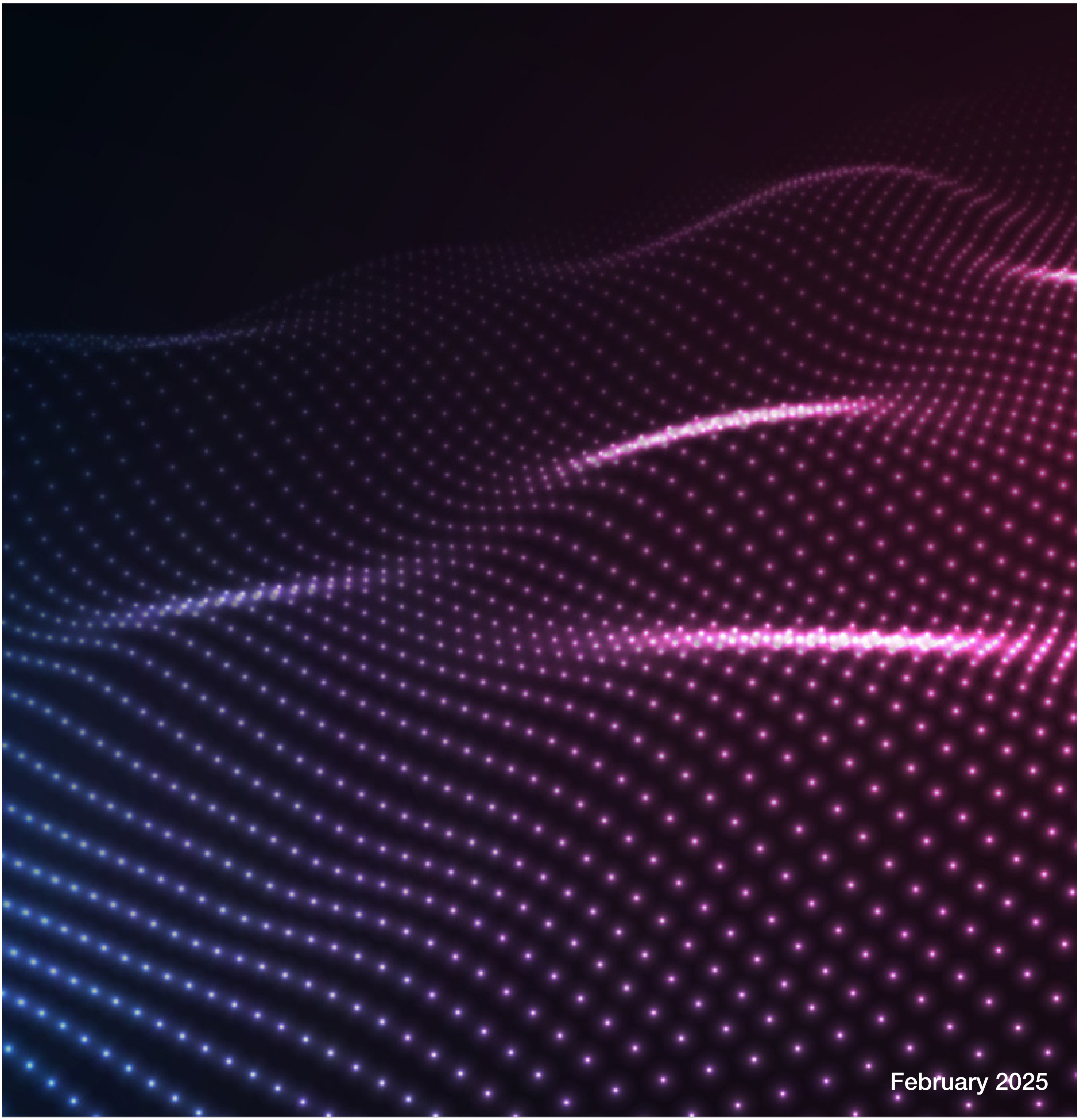
International Public Sector Fraud Forum
Bringing countries together to fight public sector fraud

International Public Sector Fraud Forum

Fraud Loss Measurement Framework



February 2025

Public Sector
Fraud Authority

Commonwealth
Fraud Prevention
Centre

Australian Government

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

Crown copyright disclaimer

The information contained in the International Public Sector Fraud Forum documentation and training is subject to Crown Copyright 2025.

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

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

The information should not be published or distributed in any way that could undermine the values and aims of the International Public Sector Fraud Forum.

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

Contents

Purpose

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

FLM exercises are part of the wider discipline of Fraud Measurement, which also includes Fraud Estimation and Fraud Management Information.

Effective FLM exercises are also dependent on other capabilities, including fraud risk assessment, fraud control testing, data sharing and data analytics. The fundamentals of these capabilities are covered in other standards and frameworks, such as the International Public Sector Fraud Forum (IPSFF) Fraud Control Testing Framework.

This Framework builds on these capabilities and enables public bodies to take a step further towards estimating a financial value for the fraud and error in the areas they are managing.

Specifically, this Framework:

- broadly defines the objectives of Fraud Measurement and specifically defines the objectives and purpose of Fraud Loss Measurement exercises
- describes the steps required to plan a FLM exercise
- explains the statistical sampling knowledge and the techniques required to undertake a FLM exercise
- explains how to identify and describe how to use evidence to test for fraud
- describes how estimation and measurement are used in FLM exercises
- describes the importance of stakeholder engagement and reporting in FLM exercises.

Who is this Framework for?

This Framework has been developed for Counter Fraud Functions across all public sector organisations. It will help Counter Fraud Professionals conduct FLM exercises in a way that provides a credible estimate of the levels of fraud and error related to a specific program, activity or function (based on a sample dataset of transactions or payments).

The Framework also supports officials with different levels of experience, and helps them to build their understanding and expertise. This knowledge can then be applied by both Counter Fraud Professionals and business stakeholders to estimate levels of fraud and error and put in place informed and targeted strategies to reduce losses.

This Framework is issued by the IPSFF in conjunction with the UK's Public Sector Fraud Authority and Australia's Commonwealth Fraud Prevention Centre. It sets out the recommended best practice for FLM. It is a principles-based document and is designed to be flexible and adapted to an organisation's individual circumstances.

Effective FLM is dependent on other capabilities, including fraud risk assessment, fraud control testing, data sharing and data analytics.

Introduction

What is Fraud Measurement?

Fraud is a growing societal and economic issue that is increasingly affecting individuals, businesses and governments around the world. This is further exacerbated by ongoing uncertainty and disruption from cost of living pressures, managing the impact of natural disasters and international events, and rapid digital transformation. These factors will continue to drive an increasing risk of fraud and present new challenges to the integrity of governments worldwide.

Executive Boards in every organisation should plan to measure and estimate the extent to which fraud is impacting their organisation. This should encompass collating Management Information on the amount of fraud being prevented, detected and recovered by existing control frameworks, and also through proactively testing representative samples of transactions to determine previously undetected fraud and error, in order to understand the level of loss that the organisation is potentially exposed to.

Fraudsters rely on deceptive techniques, which means that fraud is a hidden crime that mostly remains under the surface unless we actively look for it. As a result, there is often limited evidence to determine the extent of the fraud problem experienced by organisations. As such, proactive measurement is key to revealing this hidden crime.

The 'fraud iceberg'[1] model below visualises how the different elements of broader Fraud Measurement inform the overall picture, by providing insights around otherwise hidden elements of fraud which would otherwise not be picked up as part of detection or prevention activities.

The Fraud 'Iceberg'

Known and reported fraud (including error, bribery and corruption). This includes prevented fraud (found before payment) and detected fraud (found after payment) and also calculated prevention savings from finding and stopping a fraud that was ongoing.

Unknown Fraud

Prevented/detected fraud not reported due to failures in MI and reporting processes. Test reporting systems to provide an estimate.

Control failure resulting in fraud going unprevented or undetected, for which control testing provides an estimate.

Fraud occurring through residual risks (control gaps or weaknesses) for which FLM provides an estimate.

Unidentified and unquantified fraud

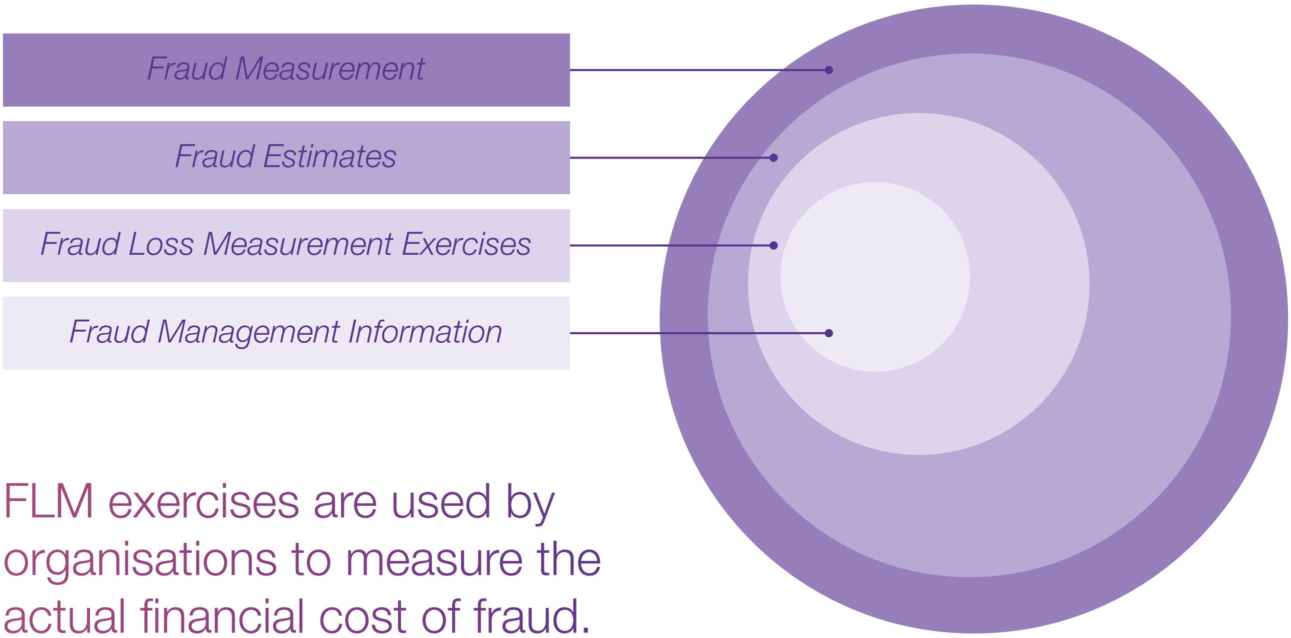
Unknown fraud due to blindspots and/or inaccessible due to a combination of data, reporting or resource limitations.

[1] The Fraud Iceberg Model (UK Government Counter Fraud Profession).

What are Fraud Loss Measurement exercises?

FLM exercises are part of the wider discipline of Fraud Measurement. FLM exercises apply a civil burden of proof[2] test to a statistically valid and representative number of transactions to identify non-compliant, fraudulent or irregular transactions within the sample. From this smaller sample, the overall level of fraud and error can be estimated by extrapolating the results across the population.

Term	Definition
Fraud Measurement	The counter fraud discipline which includes Fraud Management Information, Fraud Estimates, Fraud Loss Measurement exercises and prevention methodologies.
Fraud Estimates	Broad estimates of undetected fraud and error, derived from data indicators/modelling, comparative studies and/or Fraud Management Information. They can potentially include, or be built on, some fraud loss measurement exercises.
Fraud Loss Measurement Exercises	Specific and proactive exercises to measure the residual risk of fraud and error using extrapolations from statistical sampling and using independent evidence sources.
Fraud Management Information	The accurate reporting of the fraud and error we know about - detected, prevented and recovered fraud and error aligned to codified typologies.


Fraud Measurement
Fraud Estimates
Fraud Loss Measurement Exercises
Fraud Management Information

FLM exercises are used by organisations to measure the actual financial cost of fraud.

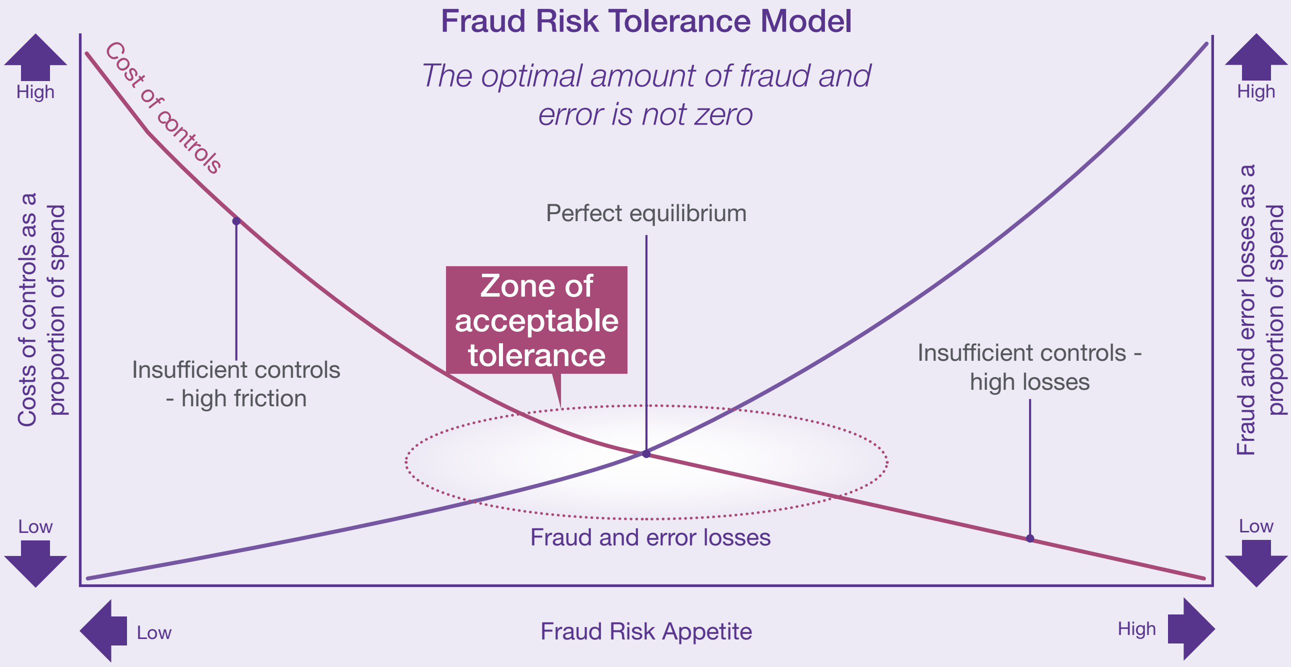
[2] The balance of probabilities’, see speech on 11th October 2023 by Lord Leggatt Justice of the (UK) Supreme Court entitled ‘Some Questions of Proof and Probability’ and also ‘Probability Reasoning in Judicial Fact Finding’ (the ‘International Journal of Evidence & Proof’, Hunt (School of Mathematics, Monash University, Australia) & Mostyn (UK Royal Courts of Justice), 2019.

Using Fraud Measurement and Fraud Loss Measurement to inform fraud appetite and tolerance levels

As fraudsters deliberately conceal their crimes, the amount of fraud detected often significantly understates the scale of the actual loss. An ability to measure, estimate and accurately report on fraud lies at the heart of an informed and effective counter fraud response. Organisations that are aware of their potential losses to fraud and error are better placed to implement targeted strategies to deal with it.

In practice, Fraud Measurement provides accountable officials with insights and perspectives necessary to make informed decisions on their appetite[3] for fraud risk and the level of fraud and error they are comfortable tolerating in order to meet the policy objectives. When the measurement shows tolerance levels are being exceeded, this can then be used as a response trigger to take remedial action, for example by implementing new controls to improve the compliance environment. These should always be balanced against the level of friction created (for example by making a customer journey so complex that a genuine applicant finds it difficult to access the service).

This can be more easily understood in the context of the below example fraud risk tolerance model:


Fraud Risk Tolerance Model
The optimal amount of fraud and error is not zero
Cost of controls
Perfect equilibrium
Zone of acceptable tolerance
Insufficient controls - high friction
Insufficient controls - high losses
Fraud and error losses
Costs of controls as a proportion of spend
Fraud and error losses as a proportion of spend
High
Low
High
Low
Low
Fraud Risk Appetite
High

An annual programme of Fraud Measurement can be used by an organisation to inform both the prioritisation of counter fraud resources in a way that is proportionate with both the value and scope of the spend activity and the estimated fraud risk exposure, as well as setting appropriate metrics based on agreed thresholds for triggering action. These should ultimately be used to shape the overarching organisational counter fraud strategy.

[3] For further context on risk appetite see the Orange Book Risk Appetite Guidance Note (UK Finance Function).

What are the benefits of proactively measuring fraud?

Taking proactive action to measure fraud and error will greatly benefit organisations and officials who are accountable for managing fraud risk, helping them make more informed decisions about their risk appetite and tolerance. FLM exercises will also help organisations take considered and decisive action to reduce losses from fraud and error, and minimise the risk of reputational damage by strengthening their control environments.

The benefits of fraud measurement go beyond gaining the knowledge of the prevalence of fraud and error. The lessons learned from these exercises can enhance business processes in organisations, delivering wider value. For example, fraud measurement:

- improves understanding of the fraud that is occurring within the organisation;
- provides evidence of the potential extent of fraud and error loss which can be expressed as a financial value and/or percentage of spend;
- improves understanding of different functions;
- helps inform the effectiveness of fraud controls;
- informs evidence-based decisions on how to manage fraud; and
- helps measure the effects of interventions, including prevention activities.

At a programme level, fraud measurement helps:

- identify the types of fraud that are happening, and how big of a challenge it is;
- inform evidence-based decisions on how to prioritise and deploy proportionate counter fraud resources and capabilities (explained in the next section); and
- measure any effects from changes in scheme design, controls, policy etc. to inform any return on investment (ROI) calculations, support new counter fraud investment cases, and potentially help develop prevention savings methodologies.

Taking proactive action to measure fraud and error will greatly benefit organisations and officials who are accountable for managing fraud risk, helping them make more informed decisions about their risk appetite and tolerance.

Why do we talk about fraud and error in Fraud Loss Measurement?

Whenever a payment is made or income is charged incorrectly, even if it was a genuine error, it demonstrates that fraud could take place – because an individual with intent could theoretically take the same process route to obtain funds or avoid charges.

Concluding whether a particular incorrect payment was fraud, rather than error, can sometimes be straightforward, even based on relatively limited evidence. Often, however, distinguishing between the two requires more information that can reasonably be obtained in an FLM exercise.

Whenever a payment is made or income is charged incorrectly, even if it was a genuine error, it demonstrates that fraud could take place.

Identifying the necessary intent required to prove fraud, even to a civil standard, can require the use of investigative powers. However, the use of such powers to prove fraud goes beyond the objective and scope of a FLM exercise. In FLM, reasonable conclusions can be drawn based on the balance of probabilities, without the need for investigatory resources and powers.

Crucially, the business actions typically taken after the exercise are the same whether the result is fraud or error: the aim is to fix the process to reduce the risk exposure. In our example above, the priority is recovery of the overpayment and consideration of how to prevent similar overpayments in the future through improved controls.

The fraud loss measurement exercise places a monetary value on the 'leakage'. The business response should be to plug the leak, thus ensuring better value for money for taxpayers.

Case Study

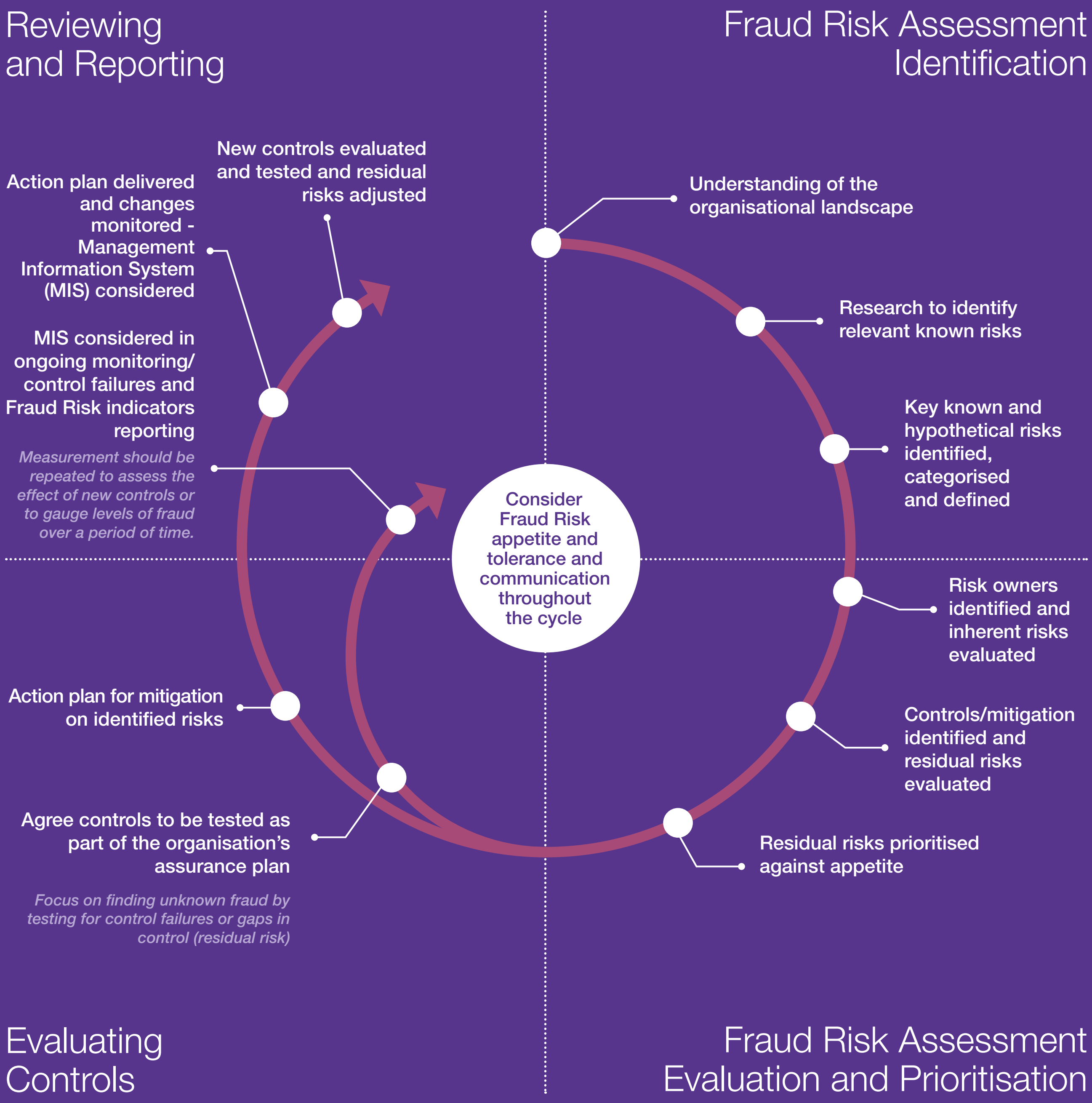
Evidence gathered shows that an inaccurate statement was made in an application for a disability support grant. The applicant stated in the form they would be purchasing a particular model of supportive equipment, but the evidence showed they benefitted by buying a cheaper model. It is clear there was an overpayment, and the applicant states in a telephone interview it was an unintentional error.

This could still have been an intentional act, but to determine whether this would constitute fraud on the balance of probabilities would require further investigative checks into both the applicant and the background of the application, which may not be proportionate.

The Fraud Risk Management Cycle

The below diagram sets out the Fraud Risk Management Cycle and highlights how fraud measurement is an integral part of the overall process.

The first half of the Fraud Risk Management Cycle relates to Fraud Risk Assessment (FRA). The second half deals with the management of the fraud risks (by the fraud risk owner) that have been identified through the FRA process.



Fraud Risk Assessment Identification

Understanding of the organisational landscape

Research to identify relevant known risks

Key known and hypothetical risks identified, categorised and defined

Fraud Risk Assessment Evaluation and Prioritisation

Risk owners identified and inherent risks evaluated

Controls/mitigation identified and residual risks evaluated

Residual risks prioritised against appetite

Evaluating Controls

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

Focus on finding unknown fraud by testing for control failures or gaps in control (residual risk)

Action plan for mitigation on identified risks

Reviewing and Reporting

Measurement should be repeated to assess the effect of new controls or to gauge levels of fraud over a period of time.

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

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

New controls evaluated and tested and residual risks adjusted

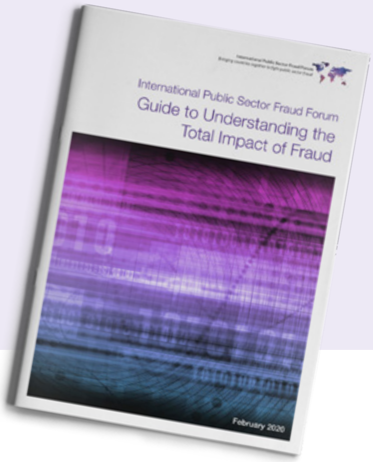
Consider Fraud Risk appetite and tolerance and communication throughout the cycle

Part of managing fraud risks includes understanding and measuring how much fraud is occurring within a particular scheme or activity. This requires ensuring that Management Information (MI) processes exist to record each instance of fraud that is either picked up before the payment is made (or the correct level of income is requested) by a preventative control, or found after payment or receipt by a detective control.

However, even in the most mature counter fraud response, there will be instances of fraud that remain undetected, and therefore unreported. This will either be through existing controls not operating as intended or through the gaps between controls (residual risk) as identified in the FRA.

Effective management will also include being able to estimate what those unreported losses might be. This is where FLM comes into play. Quantifying residual fraud risk helps risk owners make better informed decisions about their fraud risk tolerance. This in turn helps Counter Fraud Professionals work with business stakeholders to draw a conclusion on whether the control environment is mitigating fraud risk within the level of tolerance.[4]

It is also beneficial to consider the non-financial impacts of fraud when measuring residual risk. The IPSFF Guide to Understanding the Total Impacts of Fraud discusses the different impacts of fraud against the public sector, including human impacts, reputational damage and industry impacts.


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

Governance arrangements[5]

To ensure that the results and reported outcomes from FLM exercises can be compared both across different programmes and areas of spend within an organisation[6], as well as more broadly across the public sector, it is necessary to ensure that there are appropriate governance processes in place.

These should build upon the broader governance arrangements in place within your public body for managing risk (including fraud risks) based around the three lines of defence model[7].

[4] Evaluating Internal Control Systems, The Institute of Internal Auditors Research Foundation, 2014, p. 43.

[5] See also Guidance in Element 4 'Governance Commonwealth Risk Management Policy and Element 8 'Reporting and Recording Fraud and Corruption' (AU).

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

[7] Three Lines of Defence (2013; updated 202) model developed by the Institute of Internal Auditors.

Fraud Measurement across the three lines of defence

The governance arrangements within an organisation should identify the functions responsible for Fraud Measurement, including establishing objectives, roles and responsibilities, guidance on processes and procedures, and a consistent oversight and reporting regime for activities across different business areas.

While this Framework is primarily designed for Counter Fraud Professionals, the following outlines how Fraud Measurement can be deployed in different ways across the three lines of defence:

First line of defence

The first line of defence are the business areas that own and manage fraud risks. Fraud measurement builds on the work begun with fraud risk assessment and can be undertaken either independently of, or alongside fraud control testing, to apply a further layer of assurance on the effectiveness of fraud controls and measure residual risk. This enables managers and staff who are responsible for managing risk to apply their business knowledge or technical expertise to effectively evaluate residual risks.

Second line of defence

The second line of defence often involves a centralised area that oversees or specialises in compliance and/or the management of risk within a particular business area (including fraud risk), e.g. those working in Counter Fraud.

These areas can apply their knowledge of fraud risks and enablers to support the first line of defence to identify and assess specific fraud risks, test the effectiveness of fraud controls and measure the extent of fraud losses in specific high risk areas. This co-delivery approach enables the second line of defence to apply more specialised and consistent selection, sampling and testing methods, while also benefiting from the business area's understanding of complex or discrete processes and procedures, and the environment in which they operate.

Third line of defence

The third line of defence are the functions that provide independent assurance, e.g. internal audit functions with responsibility to assess the operational effectiveness of risk management frameworks and processes.

The third line of defence can work in combination with the second line to oversee and coordinate fraud measurement exercises to measure residual fraud risks in order to provide quantifiable estimates of fraud and error within identified high risk areas of spend.

Data governance

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

Fraud Measurement Function

Data integrity

FLM activities must be designed to ensure that data is not changed or modified during, or as a result of, the fraud loss measurement exercise being performed. This will enable fraud loss measurement to be repeatable and assists 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 modify 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 is 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 entity's data strategy and environment[8].

[8] For further information, see: (AU) Commonwealth Fraud Prevention Centre, Fraud Data and Analytics Leading Practice Guide.

Attributes needed to conduct Fraud Loss Measurement exercises

The attributes, such as skills and training, required for FLM will depend largely on the type of processes and testing methods that public sector entities intend to use.

Introductory skills and experience

The requisite skills and training to be able to effectively plan for and undertake a FLM exercise[9] build on those needed to conduct fraud risk assessments and fraud control testing, including:

- **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 utilise this knowledge during a FLM exercise to identify potential fraud risk indicators using evidence.
- **Risk assessment** – an understanding of how to identify inherent and residual fraud risks, including assessing and evaluating the effectiveness of controls.
- **Planning and prioritisation** – an ability to manage available resources, and identify requirements and dependencies, to effectively plan and prioritise each stage of a FLM programme.
- **Business knowledge** - skills and experience in utilising 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 effective testing and sampling methods to undertake a FLM exercise.
- **Critical analysis** – an ability to break down complex information and processes, apply critical thinking, distinguish between relevant and irrelevant information or evidence, be curious, ask questions, challenge assumptions, and think like a fraudster to identify residual fraud risks.
- **Communication and facilitation skills** – an ability to effectively utilise a range of techniques (structured and unstructured interviews, workshops, presentations, data visualisation and meetings) to engage key stakeholders in the fraud risk management process, to prepare well defined and clearly-written plans and draft reports of FLM exercises and other documentation to support logical and succinct analysis and recommendations, conforming with relevant standards, policies and procedures.

[9] Adapted from Section C 'Professional Standards and Competencies for the Fraud Measurement Discipline, (UK) GCFP Professional Standards and Guidance: Fraud Measurement (See Annex to request the Standard).

- **Statistical sampling** - knowledge of statistics and understanding and implementing various sampling techniques appropriate to the analysis required.
- **Identifying and using evidence to test for fraud** - the skills needed to identify, collect, record and store data and evidence in a correct and lawful manner, including designing tests to use this data to be able to test whether fraud has occurred.
- **Estimation and measurement** – an understanding of various techniques to estimate and measure instances of fraud and error, including methodologies to calculate future (prevention) savings.
- **Record keeping and reporting** – an ability to collect and document evidence to provide credible, fact-based research, analysis and interpretation of test results, and report outcomes and conclusions from fraud measurement activity (including the capture of what is already known and detected, actual losses and what has been recovered or prevented).

Advanced skills and expertise to support Fraud Loss Measurement exercises

Because of the complexity of FLM exercises, organisations should ensure anyone working in this area possesses the requisite knowledge, skills and abilities to fulfil their responsibilities:

- Knowledge of theories, principles, practices, and techniques of investigation and the education, ability, and experience to apply such knowledge to FLM exercises, including the identification of appropriate evidence for testing and the interpretation and categorisation of results.
- Knowledge of government organisations, programs, activities, functions, and, where applicable, their interrelations with the private sector.
- Knowledge of applicable laws, rules, and regulations such as those relating to privacy, freedom of information, data handling and protection, whistleblower protection, protective security and information.
- Ability to exercise tact, initiative, ingenuity, resourcefulness, and judgement in assessing and communicating fraud risks, collecting and analysing facts, evidence, and other pertinent data for undertaking FLM exercises.
- Ability to deliver clear, concise, accurate, and factual summaries of testing plans, processes and results, both orally and in writing[10].

Organisations will often need to commission additional support to undertake either a larger or more complex programme of FLM, such as specific technical knowledge required to complete testing and complex data analysis (including from specialists across the public and private sector).

For example:

Statisticians[11] - qualified statisticians will be able to provide guidance and insights on what is a proportionate and statistically valid sample size for testing in order to ensure that any results can be used to extrapolate across the whole of the population.

Data scientists and analysts[12] - for more advanced FLM exercises with larger sample sizes and big datasets for testing, advice and support from data scientists can help make your exercise much more efficient.

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

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

[11] Advice on sample size and selection can be given by qualified Statisticians from the (UK) Government Statistical Service (GSS); (AU) Australian Bureau of Statistics

[12] (UK) Government Operational Research Service (GORS)

Integrity, Character and Resilience

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

It is important that those engaged in FLM exercises 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[13].

They should produce reliable, high quality analysis, ensuring knowledge of related guidance and standards such as those for Fraud Risk Assessment[14], Control Testing[15] and Data Analytics[16], and the counter fraud context in which they are being applied, are up to date. As professionals they should recognise and be proactive in taking action to address any gaps within their own knowledge. They should also note any perceived gaps or weaknesses in the standards and guidance they follow, and should communicate these to those setting the standards.

Those working on FLM should continuously consult, engage and work with others in the organisation to ensure that reporting, analysis and estimation provide useful insight for counter fraud decision making, including informing the counter fraud strategy, and helping the achievement of counter-fraud outcomes.

The analysis produced should have an impact, and how that impact affects others in the counter fraud area and the wider business should always be considered when results are communicated.

They should demonstrate the utmost professionalism and personal resilience throughout the planning, testing and reporting process, recognising that fraud measurement will often involve delivering difficult messages to senior stakeholders across multiple lines of business. This will necessitate careful handling and tact to be able to optimally manage any negative reactions, while still taking care to remain impartial and objective in presenting the evidence-based findings and conclusions.

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.

The outputs from fraud loss measurement exercises will often be challenging for stakeholders to receive. Higher than expected fraud levels can be interpreted very negatively by business areas. Lower than expected fraud levels can provoke a negative reaction from counter fraud colleagues. It is common to experience strong challenges and resistance to accepting the findings.

This means those working on fraud measurement exercises must be both resilient - capable of seeing the bigger picture when receiving negative feedback and also confident in the credibility of the method which produces the results.

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

[14] (UK) Government Counter Fraud Profession (GCFP) Fraud Risk Assessment Standard, (AU) Fraud Risk Assessment Leading Practice Guidance

[15] International Public Sector Fraud Forum (IPSFF) Fraud Control Testing Framework

[16] (AU) Fraud Data Analytics leading practice guide

Guidance for Fraud Loss Measurement exercises - how to create a process

Business Drivers

Analysis of the UK evidence base on Fraud Measurement has shown there are three distinct business drivers for why a FLM exercise might be undertaken. They are labelled as ’Exploratory’, ‘Performance’ and ‘Assurance’. These drivers inform the purpose and objectives of the exercise, and the approach that should be taken.

Business Drivers

Exploratory

This approach looks at a spend (or revenue) area for which little or no fraud is currently being reported. The purpose is to undertake a FLM exercise to identify if unknown losses due to fraud or error are occurring, and to make an initial estimate of what these might be.

Performance

In this context, a FLM exercise (or exercises) seeks to provide a reliable estimate of the previously unknown fraud (and error) losses within a particular spend area. This involves testing the vulnerabilities and exposure to residual fraud risk, with the intention of reducing the exposure over time through new controls and using the measurement to track the effectiveness of this (e.g. how well the organisation is performing in reducing the fraud level).

Assurance

In this context, the use of FLM exercises sits alongside the testing of controls and provides assurance through ongoing and repeated exercises that the control framework is managing fraud losses within agreed tolerance levels (e.g. assuring that fraud and error is under a certain materiality level). This may be considered proportionate and appropriate to undertake a rolling annual programme of fraud measurement.

The reasons why a FLM exercise is undertaken may vary over time, perhaps starting with an Exploratory exercise and developing into Performance to become an ongoing (often annual) Assurance programme.

User Stories for Fraud Loss Measurement exercises

The below 'user stories', drawing upon insights and lessons learned from the UK Fraud Measurement and Assurance (FMA) programme, give examples of the typical situations in which each of these forms of FLM exercise would be appropriate.

FLM exercises are not always performed for the same business purpose, or in the same way. The variation in technical complexity and resourcing requirements between small scale and large scale exercises is vast.

Exploratory

As the leader of an immature fraud response, I want to conduct FLM work so that I can get a general idea of how much fraud and error there is in my programme.

WHY SHOULD YOU DO AN EXPLORATION MEASUREMENT EXERCISE?
- smaller sample sizes, keeping resourcing light, focussing on key risks.

Performance

As the leader of an established fraud response, I want to conduct FLM work so that the organisation can understand the return on investment on our new fraud controls.

WHY SHOULD YOU DO A PERFORMANCE MEASUREMENT EXERCISE?
- high confidence levels needed, so large sample sizes and wide risk coverage
- you want to be sure you are capturing the impact of your control initiatives.

Assurance

As the leader of a mature fraud response, I want to conduct FLM work to evidence that the level of fraud and error in my programme is below a certain level (e.g. < 1% of spend)

WHY SHOULD YOU DO AN ASSURANCE MEASUREMENT EXERCISE?
- only one side of the test is needed, so you need smaller sample sizes than for Performance, but still with wide risk coverage to capture any novel risks emerging.

“Single Risk” Fraud Loss Measurement exercises

Across all three business drivers for FLM, but particularly ‘Exploratory’, there are potential occasions where it can be worthwhile to consider an exercise based on testing one single fraud risk or thematic risk area (for example, undeclared partners in welfare payments for single persons).

Single risk exercises should only be considered where one fraud risk is of sufficient seriousness in its own right to be impacting the programme or organisational objectives.

Single risk exercises can be easier to conduct and typically require lower levels of resourcing. As such, they can be a good way to tackle emerging fraud problems. This can be particularly useful where there is a long wait time for the results from annual programmes of fraud loss measurement that are already in place in mature organisations and only produce results once a year.

Care should be taken to avoid presentation of ‘single risk’ exercises as if they are a measurement of the fraud and error level in a whole scheme or programme. A single risk fraud loss measurement exercise will **always** be an underestimate of the total level of fraud and error in the area overall.

Fraud Loss Measurement exercises - an overview

1 Area Selection

Complete or review Enterprise level FRA/Strategic Fraud Risk Profiling Tool.
Identify a suitable scheme or spend area.

2 Residual Risk ID

Complete or review a (full) fraud risk assessment.
Identify evidence to test residual risks.

3 Planning, Sampling and Initial Evidence

How we look for instances of fraud - including selection evidence.
Identify a sample and map out how data and evidence will be gathered.

4 Testing

Undertake testing on all cases in the sample.
Interpret results and reach a conclusion on each case.

5 Reporting and Next Steps

Produce a report with recommendations.
Results used to inform Counter Fraud & Integrity Strategy and public sector fraud and error evidence base.

Stage One - area selection

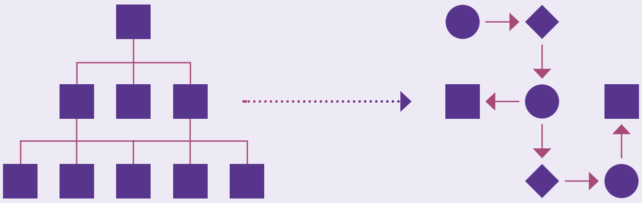
This step requires officials to identify high risk areas of business that are suitable for a FLM exercise.

Choosing which areas of fraud risk to focus on

It is impractical and inefficient for public bodies to measure losses to fraud and error in every area of residual risk.

This expectation would ultimately lead to a "mile wide, inch deep"approach, diminishing the assurance value and insights fraud measurement can produce and resulting in low value and purpose of Fraud Loss Measurement.

Therefore, public bodies should aim to focus their effort and resources on those areas of **highest fraud risk impact** and where it is **possible to use evidence to test for fraud**.



Public Sector organisations should use their Enterprise (Organisational) Fraud Risk Assessment or their own analysis to identify where fraud is most likely to be found, and therefore where FLM exercises will add the most assurance value by looking for and measuring instances of undetected fraud.

Strategic-level fraud risk profiling can assist an organisation to identify those areas of the organisation that are at higher risk of fraud. This will enable counter fraud professionals to formulate a 'heat-map' for fraud risk across the organisation, and to schedule fraud risk assessments on a prioritised basis.

An area is suitable for selection for a FLM exercise if:

- there are significant residual risks of fraud and error, and
- there is likely to be sufficient evidence available, which can be used to validate whether fraud or error has occurred.

Public Sector organisations should use their Enterprise (Organisational) Fraud Risk Assessment or their own analysis to identify where fraud is most likely to be found.

An “area” selected for a FLM exercise can cover any process by which an organisation pays out expenditure or receives income. Expenditures can be payments directly to the public, or to third party contractors that provide services to the public. They can also include payments to public sector employees to provide services. Some examples of expenditure include grants schemes, contracted procurements, or means-tested services; whereas examples of income include fees, levies and charges.

It is important to remember that the areas selected should generally be ones considered to have a high risk of fraud and error loss.

Consideration should be given to the total spend profile of the area, existing Fraud Management Information (i.e. whether intelligence, quality assurance work or other reporting indicates fraud and error is present) and what is known regarding the efficacy of the existing control framework.

FLM Process Stage 1 - Area Selection

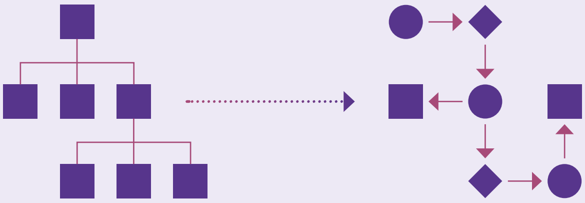
Identify a scheme or programme/spend area (entity level)

The point of area selection is to select an area:

- that has significant residual risk
- where little is known about the levels of fraud
- it is possible to use evidence to test for fraud

What is the ideal way to identify a suitable area for measurement?

- Enterprise (or thematic) fraud risk assessment
- Strategic Fraud Risk Profiling Tool



The following supporting guidance and documents, published by the Commonwealth Fraud Prevention Centre in Australia, are available to assist you in undertaking a Stage One area selection exercise:

- Information Sheet - Element 1: Fraud and corruption risk assessments
- Fraud Risk Assessment Leading Practice Guide
- Strategic Fraud Risk Profiling Tool[17]

[17] See also guidance in Element 1 and Fraud Risk Assessment Leading Practice guide.

Stage Two - identifying residual risks for testing

It is necessary to carry out a Fraud Risk Assessment (or review an existing one) to both identify the specific residual fraud risks within the area selected for a FLM exercise and also understand how these can be tested.

Fraud Risk Assessments (FRA) are key to understanding how fraud, bribery and corruption could be occurring within the area selected. The four process steps within the FRA process are detailed within the Fraud Risk Assessment Leading Practice Guide. It is vital to have a deep understanding of the eligibility (or payment) criteria for the area concerned, and how specific frauds could occur based on those criteria.

> The eligibility criteria for a disability support grant states that a payment can only be made for the installation of equipment with specific model numbers. The key control against this is that 5% of installations will be randomly selected for inspection to check the installation took place with an approved model number. Residual risk remains when the fraudster is not selected for an inspection.

There is a further step that is necessary when conducting a FLM exercise, which is to specifically analyse how the prioritised residual risks identified in the FRA could be tested. This is a creative exercise which involves thinking about exactly what data, or evidence, is needed to establish whether the residual risk has materialised.

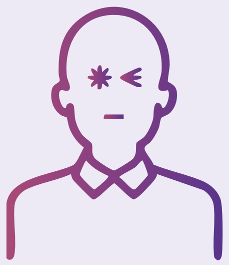
As such, it may be necessary to plan to seek engagement and input from across multiple different parts of the organisation, including risk and process owners, using a workshop led approach. For the purpose of the FLM exercise, this should be done in a similar fashion to how you would approach and manage a typical fraud risk identification workshop, but with additional considerations and questions to help inform the selection of residual risks and appropriate sources of evidence for testing.

Fraud Risk Assessments (FRA) are key to understanding how fraud, bribery and corruption could be occurring within the area selected.

Adopting the mindset of a fraudster

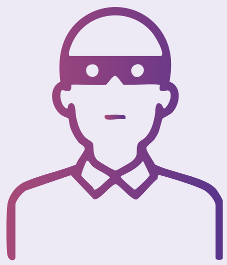
The way fraudsters operate varies in complexity and creativity. They range from opportunistic individuals taking advantage of weak controls, such as a lack of oversight, through to determined individuals or organised groups deliberately probing for ways to exploit programs and schemes, and creatively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

The following Fraudster Personas[18], developed by the Commonwealth Fraud Prevention Centre, gives Counter Fraud Professionals and business stakeholders practical direction on how to adopt a fraudster's mindset. In particular, they help those working on FLM exercises to consider ways fraudsters may be bypassing controls and identify evidence of whether fraud is occurring.



The Reckless

The Deceiver

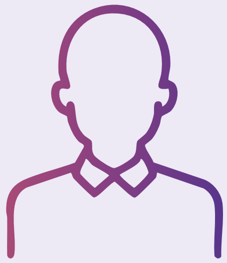


The Impersonator

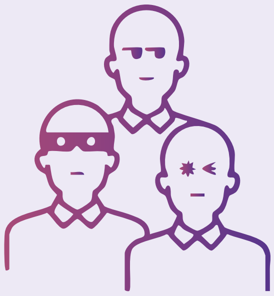
The Fabricator

The Coercer

The Exploiter



The Concealer



The Organised

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

[18] https://www.counterfraud.gov.au/discover-different-types-fraudsters

Data and evidence analysis

Testing the extent to which the residual risks are materialising involves analysing available evidence on a sample of cases. The degree to which this can be determined will depend on what evidence exists to indicate fraud, and the availability, completeness and quality of the data.

Evidence or comparator data can be categorised into three types:

- internal data or evidence collected or held by the organisation and used in the decision process or at payment,
- internal data or evidence collected or held by the organisation but that is external to, or not used by, the decision process or at payment, and
- external data or evidence external to the organisation not used in the decision process or at payment.

Once evidence has been identified you must evaluate it for availability, quality and completeness. This helps ensure you understand the limitations of the evidence when undertaking testing and drawing conclusions.

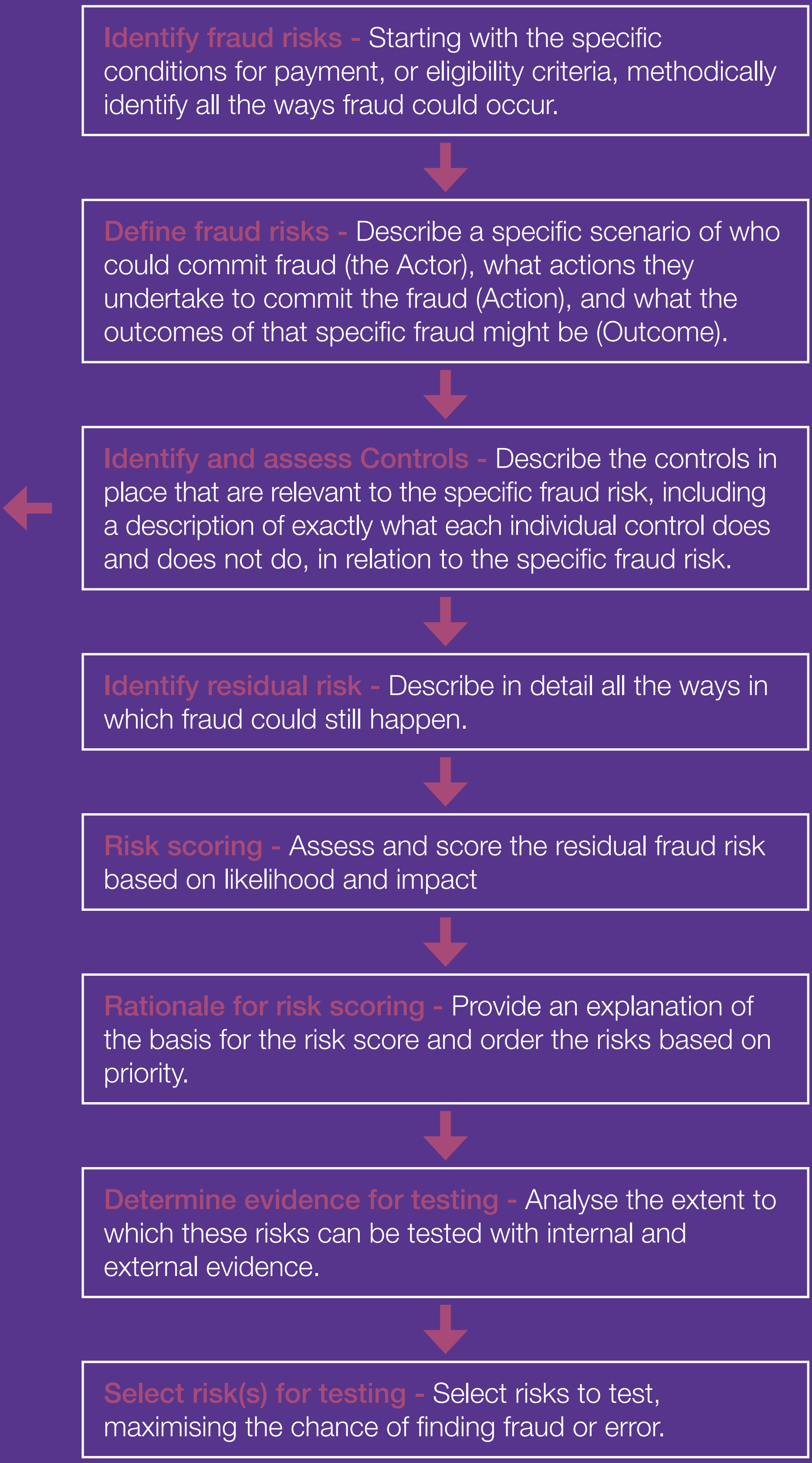
The quality of the evidence includes its accuracy, age, reliability etc, and how it is compiled and stored. If the evidence used for testing is out of date, was collected in an unreliable way, or is too ‘high level’ (general/ non-specific) to be useful for measurement purposes, then it is unlikely to be helpful in producing a reliable estimate of fraud and error losses.

Based on the evidence available, specific risks should be selected to test. The number of risks selected should be achievable based on the purpose of the exercise (i.e. exploratory, performance, or assurance) and available resources. All of the work up to this point is to increase the level of certainty that you can find and confidently determine if fraud or error has occurred within the sample. Investing effort in the foundation will yield improved efficiency and efficacy in the subsequent stages.

If the evidence used for testing is out of date, was collected in an unreliable way, or is too ‘high level’ to be useful for measurement purposes, then it is unlikely to be helpful in producing a reliable estimate of fraud and error losses.

A process flow

Common fraud control types guidance from the Commonwealth Fraud Prevention Centre



Identify fraud risks - Starting with the specific conditions for payment, or eligibility criteria, methodically identify all the ways fraud could occur.

Define fraud risks - Describe a specific scenario of who could commit fraud (the Actor), what actions they undertake to commit the fraud (Action), and what the outcomes of that specific fraud might be (Outcome).

Identify and assess Controls - Describe the controls in place that are relevant to the specific fraud risk, including a description of exactly what each individual control does and does not do, in relation to the specific fraud risk.

Identify residual risk - Describe in detail all the ways in which fraud could still happen.

Risk scoring - Assess and score the residual fraud risk based on likelihood and impact

Rationale for risk scoring - Provide an explanation of the basis for the risk score and order the risks based on priority.

Determine evidence for testing - Analyse the extent to which these risks can be tested with internal and external evidence.

Select risk(s) for testing - Select risks to test, maximising the chance of finding fraud or error.

Stage Three - Planning, sampling and gathering initial evidence

Guide to successful planning

Effective and consistent planning can be supported by a template similar to the following, found within the IPSFF Fraud Control Testing Framework suite:

FCTF-08 - CEA Testing Approach Planner

FCTF-08A - Executive CEA Plan Template

PTSF-02 - Pressure Testing Plan Template

Plans should clearly define and document the scope of the exercise, including the following considerations:

- consistency of decision-making - a documented process (including recording rationale for decision-making) should be used to facilitate quality assurance through reperforming the tests
- use of third parties - external audit is appropriate when there is a greater need for accountability, transparency and regular oversight.

The plan should identify an achievable number of fraud risks to be tested on the desired sample, and should include:

- how each fraud risk will be tested using what evidence
- how the sample selected is representative of the population
- how the evidence chosen for testing helps conclude whether a transaction was correct or irregular (i.e. either fraud or error)
- how the testing will enable any fraud or error found to be quantified.

The testing plan should aim to assign each case one of the following classifications[19]. It is acknowledged that these are based on UK specific terminology, and that different jurisdictions should use their own equivalent terminology when describing classifications whilst seeking to align as far as possible with the thematic groupings below-:

- **Regular transactions** - there is sufficient evidence to demonstrate that the transaction within the sample was valid, and that no fraud or error was present.
- **Fraud** - the key element for identifying fraud is intent. Where there is, on the balance of probability, evidence that a case or transaction is irregular through dishonest or fraudulent intent, then it should be recorded as ‘fraud’.
- **Error** - there is evidence of irregularity, but sufficient evidence on the balance of probabilities that there was no intent to defraud.
- **Indicators of Fraud** - evidence shows a case or payment as irregular and the possibility of fraudulent intent remains, but the available evidence is less than the civil standard ‘balance of probability’ test, then this should be recorded as ‘indicators of fraud’.
- **Unresolved cases** - no available evidence to determine the correctness of a case or payment, or the evidence indicates a case or payment may be irregular but this cannot be positively determined.

Cases determined to be fraud, error, or categorised as (exhibiting) ‘indicators of fraud’ are bracketed together as ‘irregularity’. Cases that are unresolved should not be included in any calculation of fraud and error level - they are neither regular, nor irregular.

[19] (UK) ‘Professional Standards and Competencies for the Fraud Measurement Discipline, GCFP Professional Standards and Guidance: Fraud Measurement Standard Section E4 p85 (See Annex to request the Standard).

Sample selection - choosing statistically valid samples for testing

While it would be ideal to be able to test every single payment for potential fraud, in reality this is impractical or too resource intensive to achieve. Fortunately, a sample of the population, if properly selected, can still provide an accurate estimate with significantly less effort and resources.

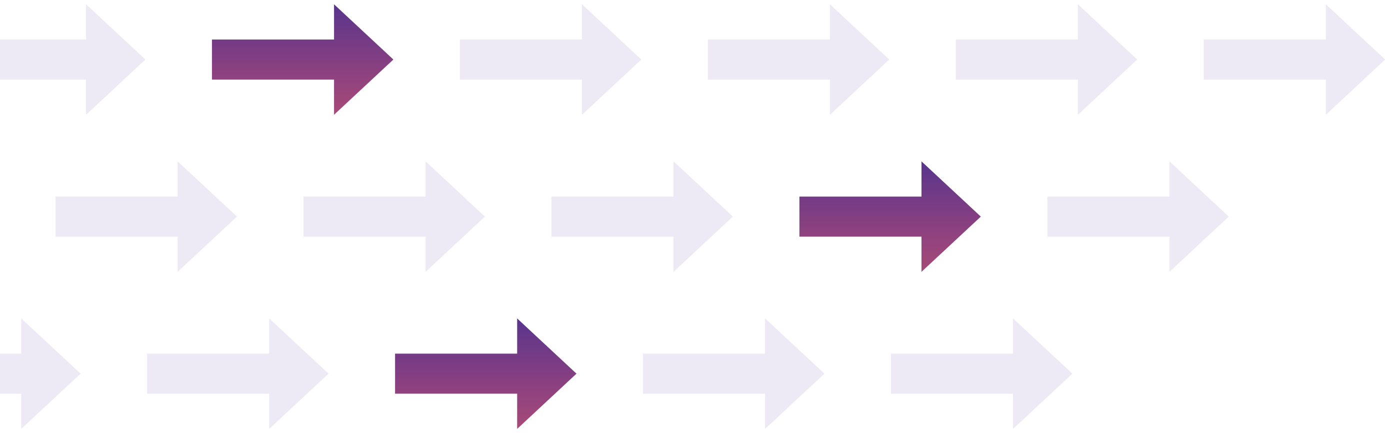
The key principle with statistical sampling is to ensure that any results derived from testing can be applied and interpreted to the population from which the sample was drawn. Therefore, the **sample selected** using a methodology that allows it to be representative of the target population.

Any sample must also be of a sufficient size to realistically reflect all the characteristics of that population, and to allow the accuracy of the findings to be established within defined margins of error.

All methodologies should:

- include some degree of randomisation
- involve a ‘probability’ sample where any unit within the population has a known, non-zero, chance of being chosen
- be supported by clear and evidenced justification.

A sample of the population, if properly selected, can still provide an accurate estimate with significantly less effort and resources.



Determine the sampling methodology

Different methodologies can be used depending on the characteristics of the area being tested and resources available. It is important to consider the advantages and disadvantages of each methodology presented below:

Simple Random Sample

A simple random sample uses a selection of random numbers that is equal to the number of items needed in the sample. These are often chosen using a random number generator function in applications such as Microsoft Excel.

Items within the population are chosen depending on whether their position in the population is matched by a generated random number. It is important to ensure that the range of possible random numbers allows coverage of the entire population being sampled.

A simple random sample may be the most appropriate sampling method to use for FLM where the whole population is smaller, have similar attributes and are geographically evenly distributed.

Advantages	Disadvantages
• Easy to implement • Each member of the population has an equal chance of being chosen • Free from bias	• If the sampling frame is large then random sampling may be impractical • Minority subgroups within the population may not be present in the sample • Testing may be disproportionately resource intensive if, for example, site visits are required and a relatively small sample has a wide geographical spread

Systematic Sample

For this sampling method, all data is sequentially numbered and every ‘nth’ piece of data is chosen. This is calculated using the below equation.

$$n = \frac{\text{size of population}}{\text{desired sample size}}$$

Advantages	Disadvantages
• Easy to select sample • Evenly spread sample over the entire population • Minimises the clustering of particular attributes	• May be biassed when the pattern used for the samples coincides with a pattern in the population. • Can be at greater risk of data manipulation than other methods

Stratified Sample

In stratified random sampling the population is divided into sub-populations (strata) and random samples are then taken from each stratum. The strata are based on specific characteristics, for example: geographic regions, age, gender or race. Within the strata, random sampling is used to choose the sample.

Stratified sampling may be the most appropriate sampling method in instances with a larger whole population size and where the choice and selection of strata is based on a belief/evidence that the characteristics of each sub-population could result in differing levels of fraud or error, and use of this technique requires knowledge of the population composition. A fraud measurement practitioner could, for example, stratify payments by value, by geographical location or by preconceived risk ratings around a particular characteristic.

If certain strata are known as 'high risk' for fraud and error, a fraud measurement practitioner may use 'weighting' to 'over-sample' those strata and 'under-sample' other strata with a lower risk of fraud and error.

What this means is that while individual cases are still randomly sampled, more will be selected from high risk strata and fewer from low risk strata. However, care needs to ensure that test results are interpreted for each stratum first before aggregating to reflect the overall population.

Advantages	Disadvantages
• Strata can be proportionally represented in the final sample • It is easy to compare subgroups • Can be used to target sub-populations for testing which can be particularly advantageous if site visits are required (e.g. choose your strata to focus on particular locations to reduce costs)	• Information must be gathered before being able to divide the population into subgroups • If assumptions around the strata are inaccurate (e.g. that there is the same risk of fraud regardless of geographic location), this will give biased results. • Care should be taken when estimating fraud levels for the population when using stratified sampling in cases where all strata are not proportionally represented. • For example, if certain strata are known as 'high risk' for fraud and error, a department may choose to sample just those strata. However, the results can only be used to estimate fraud levels in those strata, not the overall population.

Determine the size of the sample

In determining the size of the sample to be selected, there are two key considerations:

- the degree of confidence that the sample selected accurately reflects the population from which it is drawn; and
- the degree of accuracy to which the results of testing from that sample represent the actual rate of fraud and error within the overall population.

Determining the desired confidence level and margin for error

The aim is to present the level of fraud and error in the sample in terms of confidence level (how confident we are in the finding) and confidence interval (also known as precision, or margin for error). This means 'how confident we are that the measured level is within a particular range of precision'.

A 95% confidence level and a confidence interval of ±1% is generally considered best practice in fraud and error measurement. However, this sample size may not be appropriate for all exercises. If the aim of the fraud measurement is 'for performance', large sample sizes are needed.

A 95% confidence level and a confidence interval of ±1% is generally considered best practice in fraud and error measurement.

If you are conducting exploratory measurement, lowering the confidence level to 80% and the confidence interval to ±5% could be acceptable. You should aim to achieve the highest statistical precision possible, given the resources available[20].

To determine the sample size required at a given confidence level, it is necessary to know or estimate the level of fraud and error (or irregularity) expected from the testing. Often, there may be no initial evidence of the level of fraud and error expected in the areas to be tested (the 'population proportion', or the proportion of the population that would demonstrate the attribute of irregularity). In these instances, it is recommended that a sample size corresponding to a 5% estimated rate of irregularity is used.

The sampling methods set out above are based on identifying **whether an attribute is present in a population or not**, rather than the frequency of its occurrence. In practice this means we are looking at whether a case was a fraud, or not a fraud. The advantage of this is that it will produce sample sizes that are more manageable. The disadvantage is that the samples at the lower end of the spectrum will be less accurate when extrapolated across the overall population to demonstrate the spread of irregular spending. For tests in which it is necessary to test how much of an attribute is present (e.g. some of the payment on the case was regular, some of it was fraud) you should consult a statistician.

[20] (UK) 'Professional Standards and Competencies for the Fraud Measurement Discipline, GCFP Professional Standards and Guidance: Fraud Measurement Standard Section p69 (See Annex to request the Standard)

being tested.

90% Confidence Level

90%

		Precision ±						
		8%	6%	5%	4%	3%	2%	1%
Estimated Irregularity	8%	31	56	80	125	223	501	2004
	6%	24	43	61	95	171	384	1535
	5%	20	36	52	81	144	323	1293
	4%	16	29	42	65	116	261	1045
	3%	12	22	32	50	88	198	792
	2%	8	15	21	33	59	133	534
	1%	4	7	11	17	30	67	270

A small organisation is doing a FLM exercise for exploration. They use a 90% confidence level, a ±5% confidence interval, and a 5% estimated level of irregularity (as there is no initial evidence) = sample size of 52.

95% Confidence Level

95%

		Precision ±						
		8%	6%	5%	4%	3%	2%	1%
Estimated Irregularity	8%	44	79	113	177	314	707	2827
	6%	34	60	87	135	241	542	2167
	5%	29	51	73	114	203	456	1825
	4%	23	41	59	92	164	369	1475
	3%	17	32	45	70	124	279	1118
	2%	12	21	30	47	84	188	753
	1%	6	11	15	24	42	95	380

A large organisation is doing a FLM exercise for performance. They use a 95% confidence level with ±1% confidence interval, and a 2% estimated level of irregularity (based on previous exercises) = sample size of 753.

The table above (based on the simple random sampling for attributes in the UK National Audit Office Sampling guide) provides an idea on different sample sizes required. This approach sets sample sizes based on the likelihood of fraud and error, regardless of the size of the population that is

Choosing a sample size - best practice tips

- Match your sample size[21] to the type of FLM you are aiming for. It should be both representative and of sufficient size to allow any findings to be used to produce estimates of fraud and error across the whole population with a high degree of confidence. The level of confidence you need depends on whether you are looking for exploration, performance or assurance.
- When determining the sample size it is important to consider accuracy against costs in time and resources. If you want to achieve more accurate results and be able to place a higher level of confidence in the conclusions, you will have to select a larger sample size (which will also cost more).
- It is better to focus on depth of testing over breadth of population (sampling) selection. Ensure the testing of individual cases in the sample is done in sufficient depth, rather than having a larger sample size of cases that are tested with less rigour.
- Remember there will always be a trade off between the cost, time and resources invested into any fraud loss measurement exercise, against the usefulness of the work.

Identifying and selecting evidence / test data

Evidence is essential to FLM and is used to check the validity of each attribute or item within the sample. When testing for fraud, each sample needs to be rigorously investigated by examining all information that can be lawfully and appropriately accessed to verify and validate data and information held within the area of spend / income.

The evidence may be in the form of data, obtained either from inside the organisation, from another government organisation, or a third party (either open source or a paid service provider).

It is important that testing involves using evidence from outside the scheme or process being tested. If you only use data that is internal to that scheme or process, it will be more difficult to validate the information and identify any evidence that indicates fraud has taken place. You should seek to obtain all the possible sources of data that offer good value for money when testing for instances of fraud or error.

For guidance on how to plan for data acquisition see the Fraud Data Analytics Leading Practice Guide.

It is particularly important to consider the onward usage permitted with any data obtained for the purposes of conducting a FLM exercise. It may be practical to obtain data for research and policy improvement only22, practitioners should be aware that any such restrictions will constrain the testing from being used for further investigation and enforcement activity.

[21] Advice on sample size and selection can be given by Statisticians from the (UK) Government Operational Research profession (GORS) and the (UK) Government Statistical Service (GSS), or the Australian National Audit Office (ANAO)

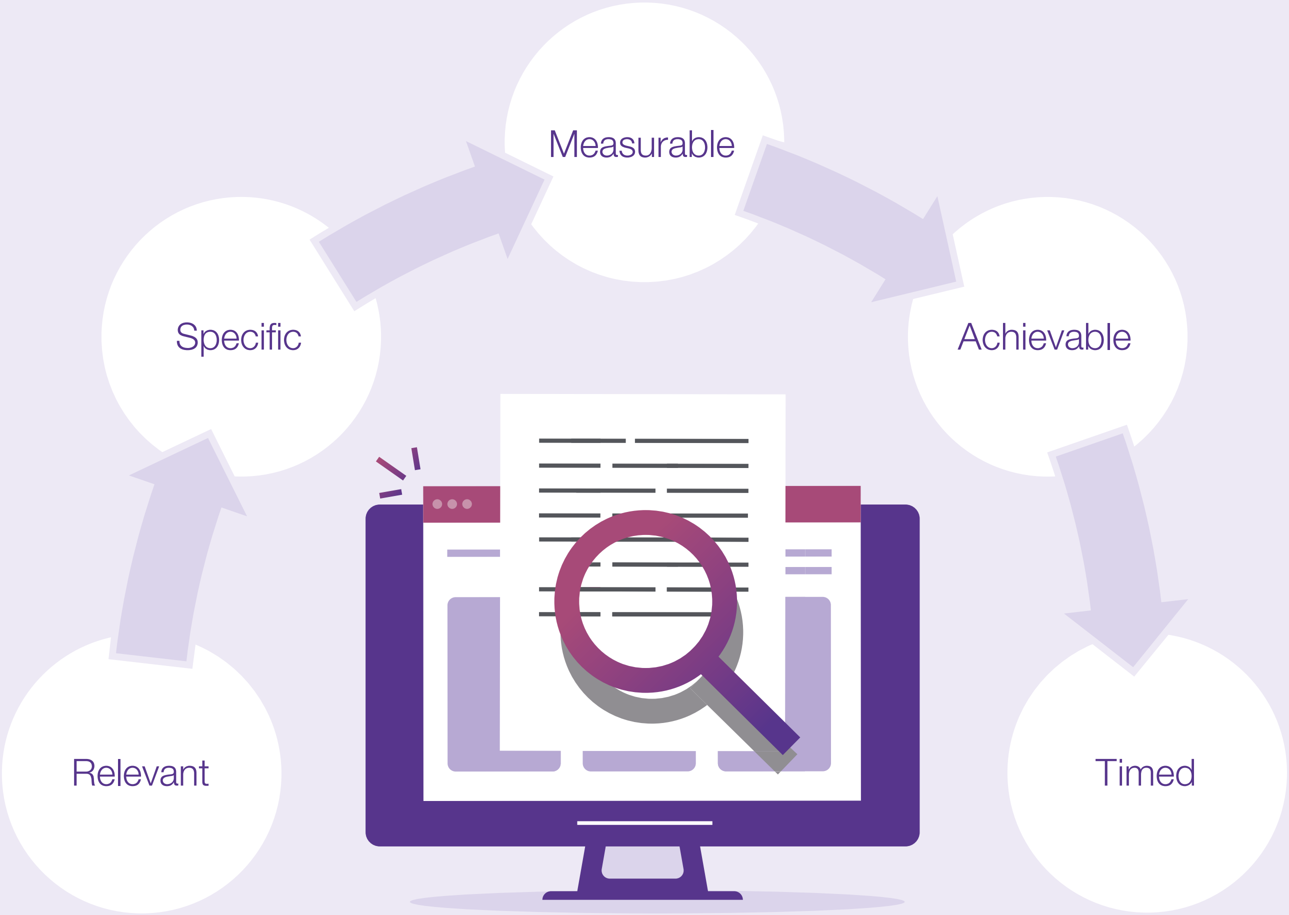
[22] The Australian Data Availability and Transparency Act 2022 enables data to be widely shared and used for three specific purposes, which does not include enforcement:
- Delivery of government services
- Informing government policy and programs
- Research and development.

Data is not the only source of evidence. If physical inspections or site visits are needed, then it is important to adequately plan for this including considering any third-party access dependencies and the impact that any planned site visit involving FLM activity may have upon business as usual. For example, depending on the chosen method of sampling it may be necessary to enlist the support of third party business process owners to help provide access to restricted areas or items, while also working to mitigate the wider impact of any sample selection on business process flow.

If interviews with payees are needed, consider preparing for these by drafting key questions to help the interview process. Consider the technology and type of engagement used (e.g. video call, audio call or a better response can sometimes be received from correspondence).

Evidence Gathering - Top Tips

- Evidence sources should be clearly described and understandable to a non-expert.
- Evidence sources should provide new information that was not used in the original decision making/payment process, or evidence used in the original decision making/payment process should be looked at in a new way, using new techniques (which may include additional comparator data).
- The evidence used should clearly demonstrate that the testing goes beyond just testing that the controls have been applied.
- The evidence sources chosen should, in aggregate, enable a decision to be made on whether fraud or error has occurred.



Stage Four - Conducting the testing

The testing stage of a FLM exercise involves methodically reviewing each case for evidence of the selected risks.

Based on the review, each case is then given one of the following five classifications:

- Regular transactions
- Fraud
- Error
- Indicators of fraud
- Unresolved.

It can be beneficial to start with the premise that every unit in the sample is irregular and seek to find sufficient proof that they can be validated as regular, and if not, they must continue to be considered as potentially irregular with additional testing required.

If no further tests can be identified and it is not possible to make a decision, then the sample item should be classified as 'unresolved'[23]. Unresolved cases are normal in a FLM exercise, and having zero unresolved cases can sometimes be an indicator of poor quality measurement work.

When conducting testing, it is vital to think about what the evidence is telling you and what it is not telling you.

Risk: In a support grant solely for single persons, the payee fails to inform the organisation of a change in circumstances, and continues to receive the grant after an additional person has started living at the property.

Comparator data: Credit reference data or similar information provided by credit reference agencies; benefit agency data; driver licencing, vehicle tax or insurance records; tax authority records.

Test: Check to see if there is a financial footprint of someone else at the same address.

You should note that the evidence might suggest fraud, but it is unlikely to be conclusive. For example, a person could live on their own but an older child might have a car registered at the address which would flag up as an anomaly if that was being used as comparator data. This would give an 'indicator of fraud' but further testing would be needed to establish the actual address of the child to determine whether fraud was actually occurring.

Different levels of testing are required to be able to definitively classify a case as fraud. Testing of the sample might find some which can immediately be classified as regular transactions. This will leave a smaller number where the possibility of fraud is indicated, and further testing will then be undertaken on that smaller number. An initial review may enable you to concentrate on more expansive and expensive types of testing, for example highlighting cases in which a site visit is needed.

One way to achieve this is to structure testing in a series of distinct phases, where a provisional classification is made and revisited at each subsequent phase:

- **Phase 1** - Initial review based on internal evidence
- **Phase 2** - Secondary review based on internal and external comparator evidence
- **Phase 3** - Further review based on cases where further evidence is needed
- **Phase 4** - Final review where no further evidence can be gathered and a determination must be made.

[23] (UK) 'Professional Standards and Competencies for the Fraud Measurement Discipline, GCFP Professional Standards and Guidance: Fraud Measurement Standard Section p64 (See Annex to request the Standard)

> An initial review conducted on a disability support scheme payment for the over 60's shows that all appears correct **(provisionally regular)**.
>
> A secondary review based on comparator data from other government organisations shows the payee has different dates of birth registered with different organisations which show he is under 60 **(provisionally indicators of fraud)**.
>
> A further review is conducted based on correspondence with the applicant, including an email in which he says he is not sure what he entered on the form **(provisionally indicators of fraud)**.
>
> A final review is then conducted based on a recording transcript of a telephone interview in which the applicant confirms he made a false representation about his age in order to receive the payment **(final decision: fraud)**.

It is important to ensure that there is an agreed and documented decision-making and recording process. Those overseeing the FLM exercise should also regularly check in with those doing the testing to stay informed of what they are finding, and in particular should pay attention and monitor for high levels of 'unresolved' cases which could otherwise undermine confidence, and inhibit any ability to draw meaningful conclusions from the results of the exercise.

Once all the phases of testing for fraud and error have been completed it is necessary to **collate the results**. The first step is to group the classified cases into the following categories:

Regular transactions	
Irregularity	Fraud
	Error
	Indicators of fraud
Unresolved cases	

'Fraud', 'indicators of fraud' and 'error' are bracketed together in the 'irregularity' category for reporting purposes. The reporting should include the number of instances out of the sample attributed to each classification and also the monetary value.

Testing - Top tips

- The initially gathered evidence alone is rarely sufficient to make a determination; testing should follow where the evidence dictates and seek further information to make a good decision.
- The aim is to test with as much rigour as possible, however it is important to note the overall limitations to what can be tested, including recording any consideration given to how these limitations could be overcome (e.g. we were unable to speak to an applicant; we didn't have a mandate to collect the required data etc).
- In the working papers, the reasons for deciding whether fraud or error has occurred should be clearly explained in a way that is understandable to a non-expert.
- It is important to ensure that the decision-making process for reaching conclusions on whether fraud or broader irregularity have occurred within an individual sample are applied consistently across the whole exercise.
- There should be a clear audit trail enabling the testing to be reperformed (e.g. by another member of the team) for quality checking purposes.

Stage Five - Reporting and next steps

Extrapolation

Once the testing is complete and each case in the sample has been classified and categorised, the findings can be extrapolated. To do this, the overall results of the testing (the percentage of cases in each category) are considered in terms of confidence level and confidence interval.

For example, a finding of 3% irregularity in the sample with a precision of ±1% allows an estimation that the 'true' value of fraud and error within the overall population is within the range of 2% - 4%.

The third step is to calculate what this means in terms of the value of the population as a whole, and also the number of transactions or items within that population. For example, if the monetary value of the population was £1m, and it involved 10,000 transactions then it can be estimated that the monetary rate of irregularity would be within the range of £20,000 to £40,000; and that the number of transactions within the population that are likely to include an element of irregularity can be estimated to be between 400 to 600 items.

> We chose a sample with a confidence level of 95% and confidence interval ±1%. We found 3% irregularity in our sample. This means we are 95% confident that irregularity is between 2%-4%.

Reporting on Fraud Loss Measurement results

The results from FLM exercises should be reported individually for each exercise and collectively to show the actual results, the extrapolated results and impact of the FLM exercise itself.

The process for reporting an individual FLM exercise should ensure that the findings from testing are categorised to show:

- the instances of fraud, indicators of fraud and error found and the respective values;
- the number and values of sample items that were verified as being regular; and
- the number and values of sample items which remain 'unresolved', in that a determination on whether the case was regular could not be made.

Details of the sampling methodology employed and the sample size selected should be documented so that these can be reflected in the report, together with extrapolation over the total population. It is essential to include:

- number of cases in the sample
- confidence level
- confidence interval
- size of spend area (population)

The FLM exercise should draw statistically valid[24] conclusions about the overall and underlying levels of fraud and error in the area being reviewed and the vulnerability of the organisation to fraud in that area.

Links to example templates to assist with reporting are included within the 'supporting additional guidance products' in the appendices below.

Considerable insight value can be gained from more detailed reporting on specific fraud risks, rather than just the totals in each defined reporting category. Understanding which fraud risks are materialising is the **key source of insights** for future control improvements or other prevention activity.

[24] E.g. an average irregularity level to a defined confidence level, with associated confidence interval

Reporting Results - Top tips

- Include a high level overview of the scheme (brief executive summary), including an overview of the approach taken and a summary of the key findings and conclusions.
- Summarise the high level process that was followed to determine residual risks for testing, and how testing was conducted.
- The report should aim to draw conclusions about the levels of fraud and error within the scheme or spend area(s), including how any testing limitations may have impacted the overall results.
- As best practice, the report may also include recommendations on control improvements identified as a result of the FLM exercise, where these have been shown to be an appropriate and proportionate response.
- If the data sharing method used to support the FLM exercise permits it, all cases of irregularity should be reported to the element of the business that deals with financial recovery. This is to determine whether it is necessary and proportionate to recover funds, and if so, to commence recovery activity.
- If the data sharing method used to support the FLM exercise permits it, all cases classified as 'fraud' or 'indicators of fraud' should be referred to your investigation teams for further review and potential enforcement activity.

Methodology for identifying and calculating preventative savings

A key benefit of FLM exercises is their usage in the evidence for preventative savings. These are generated when a payment has been stopped from being processed due to fraud / error being detected, or controls being improved. There are three points for calculating different preventative savings measures:

1. **Point of interdiction:** This refers to savings from loss prevented at the point where fraud/error has been detected. As a result, the payment scheduled to be processed has now been stopped from being processed. The value of the prevented payment can be evidenced with certainty and attributed to the measurement exercise.
2. **Future Loss Prevented:** These savings occur where it can be evidenced that, had the fraud/error not been detected by the measurement activity or exercise then it would have been more probable than not that the fraud/error would have continued for a period of time (of a duration based on the best available evidence) resulting in subsequent financial loss. As time periods go further into the future so assumptions on the behaviours of individuals used to calculate future prevented loss become less accurate. For this reason, the default maximum length of time to be considered for Future Loss Prevented should be no more than one year, unless the relevant policy area provides evidence on a more appropriate time period (e.g. a comprehensive data set showing average lengths of frauds of that type last longer[25]).
3. **Upstream prevention:** Improvements in processes on the back of insights generated from the FLM exercise may generate 'Upstream Prevented Savings'. These savings are generated from process changes based on the detected fraud/error that prevent subsequent fraud/error within the wider population, which are evidenced once the area is measured a second time (e.g. after the control improvement). In addition, savings may include the application of the test parameters to the wider population to identify similar, existing, cases of fraud/error.

[25] If this is the case, conduct a review of the operation of detective controls as a priority

The level of the first two types of savings should generally reduce over a period of time as behaviours change, once awareness of the improved fraud control has become common knowledge. Upstream prevention savings will most likely be more valuable. These savings necessitate at least two measurement exercises (e.g. one to determine the baseline level, and another to remeasure after the control improvements are implemented).

FLM exercises should be used to capture 'upstream prevention' benefits - the process is:

- Baseline levels of fraud and error using fraud measurement results
- Use baseline results to inform the prioritisation and proportionality of compliance environment in line with fraud risk appetite (Strategic)
- Design and implement controls or interventions (Tactical)
- Re-measure the fraud and error levels (ensuring these remain accurate in the current context)
- Review the results - the difference in loss is your prevention benefit.
- Evaluate the effectiveness of the control or intervention
- Adjust or change the controls or interventions, if required
- Re-measure and evaluate as required - the fraud risk management cycle

Next Steps - What to do with the findings from your exercise

In order to derive the maximum benefits from FLM exercises, it is necessary to ensure that both the **tactical** and **strategic** benefits of any individual exercises and wider programmes of fraud measurement are considered, including how these can be used to effectively support the organisation's broader counter fraud and integrity strategy.

Tactically, all instances of detected fraud and indicators of fraud should trigger:

- a root cause analysis of identified fraud or error
- an update to the relevant fraud risk assessment with the new insights
- reporting of any identified control failures to control owners.
- if the data sharing gateway permits, a referral to investigation/enforcement teams for further review

Whether the insights direct the organisation strategically depends very much on the objective of the measurement in the first place. Typically, the FLM exercise contributes to an internal feedback mechanisms that assists risk owners by ensuring they have an up to date understanding of their threat and risk environment, allowing them to:

- plan to address emerging risks and vulnerabilities
- strengthen control frameworks to prevent and mitigate future incidents
- develop indicators to support proactive detection activities
- enhance the efficiency of business processes.

If measurement is conducted for **Exploration**

The key strategic action is to use the insight from the FLM exercise to build the case for more counter fraud activities in general. This could include detection and prevention activity, fraud risk assessment and more, and more comprehensive, fraud measurement activity across the business.

If measurement is conducted for **Performance**

The key strategic action is to build business cases for the improvement of preventative controls in the subject area of the exercise. The business case should be built on 'size of the problem' as identified in the FLM exercise, with a return on investment forecast based on the amount of upstream prevention that can be gained from improving controls.

If measurement is conducted for **Assurance**

If the result is that the organisation is above its stated level of tolerance in the subject area , follow the same next steps as for performance. If the result is within the level of tolerance, the key action is to determine how the same level of fraud control can be achieved more efficiently and to give better value for the taxpayer (e.g. consider automation or removal of controls in areas where the measurement shows the risk is low).

Case Study

Case Study Example - Australian Government Department of Education

It is possible for a FLM exercise to initially begin as an Exploration or Performance exercise and to then evolve over a number of years into an annual assurance programme of FLM, as can be seen in the below real world case study from the Australian Government Department of Education-:

Background

In Australia, early childhood education and care (ECEC) is delivered to children and families by approved providers and services. Families receive help with the cost of child care through the Child Care Subsidy (CCS). CCS is paid directly to approved providers and passed on to families as a fee reduction. The CCS aims to improve access to quality ECEC by providing assistance to meet the cost of ECEC for families engaged in work, training, study or other recognised activities. In 2023-24 the Child Care Subsidy program was $13.9 billion.

Measuring the payment accuracy of the Child Care Subsidy Program

The Australian Government Department of Education uses a Random Sample Parent Check (RSPC) to measure the payment accuracy of the CCS program. The RSPC has been in place since 2014 and involves surveying a stratified random sample of parents and guardians across Australia about details of the ECEC their child received. This survey data is then compared with the data the CCS Approved child care providers submit to the Department to measure the accuracy of those claims.

The RSPC provides a statistically reliable national estimate of the level of correctness[26] of Child Care Subsidy payments that satisfies the requirements of Australian National Audit Office financial statements audits. The results also contribute towards the identification of emerging practices, including possible areas of fraud and non-compliance.

How is the RSPC used to understand program losses and support budget measures

The RSPC allows the department to quantify potential losses to fraud and non-compliance. This data is critical in developing strategies and measures to combat fraud and non-compliance. The RSPC provides data to target program vulnerabilities and provide a reliable data source for predicting potential savings from regulatory activities.

For example, the RSPC exercise conducted in 2022-23 identified that 63.8% of annual CCS program losses during the period from 2021-22 were linked to sessions of care having gap fees27 inappropriately waived by providers. This led to measures to improve the collection of gap fees, including legislative change, to require all gap fees to be paid electronically from 1 July 2023 combined with an audit program to check for compliance. As a result, the error rate of non-payment of gap fees reduced from 63.8% in 2021-22 to 4.1% in 2023-24.

The payment accuracy rate for 2023-24 was 96.4% which is the highest rate since the introduction of CCS in 2018.

[26] ‘Correctness’ is analogous with the UK term ‘regularity’ (of spending) and in this context is a measure of the amount of CCS that was claimed incorrectly, and therefore, not spent for the purpose intended by the Australian government.

[27] Gap fees are the co-contribution amount that a family is liable to pay for the care their child receives.

Fraud Loss Measurement exercises - Summary

Step	Activity	What Does Good Look Like?	Where Can It Go Wrong?
1	**Select a high-risk area** (Enterprise risk assessment/Strategic Risk Profiling Tool)	Increased understanding of highest risk areas of spend enabling the **prioritisation** of counter fraud activity (in this case **FLM**)	Selecting a low risk area; unclear rationale and decision making for area selection
2	Conduct a full **Fraud Risk Assessment**	Details of specific fraud risks captured, examination of relevant controls, leading to a **clear understanding of specific residual risks**	Fraud risks not clear, residual risk not identified properly
3	Decide what to test for fraud Identify a **sample**	Use understanding of residual risk to select a range of **evidence*** which could identify fraud **Sample size is representative**	Testing what's easy to test - this may miss more urgent or high Impact fraud risks Using evidence that won't show whether fraud or error has occurred.
4	Test for fraud in a way that allows **measurement**, and report estimates of fraud	Testing mindset **focused on finding fraud** **Clear documented reasons for sample** selection	Testing conducted like an audit - assessing controls Sample not representative
5	**Strategic insights** including analysis, reporting and use of FLM programme outputs	**Counter Fraud Strategy** transformed by an increased understanding of fraud risk exposure Increased understanding and engagement on the **scale and Impact of public sector fraud** and error	Inclusion of low confidence FLM exercises may undermine confidence in the integrity of fraud landscape reporting and any strategic decisions based on this.

Lessons Learned - Where Fraud Loss Measurement exercises fall down:

Lesson Learned

Selecting areas to test using predominantly internal evidence based on easy access, which is more akin to audit and control testing (e.g. travel and subsistence expenses fraud), which is unlikely to represent the best use of limited resources.

Lesson Learned

Basing the exercise on existing, often poor quality, FRAs, which leads to problems with identified residual risks for testing, evidence selection and ultimately lower confidence in the outcomes from the FLM exercise.

Lesson Learned

Choosing very high precision samples where there is only resources left to do very light touch testing.

Lesson Learned

Not properly assessing/understanding the evidence available in terms of what it does/does not indicate in relation to whether or not fraud has occurred.

Lesson Learned

Lacking ambition in gathering a range of external evidence (e.g. where government, open source and third party paid provider data exists but was unused in the FLM exercise).

Lesson Learned

Not involving the right stakeholders, people and teams in the process of undertaking the fraud loss measurement exercise.

Lesson Learned

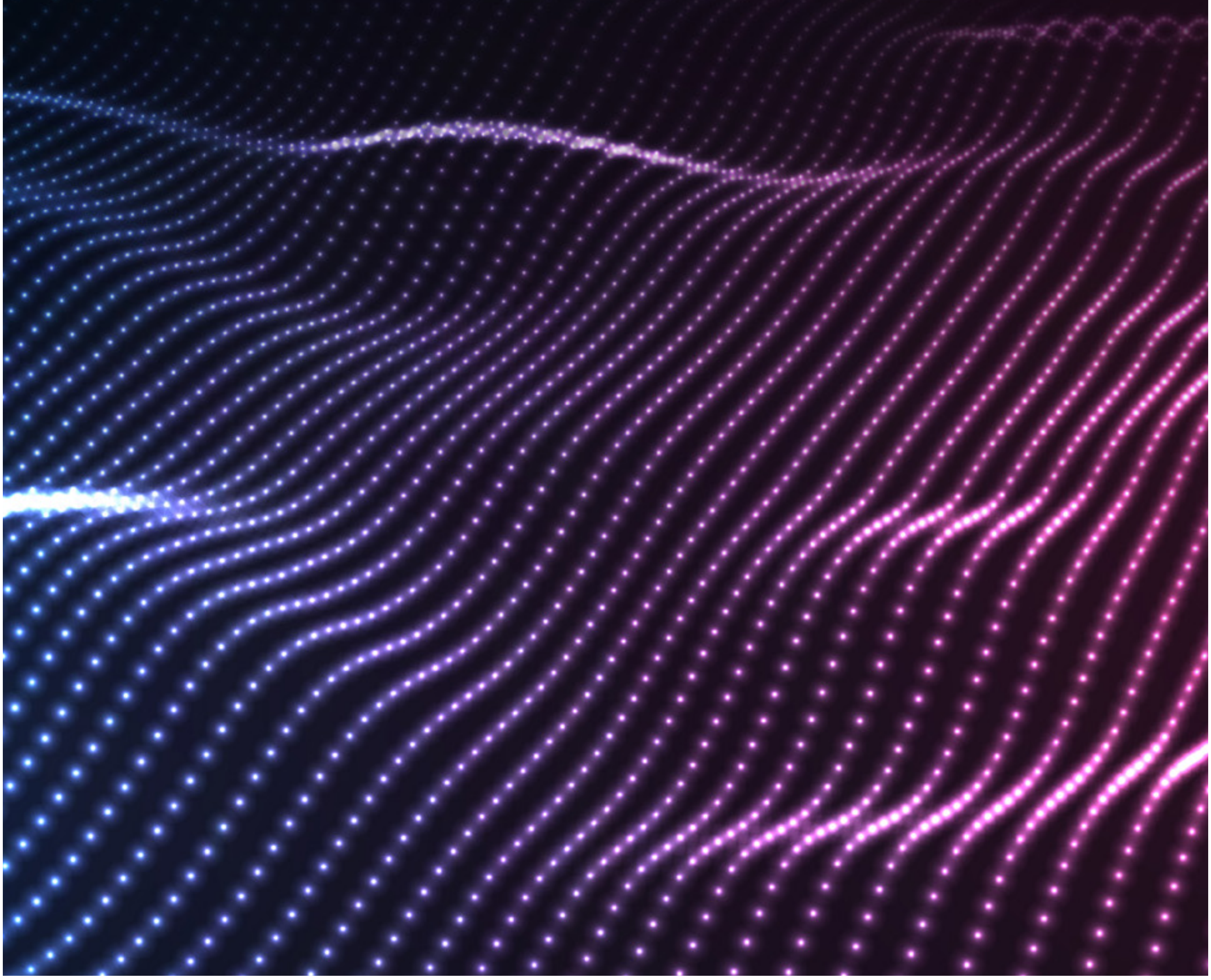
Assuming that any anomalies found in the testing automatically mean the case is fraud, rather than considering alternative explanations and using the balance of probabilities.

Appendices

International Comparators: comparing fraud estimates in other countries

Without undertaking specific FLM exercises, it is not possible to accurately estimate losses from fraud and error. However, a reasonable, although limited, alternative can be to rely on comparators in other schemes or jurisdictions.

The following international comparators reinforce the message that fraud is an ever-present challenge for all countries and all sectors. Where work is done to measure the prevalence of fraud and error, it is consistently found at much higher levels than those typically reported (or understood) where measurement is not conducted.



United Kingdom

The UK Government Counter Fraud Profession (GCFP) produced the world's first Fraud Measurement Professional Standard.

Proactive detection - of which FLM exercises are an example - has been part of the UK Government Functional Standard for Counter Fraud (GovS013) since 2019. In summary, this sets out an approach that:

- supports high quality measurement to produce a reliable estimate of fraud and error (or irregularity, which is similar to what the US call 'improper payments') for spending areas (or particular fraud risks);
- delivers a detailed approach that focuses on methodical identification of residual fraud risk in schemes, then uses independent* evidence to test how frequently that fraud risk materialises in the sample, and
- enables the result to be extrapolated against the overall spend to determine an estimated fraud and error level, resulting in a number, which will usually be expressed as a monetary value and percentage figure.

Fraud Measurement overall starts with what we know – the prevented and detected fraud (including error, bribery and corruption) that has been found and reported. However, it also recognises that it is likely that undiscovered fraud exists, which we illustrate using a picture of an iceberg.

Fraud Measurement overall starts with what we know.

The annual UK Fraud Landscape Report (PSFA, 2023) provides an 'iceberg' estimate showing the known and unknown fraud for the whole of central government. However, similar icebergs exist at different levels, many of which are represented in the overall iceberg of the Fraud Landscape Report.

Public Sector Fraud Authority

Cross-Government Fraud Landscape

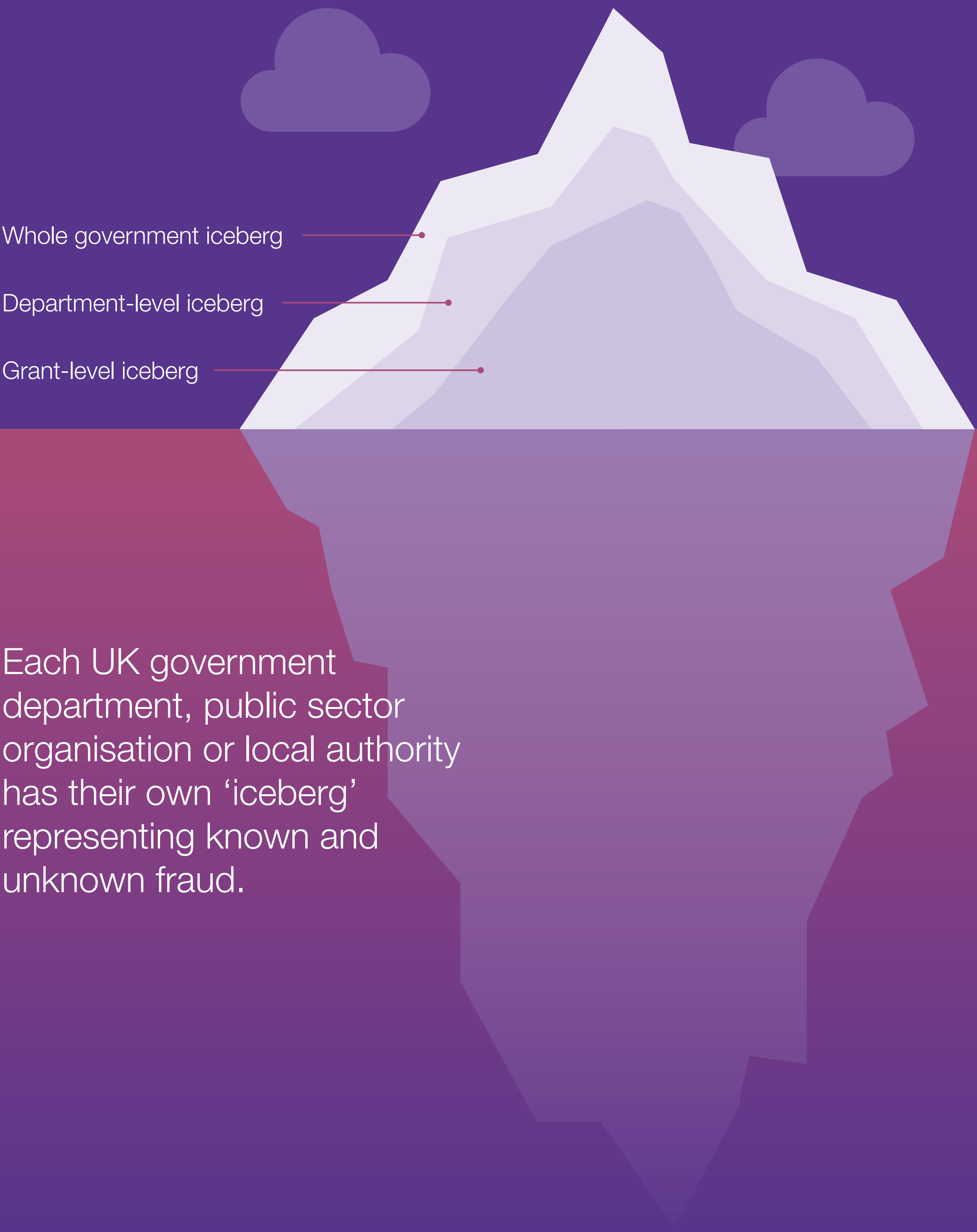
Report 2021-2022

Each UK government department, public sector organisation or local authority will have their own 'iceberg' representing known and unknown fraud. Within an organisational level iceberg, there will be smaller icebergs representing different groups of activity, such as grants (per the below example illustration), procurement, payroll, loans, expenses etc.

Within each group-level iceberg, there will be individual icebergs for particular schemes, contracts etc within it. We can liken this to the Russian 'Matryoshka (or Babushka) dolls' (Oxford English Dictionary, 2011) where smaller icebergs are stacked inside and a composite part of larger fraud icebergs.

The Fraud Iceberg ‘Stack Model’

The overall whole government picture is produced from a combination of central reporting data submitted by departments to the (UK) Public Sector Fraud Authority and the results of fraud loss measurement exercises overseen by the Fraud Measurement and Assurance Programme, which is covered in more detail later in this section.



Each UK government department, public sector organisation or local authority has their own ‘iceberg’ representing known and unknown fraud.

United States

In the United States[28], the government analyses and publishes data on Improper Payments. Improper Payments cover a wider range of payments with a level of incorrectness than solely fraud and error. They also include underpayments.

Improper Payments cover the following areas:

- **Overpayments:** These are payments that are in excess of what is due that should not have been paid. These break down into two further categories:
  - Unintentional Overpayments: Accidental in nature (e.g. error)
  - Fraudulent Overpayments: Caused by wilful misrepresentation for the purpose of obtaining funds, services or benefits. In the US, this is determined through a court or other adjudicative processes.
- **Underpayments:** Payments that are less that what is due
- **Unknown Payments:** Payments that the agency is unable to discern as proper or improper as a result of insufficient or a lack of documentation.
- **Technically Improper Payments:** Payments that were made to the correct recipient in the correct amount, but whose payment process did not follow 'all applicable statutes or regulations'.

In the US system, fraud determinations cannot be made by agency officials, they can only be made through judicial or other adjudicative systems.

In the financial year 2022-23, the US reports an average of 5.43% of improper payments (2022-23[29]) in its federal spend.

In the 2023 US fiscal year, the federal government's total spending amounted to $6.3 trillion (5.43% of this figure would equate to $342.09bn of improper payments).

The Government Accountability Office in the USA recently released its first fraud estimate[30], showing the US Federal agencies lose between 3% and 7% of their average federal obligations due to fraud alone.

[28] For more information on the US approach to improper payments and fraud, see https://www.gao.gov/assets/d24106608.pdf

[29] US government Office of Management and Budget reported Improper payments rate
US Fiscal Treasury data 2023

[30] https://www.gao.gov/assets/gao-24-105833.pdf

Australia

In 2019, the Australian Attorney-General's Department commissioned professional services firm EY to analyse the total cost of fraud against the Australian Government, including the potential scale of unreported fraud.

EY's meta-analysis of measurement exercises conducted globally concluded that losses from reported and unreported fraud and error in any organisation and any area of expenditure will be at least 3%, probably near to 6% (noting the average losses of 5.95%) and possibly more than 10%.

In this context, error is defined as losses arising from unintentional events, processing errors and official government errors. For example, this would include unintentional misapplication of identity, such as duplicate or incorrect payments because of failures to properly collect or check identity, as well as intentional identity fraud.

In the absence of fraud loss measurement exercises, Australian Government entities rely on these comparators to provide estimates of levels of fraud. However, these comparators are only used to communicate the potential scale of unreported fraud and error, challenge misconceptions about the potential size of the problem, encourage officials to place a higher priority on program integrity, and seek investment in counter fraud and program integrity resources and activities.

Error is defined as losses arising from unintentional events, processing errors and official government errors.

The UK Fraud Measurement and Assurance programme

In the UK, the Public Sector Fraud Authority (PSFA) operates the Fraud Measurement and Assurance (FMA) programme, which reviews fraud measurement exercises by individual entities to determine whether the work meets the UK Fraud Measurement Standard.

The FMA programme was initiated in 2014 to test the hypothesis that the government suffers from more fraud than it was detecting - prior to this reported losses sat at **0.1%** of government spend.

	Number of Exercises	Population of Spend	Population Tested	Gross Irregularity	Extrapolated Irregularity
Totals:	63	£224bn	£23.3bn	£671.9m	£4.7bn

In December 2018, the Oversight Board concluded, using the evidence from the programme, that the hypothesis has been proven. By that time the programme had evidence from 48 exercises, and used the better quality exercises to conclude that fraud and error levels are likely to be in the range of **0.5% to 5% fraud and error**.

Who	Description
Oversight Board	The Oversight Board makes key decisions regarding the vision, structure and running of the UK FMA programme.
Members... Cabinet Office Government Internal Audit Agency NAO National Audit Office Chartered Institute of Internal Auditors NHS Counter Fraud Authority	
Expert Panel	The expert panel is composed of members with experience of fraud measurement work or related areas. They review and provide assurance of the participating departments against the FMA criteria for each gate.
Members... Government Internal Audit Agency NAO National Audit Office NHS Counter Fraud Authority	

Supporting additional guidance products

Product	Topic	Owner
See Annex A	A document adapted and expanded from the (UK) Fraud Loss Measurement training course providing definitions of terms relevant to Fraud Measurement (including Fraud Loss Measurement).	United Kingdom Government Counter Fraud Function Government Counter Fraud Profession
(UK) Government Counter Fraud Profession (GCFP) Measurement Standard*	The full (UK) Government Counter Fraud Profession (GCFP) Measurement Standard, which this Fraud Loss Measurement Framework draws upon and is based. *Government Counter Fraud Professional Fraud Measurement Standards can be obtained by emailing: gcfp@cabinetoffice.gov.uk	United Kingdom Government Counter Fraud Profession
See Annex B	Provides a role description and terms of reference for membership of the Fraud Measurement and Assurance (FMA) Expert Panel.	United Kingdom Public Sector Fraud Authority
See Annex C	Reporting template for organisations to use when undertaking stage 2 (detailed fraud risk assessment) of the fraud measurement process.	United Kingdom Public Sector Fraud Authority
See Annex D	Reporting template for organisations to use when undertaking stage 3 (Planning, sampling and gathering initial evidence) and stage 4 (Conducting the testing) of the fraud measurement process.	United Kingdom Public Sector Fraud Authority
Fraud Personas and Guide on the practical use of fraudster personas	Discover the different types of fraudsters (personas). Understanding fraudster personas can help you and your organisation be more aware of the common methods used by fraudsters by putting you in the mindset of a fraudster, in turn helping you to better understand residual fraud risks.	Australia Commonwealth Fraud Prevention Centre
Strategic Fraud Risk Profiling Tool (Stage 1)	The Strategic Fraud Risk Profiling Tool is designed to help Australian Government officials identify high risk areas while prioritising efforts in their entities. It is good practice to first develop a strategic fraud risk profile for your organisation before embarking on a detailed fraud risk assessment.	Australia Commonwealth Fraud Prevention Centre

Product	Topic	Owner
(UK) Government Counter Fraud Profession (GCFP) Enterprise Fraud Risk Assessment - Practice Note (Stage 1)	This guide has been developed by the Government Counter Fraud Profession (GCFP) and aligns to agreed standards for Counter Fraud Professionals produced by the GCFP. This product is aimed at Counter Fraud Professionals with responsibility for overseeing the Counter Fraud Function within their department or organisation, and those responsible for the completion of an Enterprise (Organisational) Fraud Risk Assessment.	United Kingdom Public Sector Fraud Authority
(UK) Government Counter Fraud Profession (GCFP) Fraud Risk Assessment Standard	The full (UK) Government Counter Fraud Profession (GCFP) Fraud Risk Assessment Standard, elements of which this Fraud Measurement Framework draws upon.	United Kingdom Government Counter Fraud Profession
(AU) Fraud Risk Assessment Leading Practice Guidance	The fraud risk assessment guide provides key principles and methods taken from leading practices across public and private sectors.	Australia Commonwealth **Fraud Prevention** Centre
IPSFF Fraud Control Testing Framework	Guidance on Fraud Control Testing produced by the International Public Sector Fraud Forum for use by colleagues from across member nations who are engaged in counter fraud work.	**International Public Sector Fraud Forum**
(UK) National Audit Office 'A Practical Guide to Sampling'	This guide to Sampling has been produced in response to a large number of requests received by the Statistical and Technical Team relating to sampling matters. The guide aims to consolidate the information required to complete the survey process from design to reporting.	United Kingdom NAO National Audit Office
Fraud Data and Analytics Leading Practice Guide	The Fraud Data Analytics Leading Practice Guide provides a framework and principles for implementing leading practice fraud data analytics.	Australia Commonwealth **Fraud Prevention** Centre
Counter Fraud Investment Cases Leading Practice Guide	It can be challenging to develop convincing and compelling investment cases for vital counter fraud resources and activities. This guide, developed in collaboration with Deloitte, provides Australian Government officials with practical steps for developing counter fraud investment cases.	Australia Commonwealth **Fraud Prevention** Centre

Annexes

Annex A - Fraud Measurement: Definition of key terms and words

Fraud

The difference between fraud and error is 'intent' - that someone has intentionally taken an action to make gain or avoid loss. Where there is, on balance of probability (the 'Civil' test), evidence that a case or transaction is wrong or incorrect through someone knowing and intending it to be 'wrong' then it should always be recorded as fraud. Note: This does not necessarily mean that an investigation should or will be undertaken and it will be up to an organisation to set parameters for what will be investigated in line with their own Counter Fraud Policy. To be recorded as fraud, there should be a balance of indicators that the action meets one, or more, of the three categories of fraudulent action in the UK's Fraud Act (2006):

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position

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).

In the UK government, public bodies are required to report instances of fraud where the balance of probabilities (Civil) test is met - not where it being fraud is beyond reasonable doubt (the criminal test). This is because where reporting is done to the criminal test, often this results in both underreporting and late reporting, due to the time and costs involved in securing criminal convictions.

Error

Where an instance has been identified 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 and Error

A modern fraud response deals with both fraud and error (instances of loss with or without evidence of intent, or with evidence that does not meet the civil test - balance of probabilities). It does this because the modern fraud response looks to use risk assessment and data analytics tools and techniques to detect irregular payments. In dealing with these irregular payments, establishing intent adds cost and dealing with fraud and error enables businesses to prioritize where it invests in establishing intent for prosecution or formal sanctions and where it chooses to maximize return on investment by focusing on recovery and redress.

Fraud Estimation

The purpose of fraud measurement is to be able to produce an estimate of the overall level of fraud and error in a system. These estimates can be produced using a range of different methods including by **extrapolation** from statistically valid sampling exercises, which is the methodology utilized by the fraud loss measurement process described in the IPSFF Fraud Loss Measurement Framework.

However for the purposes of broader Fraud Measurement it is important to understand that this is not the only way to produce fraud and error estimates. Alternative methods which can be used to provide fraud and error loss estimates include:

- The use of **modelling** data to produce estimates, which can be used in either a top down or bottom up approach. In the case of top down modelling this can for example draw upon theoretical models from academic studies or internal analysis functions, whereas bottom up models will normally draw upon data and insights from historic reporting data and case studies to produce whole system estimates.
- The use of benchmarking to produce estimates from comparator data. In such cases the estimates produced will draw upon data from organization(s) with a similar profile, areas of spend and/or schemes to produce an estimated level of loss.

The level of fraud and error

A Fraud Loss Measurement Exercise provides an estimate of the **level** of fraud and error in a system. The statistical validity of the sample taken, and the randomness of the sample, the estimate produced will have an impact on the accuracy and reliability of the estimate produced. Generally, these exercises provide underestimates of the true level, as it is often not viable to test all of the different fraud risks identified.

FLM exercises typically provide an estimate of the **level** of fraud and error in a system, rather than **loss**. Simply, this is because any recovered fraud and error in the system will not necessarily have been netted off the estimate that is produced.

The fraud and error found in the sample may be dealt with (e.g. recovered), which would impact the loss, however this often takes considerable time (longer than the duration of the FLM exercise). In addition, the business may be taking action elsewhere in the area measured and may detect and recover fraud or error instances that would have been captured in the sample if the sample had selected different payments.

FLM usually identifies the **level** of fraud and error. If a business invests additional resources and effort to establish the intent behind the cases of fraud and error it identifies, this can be broken down further into fraud and error respectively.

Loss from fraud and error

This is the amount of money paid out and found to be 'wrong' or incorrect (i.e. through fraud or error) that cannot be recovered. In order to calculate 'loss' it is necessary to be able to calculate and know what sums have been **'recovered'** (i.e. instances of fraud and error where sums of money have been repaid by those who had benefited from the incorrect payment).

Levels of loss should be regularly updated as recoveries are made. The amount of recorded 'Loss' should be less than the calculated 'level' of fraud. This is because recoveries of some amounts of detected fraud and error will mean that losses will be less than the recorded level of fraud (and error).

There are two areas where loss from fraud and error should be considered. The first is the juxtaposition of detected fraud and error with recovered fraud and error. This shows the known loss from fraud and error. It does not show the overall loss from fraud and error and should never be referenced as such.

The second is where a calculation is undertaken to try and establish the actual loss level across known and estimated fraud and error. This calculation has a lot more uncertainty, depending on the quality of the measurement exercise, the robustness of the sample and the testing, the quality of the data on detected and recovered fraud and error and how this aligns to the risks in the FLM exercise.

Improper Payments

In the United States, the government analyses and publishes data on Improper Payments. Improper Payments cover a wider range of payments with a level of incorrectness than the UK's fraud and error data. They also include underpayments - which the UK does not consistently collect (it does in some areas, for example, welfare benefits.

Improper Payments cover the following areas:

- **Overpayments:** These are payments that are in excess of what is due that should not have been paid. These break down into two further categories:
  - *Unintentional Overpayments:* Accidental in nature (for the UK definitions, error)
  - *Fraudulent Overpayments:* Caused by wilful misrepresentation for the purpose of obtaining funds, services or benefits. In the US, this is determined through a court of other adjudicative processes.
- **Underpayment:** Payments that are less than what is due
- **Unknown Payments:** Payments that the agency is unable to discern as proper or improper as a result of insufficient or a lack of documentation.
- **Technically improper payments:** Payments that were made to the correct recipient in the correct amount, but whose payment process did not follow 'all applicable statutes or regulations'.

Of particular note is that in the US system, fraud determinations cannot be made by agency officials, they can only be made through judicial or other adjudicative systems. In the UK, officials determine fraud based on the civil test - the balance of probabilities. As a result, fraud is likely underreported, and reported with some delay (due to the lead time for adjudicative systems) in this system.

For more information on the US approach to improper payments and fraud, see GAO-24-106608, Improper Payments and Fraud: How They Are Related but Different

Irregular Payments

Under the UK Treasury's Managing Public Money rules, public bodies are expected to be compliant with the relevant legislation and wider legal principles such as subsidy control and procurement law. Delegated authorities should follow the guidance in that document.

The Comptroller and Auditor General (through the National Audit office) is expected to examine the accounts of public bodies to be confident that

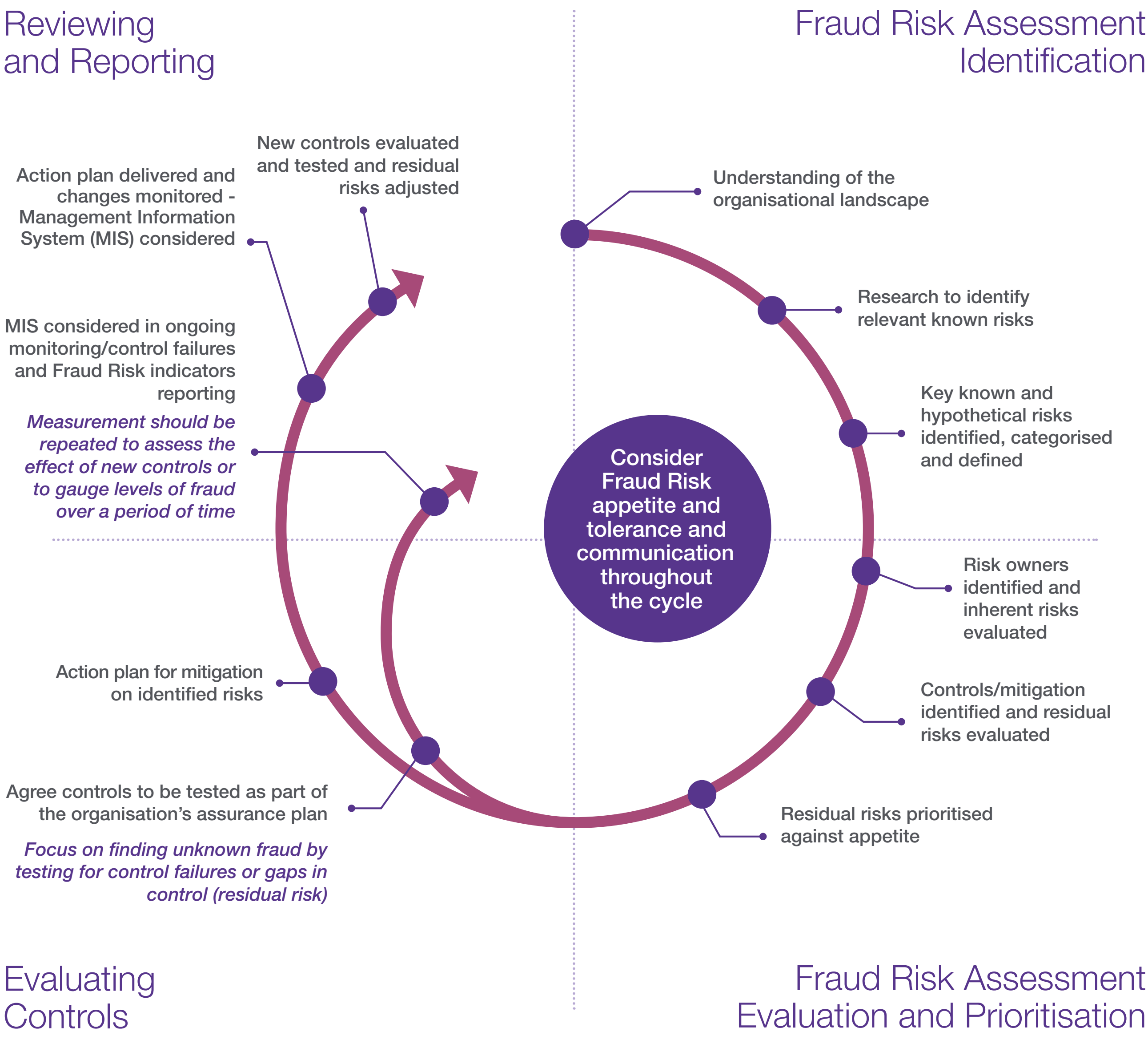
- the accounts present a true and fair view
- money provided by Parliament has been spent for the purposes intended by Parliament
- resources authorized by Parliament to be used have been used for the purposes in relation to which the use was authorized, and
- the financial transactions are in accordance with any relevant authority

Payments that are irregular include, but are not limited to, payments (or services that are provided) that are subject to fraud, or made in error.

Annex B - Fraud Measurement Assurance: Expert Panel Role Description

Background:

Below is the Fraud Management Cycle. The cycle offers an illustration of the end-to-end process, from using research to identify known risks, completing a fraud risk assessment, and using this to actually manage and mitigate those risks by informing control design. Key to delivering an effective Fraud Risk Assessment, as part of the Fraud Management process, is a thorough understanding of the organisational landscape.


Reviewing and Reporting
Fraud Risk Assessment Identification
New controls evaluated and tested and residual risks adjusted
Action plan delivered and changes monitored - Management Information System (MIS) considered
Understanding of the organisational landscape
Research to identify relevant known risks
MIS considered in ongoing monitoring/control failures and Fraud Risk indicators reporting
Key known and hypothetical risks identified, categorised and defined
Measurement should be repeated to assess the effect of new controls or to gauge levels of fraud over a period of time
Consider Fraud Risk appetite and tolerance and communication throughout the cycle
Risk owners identified and inherent risks evaluated
Action plan for mitigation on identified risks
Controls/mitigation identified and residual risks evaluated
Agree controls to be tested as part of the organisation's assurance plan
Residual risks prioritised against appetite
Focus on finding unknown fraud by testing for control failures or gaps in control (residual risk)
Evaluating Controls
Fraud Risk Assessment Evaluation and Prioritisation

The FMA Vision Statement is:

> To save public money from being lost to fraud and error by helping government departments understand their fraud risk exposure and to use measurement to estimate actual levels of fraud and error losses.
>
> Achieving this aim through making Fraud Loss Measurement sustainable and widely practised across the UK government to agreed standards, supported by the Government Counter Fraud Profession and recognised as part of the assurance landscape within each government department.

Fraud loss measurement is a key part of a robust counter fraud approach – one of the UK's Government Counter Fraud Profession disciplines and part of the fraud risk management cycle.

At an individual scheme level, fraud loss measurement helps to;

- identify what type of fraud is happening, and how much of it is taking place;
- inform evidence-based decisions on how to deploy counter fraud resources, including improved controls and what kind of resources are required; and
- measure any effects from changes in scheme design and control changes.

The UK Public Sector Fraud Authority operates a programme of fraud loss measurement review called **Fraud Measurement Assurance** (FMA) which has been running since 2014. At a cross-government level, it allows for a holistic picture to be built up of the types and value of fraud happening across government, to bring together unknown, estimated and detected fraud levels so that a better picture of total potential losses is understood, and that strategic decisions can be made based on the best evidence.

FLM Expert Panel Role and Requirements:

The expert panel is made up of colleagues with experience of conducting fraud loss measurement work to a high standard. The panel supports the government's counter fraud evidence base by reviewing and providing assurance that the quality of the work done by participating departments is good, set against the criteria in the government fraud measurement standard.

You will take part in holistic reviews of fraud measurement work undertaken by various government departments and public bodies. From this, you will provide feedback on the work which has been done and come to a conclusion as to whether you believe that the submissions have met the government fraud measurement standards.

The expert panel is made up of colleagues with experience of conducting fraud loss measurement work to a high standard

The essential criteria to be a part of the Expert Panel are as follows:

- Experience of conducting fraud loss measurement exercises
- Counter fraud knowledge and experience (including counter fraud strategy)
- Knowledge and understanding of fraud risk assessment
- Knowledge and understanding of fraud loss measurement
- Good communication skills and the ability to interpret and clearly describe fraud risks

Desirable criteria:

- Understanding of statistical sampling methods

Annex C - Fraud Measurement & Assurance: Gate 2 Feedback Summary

Scheme:	
Department Name:	
ALB Name:	
Date:	

Overall, the scheme achieved a: **Better** ○ / **Good** ○ / **Not meeting the standard** ○ rating for Gate 2 because upon review the exercise **did meet** ○ / **did not meet** ○ the majority of the criteria as per the Fraud Measurement and Assurance standards. General feedback leading to the rating are provided below with key recommendations. Further detailed feedback is provided on subsequent pages.

Overall Feedback:

General Recommendations:

Criteria	Detailed Feedback	Recommendations
Description of fraud risks		
Control		
Residual Risk		
Residual Risk Scoring		

Criteria	Detailed Feedback	Recommendations
Internal Evidence		
External Evidence		
Testing Plan		

Annex D - Fraud Measurement & Assurance: Gate 3 Feedback Summary

Scheme:	
Department Name:	
ALB Name:	
Date:	

Overall, the scheme achieved a: **Better** ○ / **Good** ○ / **Not meeting the standard** ○ rating for Gate 3 because upon review the exercise **did meet** ○ / **did not meet** ○ the majority of the criteria as per the Fraud Measurement and Assurance standards. General feedback leading to the rating are provided below with key recommendations. Further detailed feedback is provided on subsequent pages.

Overall Feedback:

General Recommendations:

Sample Criteria	Detailed Feedback	Recommendations
Sample Selection		

Testing Criteria	Detailed Feedback	Recommendations
Evidence		
Testing goes further than checking controls		
Approach to testing		

Reporting Results - Criteria	Detailed Feedback	Recommendations
Decisions on irregularity		
Confidence in the fraud estimates produced		
Report		