemented, it is important to estimate the collective effect of all interventions. This is because, in practice, controls do not operate in isolation, and their impact may 'offset' each other. For example, where 20% fraud has been

prevented by a primary intervention, a tertiary intervention that would have recovered 20% fraud loss on its own would only recover 16% of fraud losses (compared to the counterfactual). In another example, implementing one primary intervention may have a 10% effect. However, similar to the economic principle of diminishing return, implementing two primary interventions may only have 15% effect.

One method organisations may employ is to estimate the impact of interventions in a sequential order, beginning with primary interventions first, and then using the residual risk of fraud and error to develop an adjusted counterfactual to continue estimating the impact of secondary interventions, followed by tertiary interventions. This method can however lead to other issues, such as a decreasing reliability in estimation in the later stages of interventions. Validation exercises can help confirm or adjust predictions as interventions are implemented. Ultimately, the most suitable method of estimation will depend on the specific circumstances.

Factors to consider when calculating primordial and primary prevention

Calculating the value of primary loss prevented by reducing fraud and error from the outset (primordial prevention) or reducing levels of ongoing fraud or error due to new prevention interventions (primary prevention) may need to consider:

- the number of beneficiaries,
- the average transaction value,
- the proportion of the average transaction value saved through reduced fraud and error,
- the average length of entitlement, and
- other relevant factors.

Factors to consider when calculating secondary prevention

Calculating the value of future loss prevented by detecting fraud or error earlier and reducing time to action (secondary prevention) may need to consider:

- the number of beneficiaries (e.g. detecting and stopping a high-value fraud relating to a single beneficiary or detecting and stopping low-value error relating to multiple beneficiaries),
- the transaction values,
- the proportion of the transaction value saved through reduced fraud and error,
- the average length of entitlement, and
- other relevant factors.

Factors to consider when calculating tertiary prevention

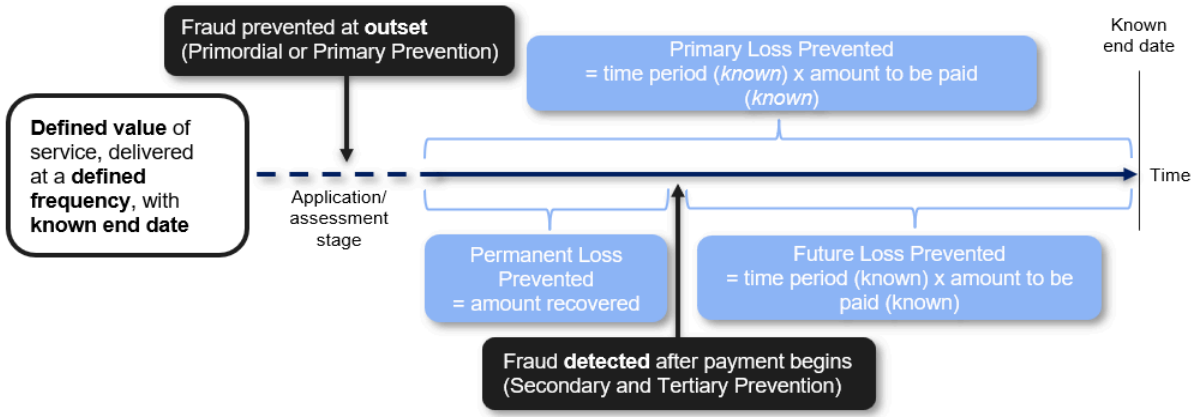
Calculating the value of permanent loss prevented through recovery action (tertiary prevention) may need to consider:

- the number of debtors targeted by the intervention,
- the value of the overall debt due to detected fraud or error,
- the proportion of debt likely to be recovered without the intervention (counterfactual),
- the proportion of debt expected to be collected due to the intervention, and
- other relevant factors.

Tertiary prevention may also reduce future losses in some cases, if implemented earlier than a normal review or detection process. An example is a case cleanse exercise, which is not standard enforcement activity, but occurs earlier than standard review periods or other pre-existing process interventions. The later the point of intervention, the more evidence is needed to support an assertion that future loss has been prevented, as opposed to only recovering funds that have already been lost to fraud or error.

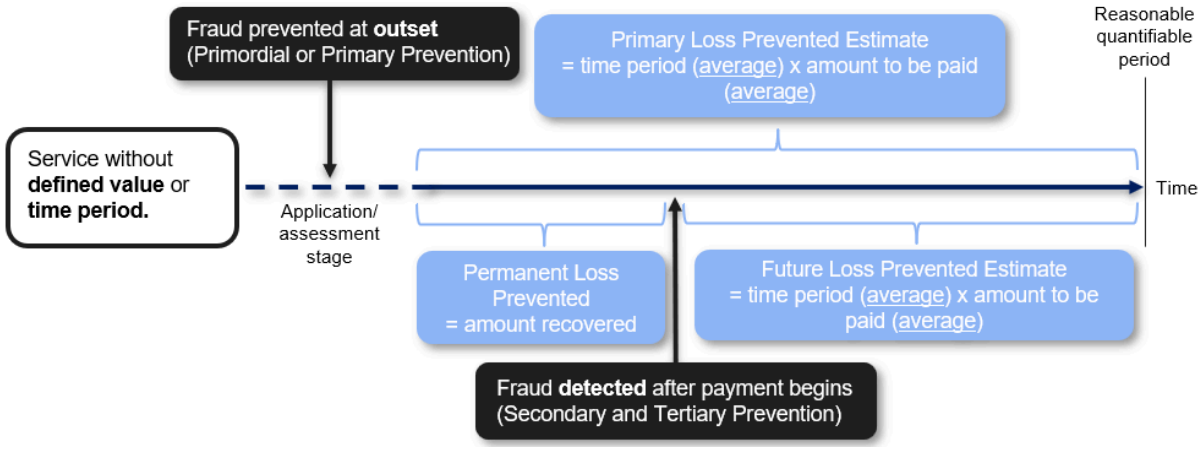
Figure 10 provides a simple illustration of how these distinct types of savings can be calculated where there is a fixed or defined value over a set period.

Figure 10 - Calculating savings where there is a fixed or defined value over a set period



Where there is no pre-defined boundary, judgement should be used to figure out a reasonable quantifiable period. As assumptions on individual behaviours (which is used to calculate future prevented loss) become less exact as time periods go further into the future, the maximum length of savings period should generally be no more than two years, unless the circumstances or evidence support a different period. See ***Figure 11***.

Figure 11 - Calculating savings where there is no fixed or defined values or time periods



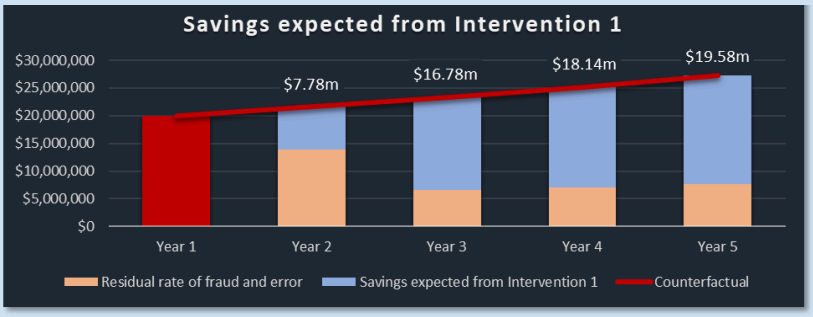
Case Study – Green Homes Subsidy Scheme

Intervention 1 (a form of primary prevention) is expected to reduce the existing rate of fraud and error loss (10%) in the GHS Scheme by 72% (80% coverage x 90% effectiveness). This reduction can be classified as primary loss prevented.

Intervention 2 (a form of tertiary prevention) is expected to reduce permanent loss by recovering funds incorrectly paid due to fraud and error, with an expected recovery rate of 50%. $20m was incorrectly paid in the first year of the GHS Scheme, therefore $10m is expected to be recovered through compliance actions. As the overall rate of loss is expected to reduce after Intervention 1 is implemented, less funds will need to be recovered beyond halfway through year 2 of the GHS Scheme.

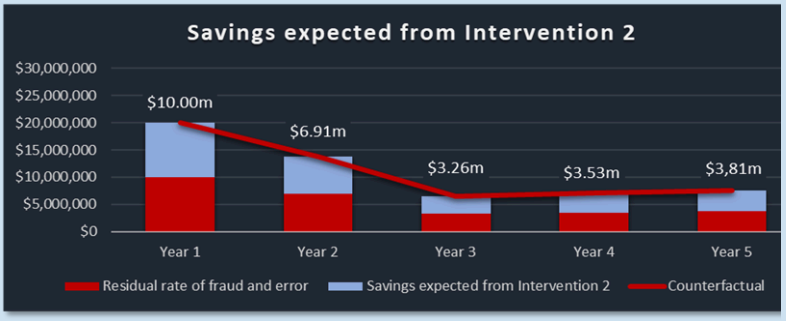
The digital claiming process, which has an estimated 72% impact on fraud and error loss in the GHS Scheme, will become effective halfway through year 2. The primary loss prevented from the point of intervention is quantified to be:

- Year 2: $10.8m expected fraud and error loss x 72% loss prevented = $7.78m
- Year 3: $23.3m expected fraud and error loss x 72% loss prevented = $16.78m
- Year 4: $25.2m expected fraud and error loss x 72% loss prevented = $18.14m
- Year 5: $27.2m expected fraud and error loss x 72% loss prevented = $19.58m
- **Total: $54.53m**



The digital claiming process is also expected to reduce collateral costs (costs involved in compliance and investigations) in years 3-5 by $3.5m. The compliance action is expected to be 50% effective in recovering funds paid due to error or fraud throughout the entire life of the scheme (5 years). After accounting for the expected impact of Intervention 1, the permanent loss prevented is quantified to be:

- Year 1: $20.00m known fraud and error loss x 50% recovery rate = $10.00m
- Year 2: $13.82m known and expected fraud and error loss X 50% recovery rate = $6.91m
- Year 3: $6.54m expected fraud and error loss X 50% recovery rate = $3.26m
- Year 4: $7.06m expected fraud and error loss X 50% recovery rate = $3.53m
- Year 5: $7.62m expected fraud and error loss X 50% recovery rate = $3.81m
- **Total: $27.61m**



What is the return on investment?

Calculating the return on investment (ROI) involves comparing the savings expected or achieved by the intervention against the full cost of implementing the intervention (including broader costs, such as regulatory and compliance costs). For an intervention to be considered cost effective, it would need to have a ROI ratio greater than 1:1.

The earlier section illustrates how savings from interventions can be estimated or measured. The costs of interventions mainly consist of the resources and money needed to:

- undertake preliminary activities, and
- implement and maintain the interventions to reduce fraud and error losses.

Case Study – Green Homes Subsidy Scheme

Calculating the ROI for Intervention 1

The capital costs to implement Intervention 1 are $7.00m. After also attributing half the costs of delivering the preliminary activities to this intervention, the total investment is $7.01m. When dividing the expected savings attributable to this intervention ($65.78), the ROI is 9:1. ***See Table 3***.

Table 3 - Calculating the ROI for Intervention 1 (the digital claiming process)

Investment (Costs)		Return (Savings)	
Preliminary activities	Primary prevention	Primary loss prevented	Collateral costs avoided*
$0.01m	$7.00m	$62.28m	$3.50m
	Total: $7.01m		**Total:** $65.78
			ROI: 9:1

*The effect of this intervention is also expected to reduce the costs involved in compliance and investigations in years 3-5 by $3.5m.

Calculating the ROI for Intervention 2

The resources to implement Intervention 2 will cost $8m ($5m for years 1 and 2, before reducing to $1m per year for years 3, 4, and 5). After also attributing half the costs of delivering the preliminary activities to this intervention, the total investment is $8.01m. When dividing the expected savings attributable to this intervention ($27.51m), the ROI is 3:1. ***See Table 4***.

Table 4 - Calculating the ROI for Intervention 2 (the compliance actions)

Investment (Costs)		Return (Savings)	
Preliminary activities	Tertiary prevention	Permanent loss prevented	Collateral costs avoided
$0.01m	$8.00m	$27.51m	$0.00m
	Total: $8.01m		**Total:** $27.51
			ROI: 3:1

Calculating the combined ROI for both interventions

The total investment for both interventions was $15.02m. When dividing the expected savings attributable to this intervention ($93.29m), the ROI is 7:1. ***See Table 5***.

Table 5 - Calculating the combined ROI for Interventions 1 & 2

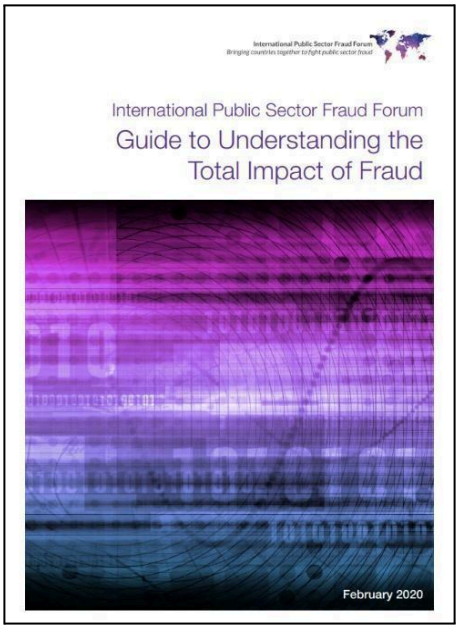
Investment (Costs)			Return (Savings)		
Preliminary activities	Primary prevention	Tertiary prevention	Primary loss prevented	Permanent loss prevented	Collateral costs avoided
$0.02m	$7.00m	$6.00m	$62.28m	$27.51	$3.50m
		Total: $13.02m			**Total:** $93.29
					ROI: 7:1

Showing indirect and non-financial benefits

Where possible, organisations should also try to measure the indirect and non-financial benefits of counter-fraud activity.

The impact of effective counter-fraud activity goes beyond the direct financial benefits. For example, an effective detection program can deter fraudulent actors, increase public confidence in services, lead to improved compliance, reduce business costs and reduce public harm.

The IPSFF Guide to Understanding the Total Impact of Fraud sets out the key extending impacts of fraud, noting that many cases of fraud will have a number of different impacts. This includes:



- Human impacts
- Government outcomes impacts
- Reputational impacts
- Government system impacts
- Environmental impacts
- Security impacts
- Financial impacts

Understanding these impacts enables organisations to prevent or mitigate these impacts and educate their employees and stakeholders on the importance of counter-fraud measures.

Organisations should also try to measure these non-financial benefits where possible. This could involve setting up or using Key Performance Indices (KPIs) or conducting questionnaires and surveys. Appendix B provides further information on how to show non-financial benefits.

Non-financial considerations can also be cyclical with one leading to another and become a self-sustaining cycle.

In considering the non-financial impacts of fraud, organisations are encouraged to consider fraud in the broad context of society, which can be done through regular monitoring of media outlets, information and intelligence, social media platforms, academic research and professional body reports.

Table 6 - Examples on how non-financial impacts can be measured[10]

 **Public confidence**	• **Quantitative** – performance of the organisation on international indices with comparable institutions in other jurisdictions • **Qualitative/Narrative** – staff, stakeholder or client engagement surveys or research showing increased trust and integrity in organisations that invested in countering fraud • **Narrative** – comparative examples of the reputational damage that other organisations suffered because of similar fraud
 **Government resources**	• **Quantitative** – comparison in cost of early detection and disruption against total costs of delayed intervention (e.g. prosecutions) • **Quantitative/Narrative** – value of reduced likelihood of systemic fraud, policy failures or the need to redesign government programs
 **Access and efficiency of government programs**	• **Qualitative** – victim impact statements highlighting any poor outcomes currently experienced by service recipients • **Quantitative** – improvements to client satisfaction • **Quantitative** – safer and more effective services delivered with reduced instances of fraud or sharp practice
 **Industry or sector**	• **Qualitative** – consultation with delivery partners about existing impacts and how counter-fraud investment may address them
 **Safety and security**	• **Quantitative** – reduction in account or identity compromise • **Quantitative** – efficiency of policing, counterterrorism or anti-fraud disruption operations through greater capacity or capability • **Qualitative** – intelligence that shows criminals are finding it difficult to commit specific types of fraud • **Qualitative/Narrative** – unsafe practices avoided through improved standards

Even where some benefits cannot reasonably be measured, showing non-financial benefits can be useful to:

- present a more holistic picture to decision-makers
- strengthen an investment case
- demonstrate the wider value achieved by reducing fraud and error.

See '*communicating prevention savings*' below on how to communicate and build a narrative around the non-financial benefits of reducing fraud and error losses.

[10] Counter Fraud Investment Cases – Leading Practice Guide. Commonwealth Fraud Prevention Centre. Counter Fraud Investment Cases Leading Practice Guide | Commonwealth Fraud Prevention Centre

UK Universal Credit Advance Fraud 2019

The UK Department of Work and Pensions looked to address potential hardship experienced by people waiting to receive welfare payments on new claims by implementing advance payments. Applications for advances were made to be simple and low friction. As any advance would be recovered from the final award, the risk of loss was considered small.

However, the system was soon inundated with claims for advances for what would happen to be bogus claims and could not be recovered – c.100,000 by December 2019. The direct financial implications of this were straight forward. However, its wider impacts can also be proved through management information (MI) data analysis. The processing capacity for the surge in advance payments impacted those waiting on legitimate claims, causing delay and potential hardship.

Another useful source of data is the civil court claims statistics. Public bodies instigating significant volumes of fraud recovery actions place the civil court system under strain, affecting not only public offices but also individuals accessing the legal system. This can further lead to other non-financial impacts such as stress, anxiety and ultimately potential financial impacts as individual court delays can cause further costs and losses of income.

Checkpoint

Now you have quantified the savings from the intervention/s and found indirect and non-financial benefits, you can now prepare how you will communicate these.

Communicating prevention savings

Communicating financial and non-financial benefits

When reporting the financial and non-financial benefits of preventative activities, the way in which data is presented is critically important to communicating the results as clearly and impactfully as possible.

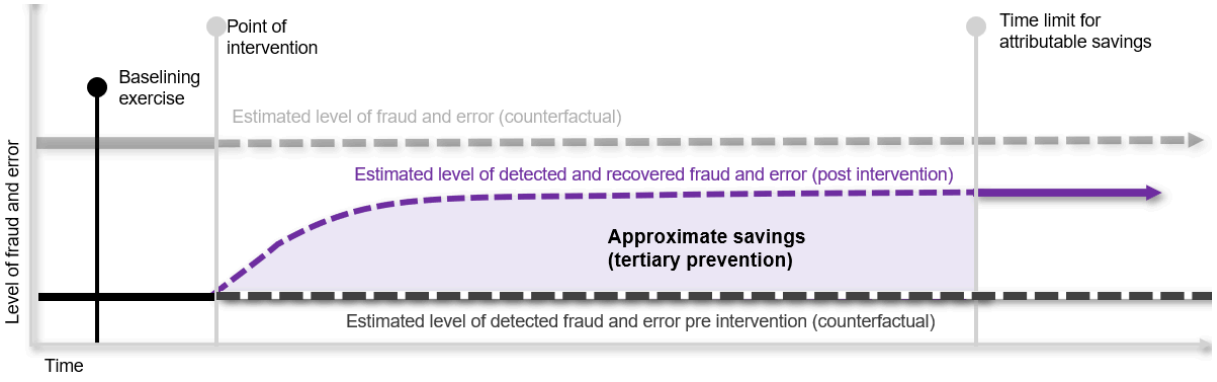
Data visualisation and narrative are key to communicating results as clearly and impactfully as possible.

Data visualisation is a powerful tool for transforming complex data into clear, meaningful insights by using visual elements like charts, graphs, maps, dashboards, and infographics. It transforms raw data into visual formats that are easier to understand, interpret, and communicate, helping people quickly grasp complex patterns, trends, and insights.

When deciding on a visualisation technique, the most important consideration is the intended audience. Data visualisation is vital to convey in easy to grasp ways what might be complex algebraic or other calculating approaches. The visualisation should be able to express the results with little, if any, further explanation needed.

Figure 12 below gives an example of how you might visualise an increase in fraud and error detected and recovered because of a new intervention (e.g. investment in compliance resources) in comparison to the counterfactual. In this scenario the current level of detected fraud and error is below the estimated level of fraud and error. The intervention is expected to increase the amount of fraud and error detected and recovered, leading to savings by reducing permanent loss.

Figure 12 - Illustrative example of visualising approximate savings from Tertiary Prevention



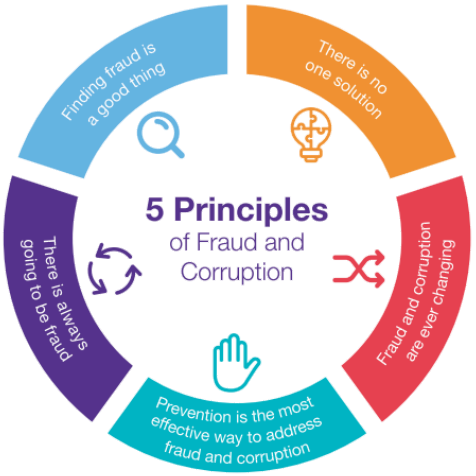
The Australian Commonwealth Fraud Prevention Centre has published the Fraud Data Analytics Leading Practice Guide, which includes further information on data visualisation and design principles.

Online sources, such as Tableau and GoodData, also provide helpful tips and best practices for data visualisation.

Developing a persuasive narrative

It is also important to consider a strong counter-fraud narrative to communicate the importance of fraud prevention and the non-financial harms that preventative activity can also mitigate.

The International Public Sector Fraud Forum developed **five principles** of fraud and corruption. These principles provide a solid foundation to communicate the benefits of measuring fraud prevention savings:



1. Recognising that **there is always going to be fraud** underscores the need for robust prevention efforts, which can be quantified through Savings Measurement to show effectiveness.
2. Embracing the idea that **finding fraud is a good thing** helps shift the focus to proactive identification and prevention, where measuring savings highlights the value of early intervention.
3. Since **there is no one solution**, measuring prevention savings supports a comprehensive approach by providing evidence of how different strategies contribute to reducing losses.
4. Acknowledging that **fraud and corruption are ever changing** reinforces the importance of continuously tracking savings to adapt prevention efforts in response to emerging threats.
5. Finally, emphasising that **prevention is the most effective way to address fraud and corruption** shows that measuring prevention savings not only justifies the investment in proactive controls but also shows cost efficiency compared to detection and recovery, helping build a strong business case for ongoing fraud prevention initiatives.

When constructing a counter-fraud narrative, organisations may consider the following:

- why change is needed
- examples of the financial and non-financial impacts of fraud (e.g. social harm, erosion of trust/ faith, security, environment etc.)
- legislative/policy/regulatory requirements
- fraud is preventable
- benefits to the organisation in preventing fraud.

With any narrative it is vitally important to consider the audience you are writing to and what you want from them:

- Are they counter-fraud experts or are they another discipline such as finance or policy development - ensure you are using language and terms they will understand so explain terms and acronyms – never assume knowledge?
- Consider their perspective on countering fraud and what they would most need or want to know about the wider subject and the specific proposal.
- Tell a story and set the context of how we have got here and what is proposed/where we want to get to and why – the core message.

For more information on how to develop a strong counter-fraud narrative, see the Commonwealth Fraud Prevention Centre's Counter Fraud Investment Cases Leading Practice Guide.

Reporting and communicating outcomes internally and externally

Effectively communicating the outcomes of Savings Measurement activities is crucial for showing the value of counter-fraud initiatives within a public body. By clearly reporting the financial and non-financial impact of these efforts, public bodies not only justify their investment in counter-fraud activities but also foster transparency, support strategic decision-making, and reinforce a culture of integrity and accountability.

Communication will likely be needed across a range of stakeholders, both internal and external to the public body.

Internal communication can help:

- promote awareness and engagement across an organisation about the importance of counter-fraud efforts
- officials feel empowered to prevent and address fraud through basic fraud risk planning
- provide insights on the reduction of risk, and
- drive continuous improvements by learning from outcomes to improve processes, controls and future counter-fraud strategies.

Internal communication may include reporting the results of the prevention savings activities through management chains and to Executive Committees, governance bodies or teams that approved the investment and resourcing, or more broadly across the organisation.

Communicating externally can help:

- build public trust and confidence that public funds are being protected
- justify the value of funding and resources to external funding bodies
- meet reporting obligations
- develop a government-wide understanding of the fraud landscape
- deter those considering fraudulent activity.

External communication may include reporting to a centralised counter-fraud body responsible for counter-fraud policy, or other agencies such as finance ministries and audit offices. Some organisations may also wish to communicate successes publicly, either as public announcements, publications, or as part of focused behaviour change activity, to deter fraud and increase public trust. For example, the UK government published 'efficiency savings' that include the preventative activity in counter-fraud with total savings of over £1bn of audited savings for 2022-23.[11]

Checkpoint

Now you have prepared to communicate the results as clearly and impactfully as possible, you are ready for your savings measurement to be evaluated and approved.

[11] Government efficiencies and savings (2022/23) - GOV.UK

3

Governance, approval, assurance and review

To ensure that the results and reported outcomes from Savings Measurement can be compared within an organisation[12], as well as more broadly across the public sector, it is necessary that there are governance, approval and assurance processes in place.

> Good governance arrangements ensure methods used to figure out prevention savings are reasonable, robust, consistent and credible.

There is no one-size-fits-all approach to setting up and maintaining governance arrangements for Savings Measurement. Arrangements and processes should be fit-for-purpose and adaptable to enable:

- efficiency and applicability for smaller organisations or internal budget measures, as well as
- robustness and credibility for more significant budget proposals and business cases.

Central governance, approval and assurance structure

A good example of a governance model that applies across a jurisdiction is the UK government's Prevention Panel, which is an independent panel of experts that meets quarterly to review methods used by UK public bodies to calculate fraud or error savings due to counter-fraud initiatives.

This arrangement helps ensure methods used by public bodies to generate figures of fraud and error savings are reasonable, robust, consistent and credible. Robust reporting enables the scale of the fraud challenge to be accurately assessed, as well as the impact of counter-fraud activity to be proved. This provides a compelling evidence base for departments to build the case to invest in counter-fraud capability and capacity, and ensures an up-to-date repository of approved methods via the Methodology Bank which all public bodies can use.

A Prevention Panel model can also validate methods after predicted savings can be verified and confirmed (see Retrospective review). This may form part of a wider audit and assurance process for savings.

Setting up the Prevention Panel

For a Prevention Panel to produce better results, it is important to establish the reputation of the Panel as an independent authority. This includes:

- maintaining reputable and qualified experts with proper, specialised skills (e.g. economist and statisticians) to provide assurance over complex statistical methods
- recruiting experts through formal Expressions of Interest to look for broad and diverse representation
- regularly rotating panel membership to ensure engagement.

See Appendix D for skills, training and other important attributes needed in conducting fraud prevention saving measurement.

[12] As depicted in the 'Fraud Iceberg Stack Model' in the Appendices (adapted from the UK Government Counter Fraud Profession)

Rules and regulations should predetermine parameters for when a method for Savings Measurement must be given to the Prevention Panel for approval. While the Prevention Panel can increase credibility, requiring all methods to go through the Panel's process may create huge burdens on smaller organisations or small-sized programs, functions or activities, thereby discouraging organisations to measure their fraud prevention savings. This can also create huge pressure on the Prevention Panel, and cause delays to the approval process.

Each jurisdiction should find the balance between resourcing and ensuring the quality of methods, depending on their own circumstances. For example, a jurisdiction may decide that, for programs, functions or activities involving resources under a certain threshold, it may be sufficient for any Savings Measurement methods to go through their organisation's internal audit committee. However, even in these circumstances, organisations should still provide their methods to the Prevention Panel for visibility and, if needed, feedback. Moreover, where rules or regulations require a method to be approved by the Prevention Panel, there should be clear expectations and consequences for non-compliance with reporting obligations.

The Prevention Panel's process for screening and endorsing methods must be clear and easy to navigate. This includes providing a clear and streamlined Submission Template for participating organisations to use when they submit their methods for endorsement.

For the Prevention Panel to be effective in promoting and improving Savings Measurement, the Panel should use the process as an opportunity to consult with public bodies and aid in their development of methods. Where submissions are unsuccessful, the Panel should provide detailed feedback and guidance to help departments improve their proposed methods.

To further improve the overall rigour and credibility of all preventative savings, the Panel should also perform a secondary assurance process when forecast/estimated savings have been subject to re-measurement. On completion of a retrospective review that evaluates the assumptions and predictions made for estimated savings, the Panel should offer a view on the impact of the new evidence. This could range from verifying actual calculated savings, confirming the estimate or reducing the forecast impact of the change.

Methodology Bank

Aside from ensuring the credibility of methods employed by public bodies, another important value of the Prevention Panel is overseeing the development and management of a Methodology Bank. This is a repository of all methods which have been approved by the Prevention Panel and can be used by other public bodies as a starting point to develop their own methods. This promotes efficiency and consistency at the national level, and allows smaller public bodies, which may not have the resources or ability to develop their own methods, to also take part in Savings Measurement.

The Methodology Bank should categorise methods either by fraud typology (e.g. internal fraud) or type of intervention (e.g. secondary prevention) and outline the background and method used to calculate savings. To further aid public bodies in making better use of the Methodology Bank, there should be guidelines on circumstances under which each method might best be applied.

Retrospective review

All methods should be subject to retrospective review. These are undertaken for two principal reasons:

1. After new interventions have fully taken effect, the assumptions used to forecast their effect should be evaluated to confirm whether they hold true. Re-testing may confirm the forecast, or show the intervention had a greater or lesser impact than expected. In any case the revised savings figure will become more robust and provide added credibility to claimed savings.

2. A review of the estimate will inform how any enduring value should be attributed. If the savings period is a year or less, this may be drawn from the first re-test. If the savings period is longer, review should be undertaken towards the agreed end point of the savings period, prior to commencement of the enduring value period.

Retrospective reviews may also uncover unattended fraud risks or control weaknesses, on which organisations may invest more resources. This can lead to the control environment being further improved, with other reductions in fraud and error loss being measured throughout the lifecycle of the program, function or activity.

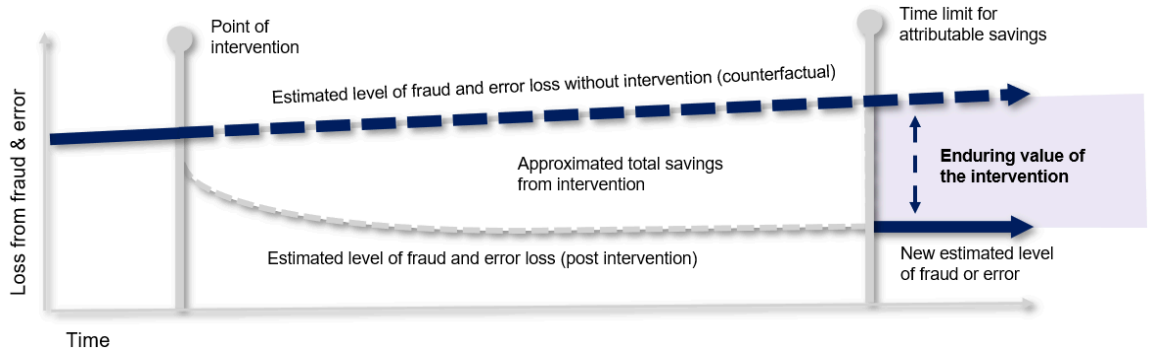
Another benefit of re-testing is that it can provide evidence to support other prevention savings proposals, where previously forecasted impacts can be broadly confirmed and attributable to specific interventions. The evidence and methods can then be confidently replicated, including extrapolating results for comparable programs, activities or functions (e.g. included as part of the Methodology Bank).

To ensure fair comparison, methods for retrospective reviews will likely be the same as those used to show the level of fraud losses during baselining. However, other ways to evaluate the veracity of the savings may be needed. For example, if the original risks and mitigating interventions were identified through a full fraud risk assessment and control plan, but only one risk was addressed with one intervention, a straightforward measure of the reduction in expenditure or service provision may be sufficient to demonstrate the impact (assuming the reduction is not attributable to other variables).

Enduring value

Enduring value is the ongoing financial value of keeping an intervention in place after the quantifiable period ends. In some circumstances, e.g. a program, activity or function with no defined end date, the enduring value of interventions can be quantified and attributed via retrospective reviews or an ongoing cycle of measurement. Ongoing costs to maintain interventions (e.g. keep a control in place) should also be estimated at this point.

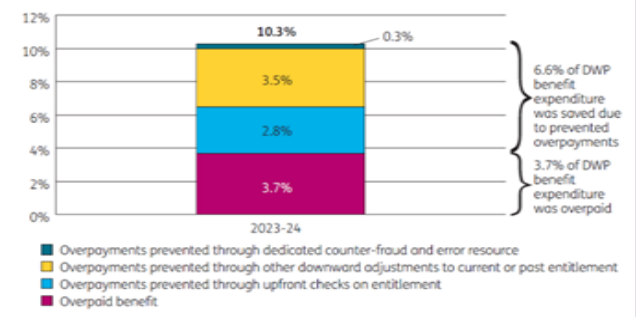
Figure 13 - Enduring value



Recognising and, where possible, quantifying the enduring value of interventions can help support decisions to maintain controls or ongoing investment of resources. This can also help with undertaking an informed cost/benefit analysis of the impacts, including non-financial impacts, of removing a control at a future point.

Example of the UK Department of Work and Pensions (DWP)

The upfront interventions, and later ongoing verification of entitlement, significantly prevents more fraud and error than the dedicated counter-fraud resource. Many of these ongoing checks originally started as counter-fraud initiatives which became business-as-usual (BAU) activities, and the value of savings these measures generate are no longer attributed to counter-fraud activity.



For example, the identity verification process had been saving £140m per annum until 2022/23 when it moved to BAU delivery.

Managing risks associated with savings measurement

Savings measurement can create perverse incentives if not carefully designed and implemented. For example, public bodies may prioritise specific types of interventions that yield financial returns at the expense of overall program integrity. Another example would be setting performance targets based on financial results, which may bias effort towards easy wins at the expense of more important, yet more complex and uncertain outcomes.

Reporting on savings could also be open to manipulation, especially when linked to a reward, such as increased funding.

The preliminary activities and governance arrangements outlined in this Framework are key guardrails that help mitigate risks relating to Savings Measurement. Additionally, any governance, approval, assurance and review processes should ensure proper actions are taken to avoid perverse incentives, such as ensuring approaches to Savings Measurement:

- are holistic – evaluating risks, interventions and savings in a broad way to avoid fixating on just one element to define success, e.g. financial returns
- use a variety of metrics – collect, track and analyse a variety of different outputs and outcomes
- are consultative – consult and obtain buy in from all levels of the organisation, including both management and staff
- align incentives – do not tie performance on a specific fraud metric to a function's budget.[13]

[13] Demonstrating Integrity: A Technical Appendix to A Framework for Managing Fraud Risks in Federal Programs, US Government Accountability Office, Combating Fraud: Approaches to Evaluate Effectiveness and Demonstrate Integrity | U.S. GAO

Conclusion

Fraud is a growing societal and economic issue that is increasingly affecting individuals, businesses and governments around the world. However, in the absence of consistent, credible measurement approaches, public bodies have often found it challenging to secure investment to prevent fraud in existing programs or functions, or to account for savings derived from fraud prevention when designing new policies or programs.

> The work now begins to use this Framework to prove the true value and impact of our work in counter fraud.

Moreover, geopolitical shifts, socio-economic factors, digitisation and technological advances are material drivers for fraud risk and are significantly altering the fraud landscape. This is exposing public bodies to new risk vectors and vulnerabilities and creating the potential for fraud to occur at increased scale and velocity.

Unlocking investment to prevent fraud at the earliest possible stage is the only way we can effectively address this adaptive problem in a less certain future. This requires collective effort to build and embed capability within the public sector to measure both the scale of the fraud problem, and our successes in addressing it – essentially lifting the iceberg out of the water and starting to reduce its overall size.

This Framework sets out the key principles and activities needed to credibly estimate and quantify the financial and non-financial benefits of fraud prevention and compliance activities. The work now begins to use this Framework to:

- demonstrate how fraud risk planning and development of controls translates into measurable savings,
- demonstrate the true value and impact of our work in counter fraud,
- enable informed decision-making for how fraud should be managed,
- strengthen business cases for investment in preventing fraud, and
- put counter fraud functions on a long-term sustainable footing.

Our collective efforts across the IPSFF to embed prevention measurement capability has never been more important – nor has it had more opportunity to make an impact.

Shifting the focus and investment away from reactive approaches towards more cost-effective prevention initiatives will not only deliver more economic value for governments and public bodies, it will also deliver significant societal benefits for the communities we serve by ensuring public policies and expenditure achieve their intended purpose.

Glossary

Baseline	The benchmark for measuring the effect of any type of intervention. This is usually the known or estimated level/rate of fraud and error; however it can be broader, e.g. total transactions within a specific program, activity or function.
Control	A process, policy, device, practice or other action put in place to regulate or modify a risk.
Counterfactual	A key part of the method that looks to show 'what would have been' had the change not occurred.
Enduring value	The value realised from maintaining existing interventions and assurance of entitlement to services.
Error	Where an instance has been found that the payment or transaction is incorrect or wrong but, based on the evidence available, the balance of probability is that there is no intent, then this is classified as error. It is possible that the evidence available on the intention behind an action may vary as time goes on - and as such an instance may be reported as error initially, and then part or all of the loss be defined as fraud at a later stage (and vice versa).
Fraud	Dishonestly obtaining (including attempting to obtain) a gain or benefit, or causing a loss or risk of loss, by deception or other means. A benefit or loss is not restricted to a material benefit or loss, and may be tangible or intangible. A benefit may also be obtained by a third party.
Fraud control	Activities or mechanisms that can help an organisation prevent, detect and respond effectively to fraud. The Commonwealth Fraud Prevention Centre's Fraud Control Catalogue includes over 70 types of fraud controls.
Fraud control testing	A process that applies different testing methods to measure the effectiveness of fraud controls.
Fraud loss measurement	Specific and proactive exercises to measure the residual risk of fraud and error using extrapolations from statistical sampling and using independent evidence sources.
Fraud measurement	The counter-fraud discipline which includes fraud management information, fraud estimates, fraud loss measurement exercises and prevention methods.
Fraud risk assessment	A process to assess and understand the organisation's exposure to fraud, the associated risks and the strength of existing controls.
Fraud typologies	The type of fraud that the change has sought to reduce (e.g. internal, mandate, third party).
Intervention	Any activity undertaken with the aim of reducing the likelihood (probability and frequency) or consequence (duration and impact) of fraud and error in a program, activity or function. For example, an intervention will implement a new control.
Methods	The technique by which expected or actual savings are figured out – this may include financial calculations as well as evidence of non-financial benefits.

	Estimation	An informed and evidence-based assumption of how the intervention will reduce fraud and error levels (or has reduced fraud and error levels) in comparison to the counterfactual.
	Quantification	Calculating the amount expected to be saved based on the difference between the predicted reduced rate of fraud and error and the counterfactual over a defined period.
	Validation	Assuring the measurement of prevention savings via governance arrangements and audits and will consider what was estimated against what the quantified impacts were.
	Communication	Communicate and present the impact of counter-fraud interventions to key decision-makers
Methodology Bank	A repository of all methods which have been approved by the Prevention Panel, and can be used by all other public bodies wishing to claim prevented savings based on an estimated value.	
Prevention	There are four distinct types of prevention interventions:	
	Primordial prevention	Interventions at the design stage that reduce the risk of fraud from manifesting in the first place.
	Primary prevention	Interventions at the application stage of existing programs to reduce the likelihood of fraud.
	Secondary prevention	Detection mechanisms that find and stop fraud and error losses at an earlier stage.
	Tertiary prevention	Recoveries made from responding to fraud that has occurred to reduce its impact and severity.
Prevention Panel	An independent panel of experts that meet quarterly to review preventative methods used for the calculations of fraud or error savings in counter-fraud initiatives	
Prevention savings	The amount of benefits, in monetary terms, that have been saved due to implementation of fraud interventions. Savings include the value recovered from compliance activities.	
Return on investment	The ratio between the savings attained from implementing relevant fraud prevention measures, and the cost of implementing the said fraud prevention measure.	
Savings period	The time period used when calculating and estimating the future prevented loss. The default maximum length of time to be considered for Primary or Secondary Savings should be no more than two years unless the circumstances or evidence support a different period. Any savings from Tertiary Prevention will require evidence to show that such late interventions have prevented any permanent losses.	

Appendix A – Supporting tools, guides, frameworks and standards

Fraud Prevention Savings Calculator

This calculator has been developed to help organisations apply a method that is consistent with the IPSFF Fraud Prevention Savings Framework to estimate and quantify the financial savings delivered by preventing fraud and error.

Fraud Prevention Standard for Counter Fraud Professionals

This standard by the UK Public Sector Fraud Authority contains the agreed professional standards and guidance for fraud prevention professionals in the public sector. They are designed to present a consistent cross-government approach to prevention, raise capability and through this, increase the knowledge and competency of those working in this field.

Counter Fraud Investment Cases Leading Practice Guide

This guide by the Commonwealth Fraud Prevention Centre provides practical steps for developing a business case for investment, helping you communicate the problem to senior leaders, educate them on the financial and non-financial benefits of prevention, and make a strong case for investing in effective counter fraud or anti-corruption measures and resources.

Fraud Risk Assessment Standard for Counter Fraud Professionals

This standard by the UK Public Sector Fraud Authority contains the professional standards and guidance for people and organisations who are undertaking fraud risk assessments in central government.

Fraud Risk Assessment Leading Practice Guide

This guide by the Commonwealth Fraud Prevention Centre provides key principles and methods taken from leading practices across sectors on the fraud and corruption risk assessment process (can be used to help inform the development of targeted fraud and corruption risk assessments).

IPSFF Fraud Control Testing Framework

This framework sets out key principles, processes and tools for conducting fraud control testing within public sector organisations.

IPSFF Fraud Loss Measurement Framework

This framework helps public sector organisations conduct Fraud Loss Measurement exercises that provide a credible estimate of the levels of fraud and error related to a specific program, activity or function in an organisation.

Controlling Fraud and Corruption Risk Leading Practice Guide

This guide by the Commonwealth Fraud Prevention Centre helps officials better understand the factors that lead to fraud and corruption, and advise on a range of strategies that public

bodies can implement to mitigate the probability of these risks as well as the harm they cause for the public sector and those who rely on us.

Fraud Control Catalogue

This catalogue, developed by the Commonwealth Fraud Prevention Centre, provides an extensive reference of over 70 types of fraud controls that can prevent, detect and respond to fraud and error.

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.

Fraud Data Analytics Leading Practice Guide

This guide by the Commonwealth Fraud Prevention Centre provides a framework and principles for implementing leading practice fraud data analytics.

Fraud Data Analytics Catalogue of Techniques

This catalogue, developed by the Commonwealth Fraud Prevention Centre, provides helpful direction on the types of analytics techniques to explore, and examples of when and how to deploy them.

IPSFF Guide to Understanding the Total Impacts of Fraud

This guide combines leading global perspectives to provide useful information that raises awareness of the impacts of fraud.

Appendix B – Demonstrating non-financial benefits

There are three primary approaches for showing the preventative benefits on non-financial impacts of fraud. These are:

- quantitative approaches (e.g. KPIs or other metrics)
- qualitative measures (e.g. surveys and questionnaires)
- narrative (i.e. describe the non-financial impacts that fraud can have and how its reduction also reduced these wider harms).

Quantitative approaches

Quantitative approaches require numbers to prove a point. Non-financial benefits may not lend themselves to obvious KPIs. However, there may be other metrics that can show the non-financial repercussions that result.

Capturing data on the non-financial impacts of fraud

Improving non-financial quantitative data capture helps build a feedback loop, where control weaknesses found from enforcement activities provide insights to fraud control experts and senior leaders on potential areas of investment.

Initial fraud referrals should record any alleged or suspected non-financial impact or loss, which should be reviewed and marked as confirmed or otherwise after investigations are completed, in the same way as financial allegations have always been. Over time, the organisation can build a credible data set on the volume and types of non-financial aspects of fraud. Organisations may contact the Australia CFPC or the UK PSFA for advice on how they can set about doing this.

Retrospectively using data on the non-financial impacts of fraud

Baselining exercises such as FLM may retrospectively use non-financial data to measure the effectiveness of an intervention. For example, once the volume of fraudulent applications is measured, the time taken to process these applications can be extrapolated to estimate delays caused to legitimate applicants. Post intervention re-measurement can then assess the reduction in fraudulent claims by contrasting with the pre-intervention sample and, from this, show the improvement in processing times for legitimate applicants.

Qualitative measures

Qualitative measures are useful in considering non-financial impacts of fraud when the impacts are not easily quantifiable. Qualitative approaches such as surveys, questionnaires, interviews and observations can be used to understand and analyse experiences and behaviours. The outcomes can then be extrapolated into quantitative data.

Qualitative surveys can be used in a range of ways – from assessing individual experiences in dealings with an organisation (e.g. assessing customer satisfaction) to the level of confidence in an organisation or service. Loss of public confidence in an organisation's ability to manage fraud can undermine the delivery of that service and increase fraudulent attacks if controls are perceived to be weak. Organisations may look to show the moving of the dial on this as part of any wider fraud prevention and compliance activity.

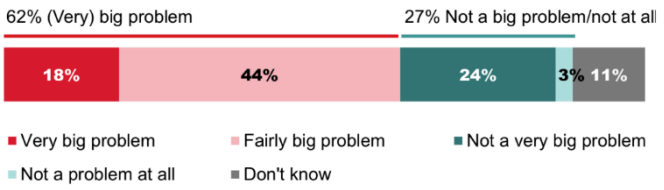
DWP 2023 survey of public perceptions of fraud in the welfare system[14]

A survey by the UK DWP sought to understand public perceptions of fraud, error and debt in the welfare benefits system, and to gauge attitudes toward a range of proposed new powers to reduce it.

These include providing greater third-party access to data, modernising information-gathering powers, seeking law-enforcement powers, developing debt recovery, and reforming the current penalty regime.

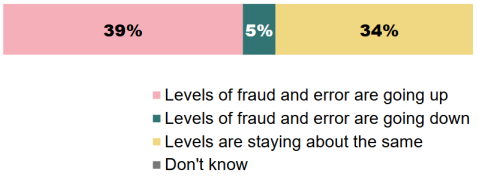
The intent of this survey, and the publication of the results, was to gauge public attitudes prior to the proposal of new powers that would look to reduce fraud and error within welfare.

Figure 3.1: People were twice as likely to believe fraud and error was a big problem in the welfare benefits system, as believe it is not a big problem
In general, how big a problem, if at all, do you think fraud and error in the welfare benefits system is in the UK?



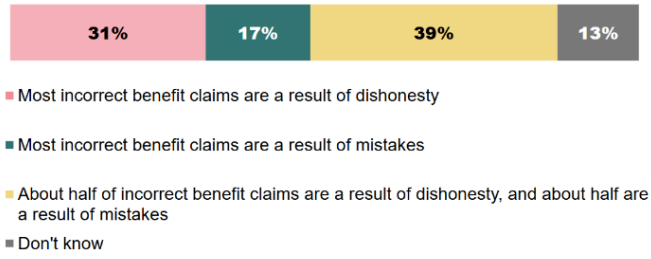
Base: 2,127 UK adults 18+

Figure 3.2: The majority of respondents were split between whe and error were increasing or staying the same
Do you think that levels of fraud and error in the welfare benefits sy going up, going down or staying about the same?



Base: 2,127 UK adults 18+

Figure 3.3: Respondents were more likely to blame dishonesty than mistakes for the majority of incorrect claims
Which of the following statements is closest to your view?



Base: 2,127 UK adults 18+

Narrative

When no direct evidence is available or reasonably obtainable, organisations may rely on expert opinions, research, or comparable case studies to estimate and describe the non-financial impacts that fraud prevention and compliance activities can have.

[14] Survey of public perceptions of fraud, error and debt: research report - GOV.UK

Appendix C - Data governance

A savings measurement function should have a process to manage data, with guiding principles that include:

- **Data integrity** – Measurements must be designed to ensure that data is not changed or modified during, or because of, the Savings Measurement being performed (except to rectify errors). This will enable measurement to be repeatable and aids with defending conclusions and providing transparency.
- **Maintaining security and access over data** – This will ensure that data cannot be accessed and used outside of the intended purpose of measurement, particularly in cases where data is collected only for this specific purpose.
- **Stable and unmodified data models** - Any data transformation activities undertaken must not change data tables, relationships or structures used for analysis and measurement. Repeatable analysis requires a stable data model which is not at risk of modification.
- **Data quality** – The completeness, accuracy, timeliness, and appropriateness of data are important to producing accurate and useful measurement. Where data quality has been compromised, any results will likely be an inaccurate and unreliable measurement of fraud or error.
- **Governance** – An organisation's data governance policies and procedures must be defined and followed (for both internally and externally sourced data) to ensure that officials undertaking fraud measurement can rely on the quality of data being used for analysis.

Data management is not static – processes and procedures should be regularly reviewed and/or updated to reflect any changes in the organisation's data strategy and environment[15].

[15] Fraud Data Analytics – Leading Practice Guide. Commonwealth Fraud Prevention Centre. www.counterfraud.gov.au/library/fraud-data-analytics-leading-practice-guide

Appendix D - Skills, training, and other important attributes

Important skills and experience needed to plan fraud prevention saving measurements, including the identification of typologies, determination of counterfactuals, and design of methods, are as follows:

- **Counter-fraud knowledge** - an understanding of the different types of fraud (and broader bribery and corruption), how the organisation may be vulnerable to each type of fraud, and an ability to find potential fraud risk indicators using evidence.
- **Risk assessment -** an understanding of how to find inherent and residual fraud risks, including assessing and evaluating the effectiveness of controls.
- **Business knowledge -** skills and experience in using a range of research methods to gain knowledge and understanding of the organisation's structures, processes, people and business activities in the context of specific fraud risks and controls present across different areas of the business.
- **Stakeholder engagement -** an ability 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 and risk indicators work, and co-design reliable methods.
- **Statistical sampling** - knowledge of statistics and understanding and implementing various sampling techniques appropriate to the analysis needed.
- **Finding and using evidence** - the skills to find, collect, record and store data and evidence in a correct and lawful manner, including knowledge of laws and regulations relating to privacy, freedom of information, data handling and protection, and protective security and information.
- **Estimation and measurement -** an understanding of various techniques to estimate and measure instances of fraud and error, including methods to calculate prevention savings.
- **Record keeping and reporting -** ability to deliver clear, concise, accurate, and factual summaries of testing plans, processes and results, both orally and in writing[16].

Technical and expert support

Organisations will often need more support (including from specialists across the public and private sector) when building fraud prevention saving measurement capabilities in a new area, such as specific technical knowledge and complex data analysis. For example:

- **Statisticians**[17] - qualified statisticians can provide guidance and insights on the design of methods, and what is a proportionate and statistically valid size for measuring the impact of fraud controls.
- **Data scientists and analysts**[18] - for advanced fraud prevention saving measurement exercises, advice and support from data scientists can improve efficiency and accuracy.

[16] Adapted from the Quality Standards for Investigations issued by the US Council of Inspectors General on Integrity and Efficiency
[17] Advice on sample size and selection can be given by qualified Statisticians from the (UK) Government Statistical Service (GSS); (AU) Australian Bureau of Statistics
[18] (UK) Government Operational Research Service (GORS)

- **Technical subject matter experts** - depending on the specific fraud risks, it may be necessary to engage with specific technical ability. For example, if the fraud risk is around quality in construction, a quantity surveyor may be needed.

Integrity, Character and Resilience

Individuals and teams engaged in fraud prevention saving measurement must have 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 organisational vulnerabilities in processes and controls.

It is important that those engaged in fraud prevention saving measurement are impartial and ethical when using data. They must understand and implement the necessary data governance and ethics legislation, principles and practices when handling, sharing and using data[19].

As professionals, they should ensure their knowledge of related guidance and standards are up to date and be proactive in addressing any gaps within their own knowledge. They should also note any perceived gaps or weaknesses in the standards and guidance they follow and communicate these to those setting the standards.

Fraud does not stand still, and those working on fraud measurement should understand the evolving nature of fraud, and seek out innovative ways of testing for fraud, including cost-effective applications of data analytics to address new challenges.

[19] (UK) Data Protection Act, (UK) Digital Economy Act and the (UK) Freedom of Information Act