



Government
Counter Fraud
Profession

Operated by the Public Sector Fraud Authority

Government Counter Fraud Profession

Practitioners Standard for Fraud Measurement

Alternative format versions of the report are available on request from the Public Sector Fraud Authority: PSFA@cabinetoffice.gov.uk

Public Sector Fraud Authority

Publication date: October 2026

© Crown copyright October 2026

Produced by the Government Counter Fraud Profession operated by the Public Sector Fraud Authority.

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/> or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

Document Control

Information	This document is part of the Government Counter Fraud Profession (GCFP) Standards and Guidance.
Date Published	October 2026
Review Date	October 2029

Version Control

Version	Date
V 1.0	January 2021
V 2.0	October 2026

Contents

A. Professional Standard and Competencies for Fraud Measurement Practitioners	6
A1. Purpose	6
A2. Introduction	7
A3. How This Document is Structured	8
A4. Government Functions (UK)	8
A5. Public Sector Fraud Authority	10
A6. Government Counter Fraud Profession	10
A7. Government Counter Fraud Framework	11
A8. Roles and Responsibilities	13
A9. Key Components Explained	13
A10. Competency Levels	14
B. Fraud Measurement Competency Framework	15
C. Guidance on Processes for Fraud Measurement	23
C1. Introduction	23
C2. Identifying and Reporting Detected and Prevented Loss (Known Fraud)	24
C3. Estimating Undetected Fraud and Error	25
C4. Carrying Out and Adapting a Full Fraud Risk Assessment	31
C5. Planning Fraud Loss Measurement	36
C6. Choosing Statistically Valid Samples for Testing	39
C7. Other Sampling Methods	46
C8. Identifying and Selecting Evidence/Test Data	46
C9. Testing	49
C10. Estimating and Measuring Levels of Fraud and Error Losses	51
C11. Methodology for Calculating Savings	52
C12. Reporting on Fraud Testing and Estimation	55
C13. Managing Instances of Fraud and Error	56
D. Guidance on Products for Fraud Measurement Practitioners	57
D1. Introduction	57
D2. Fraud Reporting – What to Include in the Reporting of Known Fraud and Error Found Through the Operation of Existing Controls	57
D3. Fraud Loss Estimation and Measurement – Outputs from Fraud Measurement Exercises	60
D4. Calculation of Savings Generated Through a Fraud Loss Measurement Programme	62
D5. Updating Full Fraud Risk Assessments	62

Contents

E. Guidance for Organisations	63
E1. Introduction	63
E2. Mapping and Understanding Assurance Requirements	65
E3. Building a Fraud Measurement Programme within the Organisation	68
E4. Developing and Implementing an Annual Plan as Part of the Ongoing Fraud Measurement Programme	69
E5. Governance and Oversight of the Fraud Measurement Programme	70
E6. Measuring the Effectiveness of the Counter Fraud Strategy	71
F. Further Guidance	72
F1. Further Information	72
F2. Functional Standards	73
F3. Further Reading	75
Glossary	77
Appendix 1 – Full Competency Framework	83
Appendix 2 – Fraud Reporting Categories and Typologies	91
Appendix 3 – Spend Area Assessment	93
Appendix 4 – Fraud Prevention Savings Framework	94
Appendix 5 – Reporting Findings From Fraud Measurement Exercises	95

A. Professional Standard and Competencies for Fraud Measurement Practitioners

A1. Purpose

This document is part of the wider Government Counter Fraud Standards and Guidance which cover all the core disciplines and subdisciplines in the Government Counter Fraud Framework.

The Government Counter Fraud Professional Standards and Guidance are designed to present a consistent cross-government approach to countering fraud, raise the capability of individuals, and through this increase the quality of an organisation's counter fraud work.

Their aim is

- To describe the knowledge, skills and experience (professional standards and competencies) needed for an **individual** to demonstrate practitioner level. The document directs you to a competency framework which outlines how someone can progress to this standard
- To provide **guidance** to those using the standards on the processes and products they will use to deliver the discipline and what they may seek to put in place in the organisation to deliver the discipline effectively. This standard forms the basis of the **Fraud Measurement** core discipline within the Government Counter Fraud Profession (GCFP).

The professional standards and competencies are not intended to cover every eventuality or every specific issue that may arise and should be adapted to the organisation's resources and fraud risk profile. This standard should be read in conjunction with all other GCFP Standards. The standard does not supersede an organisation's operating procedures. The GCFP standards are designed and intended for individuals and should be read in conjunction with organisational operating standards where these exist.



The Government Counter Fraud Professional Standards and Guidance are designed to present a consistent cross-government approach to countering fraud

A2. Introduction

Fraud against the public sector increases the cost of public services, and understanding, finding and reducing fraud is an essential part of government efficiency.¹

In order to understand fraud, organisations need to be able to accurately measure the fraud they are faced with.

Fraud Measurement is the process of quantifying and estimating the extent of fraud and error within a specific area of an organisation or across the organisation as a whole, using data analysis, sampling, and modelling techniques to understand both known and unknown fraud and error.

Measurement provides insight into the nature and extent of fraud and error, which enables public bodies to better manage the problem.

This core discipline is focused on the skills, knowledge and experience required when measuring, estimating and reporting instances of fraud and error.

The scope of this Standard covers the following activities:

- Reporting of instances of fraud or error as detected or prevented by existing controls, which provides a baseline for further measurement on undetected fraud and error
- Measuring and estimating levels of undetected fraud through fraud loss measurement exercises
- Measuring levels of undetected fraud and error through failures in controls
- Calculating and reporting recoveries of detected fraud
- Using methodologies for calculating ongoing savings of prevented fraud and error.

Measurement as an activity includes methodologies for undertaking sampling exercises to deliver statistically valid estimations of fraud and error in a system or process.

The word fraud will be used in this document to refer to all forms of fraud, bribery and corruption.

Error is included within the scope of Fraud Measurement for two main reasons:

Firstly, from an operational view, a process that is vulnerable to error is also vulnerable to fraud. They are measured together because trying to prove fraudulent intent for every event is impractical and inefficient, particularly when measuring at scale. Secondly, the financial loss is the same regardless of the cause. Therefore, the required organisational response is identical whether the loss came from error or fraud that is, recovering the funds and improving controls.²

Fraud Measurement in this context therefore focuses on money and the amount lost due to fraud and error. There can be other impacts from fraud such as reputational, physical, environmental or wider societal harm or the undermining of government policy objectives. These impacts fall outside the scope of this document.

Effective fraud measurement cannot be undertaken in isolation from other counter fraud disciplines. Risk assessment is key to determining the scope and target of measurement exercises. Therefore this standard draws upon and uses elements from counter fraud disciplines such as Fraud Risk Assessment and others (particularly within the Fraud Control cluster) and should be read in conjunction with all other GCFP Standards and Guidance.

¹ <https://www.gov.uk/government/publications/public-sector-fraud-authority-mandate>

² https://assets.publishing.service.gov.uk/media/67b85a45ba253db298782c0c/IPSFF_Fraud_Loss_Measurement_Framework_.pdf

A3. How This Document is Structured

This document contains the following

- The **Competency Framework** outlining the knowledge, skills and experience required by those undertaking work within fraud measurement to operate effectively and how these develop through the competency framework levels of Foundation and Practitioner.
- **Guidance for Professionals**
 - **Process guidance** describing the recommended processes to implement fraud measurement
 - **Product guidance** setting out the recommended guidance on developing good quality outputs in relation to fraud measurement
 - **Organisation guidance** which has been agreed as Approved Professional Practice and may be followed by all counter fraud professionals and their organisations.

These standards have been created, reviewed and agreed by the GCFF Board, the body with oversight of the profession, and the responsibility for the development and maintenance of the Counter Fraud Professional Standards and Guidance.

A4. Government Functions (UK)

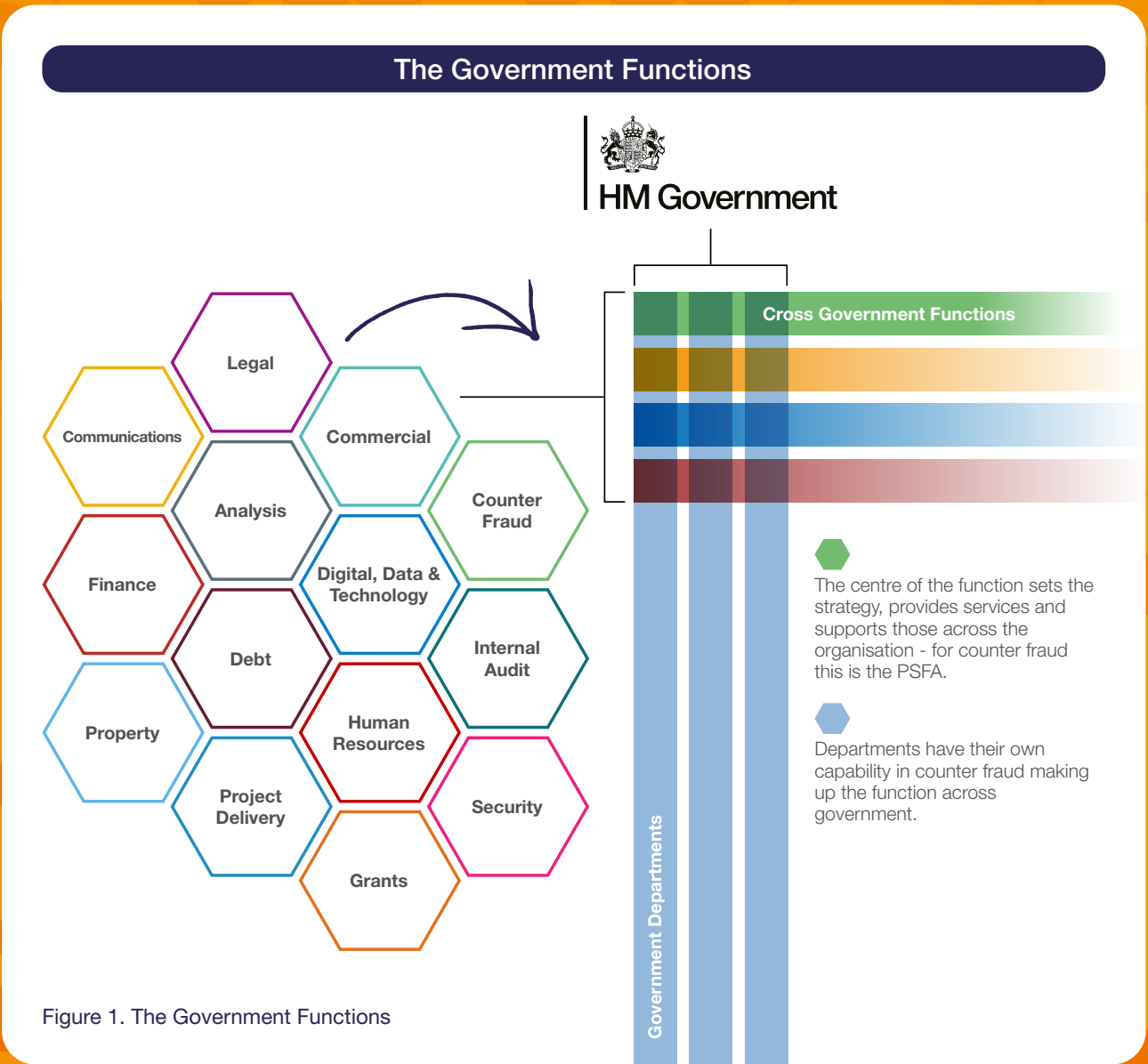
In the United Kingdom, the central government operates under a functional model.

The Government Counter Fraud Function (GCFF) is one of the government's fourteen functions. The GCFF has published a functional standard, a strategy and in 2018 launched the World's first counter fraud profession. The vision of the GCFF is

“Working across government to make the UK the world leader in understanding, finding and stopping fraud against the public sector”

Functions are embedded in government departments and arm's-length bodies. The teams that make up the wider government function are supported by expertise in other public bodies and the functional centre. The Public Sector Fraud Authority (PSFA) provides support and expertise for the GCFF.





A5. Public Sector Fraud Authority

The Public Sector Fraud Authority (PSFA) provides increased scrutiny of activity to reduce fraud and economic crime and builds broader and deeper expert services to support departments and public bodies to further improve their capability. The PSFA builds on the foundations of the Functional Centre for Counter Fraud, formerly known as the Centre of Expertise. The PSFA has an established mandate that sets out its roles and responsibilities and those of ministerial departments and public bodies interacting with it.

The purpose of the PSFA is to work with ministerial departments and public bodies to understand and reduce the impact of fraud.

It brings

- A greater focus on performance and outcomes
- Increased depth and breadth of support
- Integrated partnership between Cabinet Office (CO) and HM Treasury (HMT).

The PSFA is changing the way that government manages fraud, its mission is to³

- Modernise the fraud and error response by widening access and use of leading practices, tools and technology, better protecting taxpayers' money
- Build expert-led services developed in collaboration with experts in departments and public bodies to better fight fraud and error through risk, prevention, data and enforcement techniques
- Develop capability in the public sector to find, prevent and respond to fraud both organisationally and individually
- Put performance at the heart of the public sector fraud conversation focusing on investments and outcomes

- Aim to be seen as a beacon of fraud and error expertise and a destination for those wanting to make a difference in fighting public sector fraud.

The PSFA structure is composed of three service and three functional areas, one of which is Practice, Standards and Capability (PSC). This central team supports the oversight and development of the Government Counter Fraud Profession (GCFP). The PSC works with a number of public bodies, via an oversight board, to agree the strategy, focus and products of the profession. The PSFA is also the home of the Centre of Learning for Counter Fraud, which is responsible for building a vibrant learning community, improving counter fraud capability and providing fraud leaders with industry leading skills.

A6. Government Counter Fraud Profession

The Government Counter Fraud Profession (GCFP) has a clear governance structure. Its board leads oversight of the profession, with senior members selected from public sector organisations with a mature response to counter fraud and economic crime. Member organisations vary in size and the number of staff they have working in counter fraud, but all have an equal vote on the board. The key principles when developing the profession, as agreed by the board, were Collaboration, Choice, Empowerment and Pace.

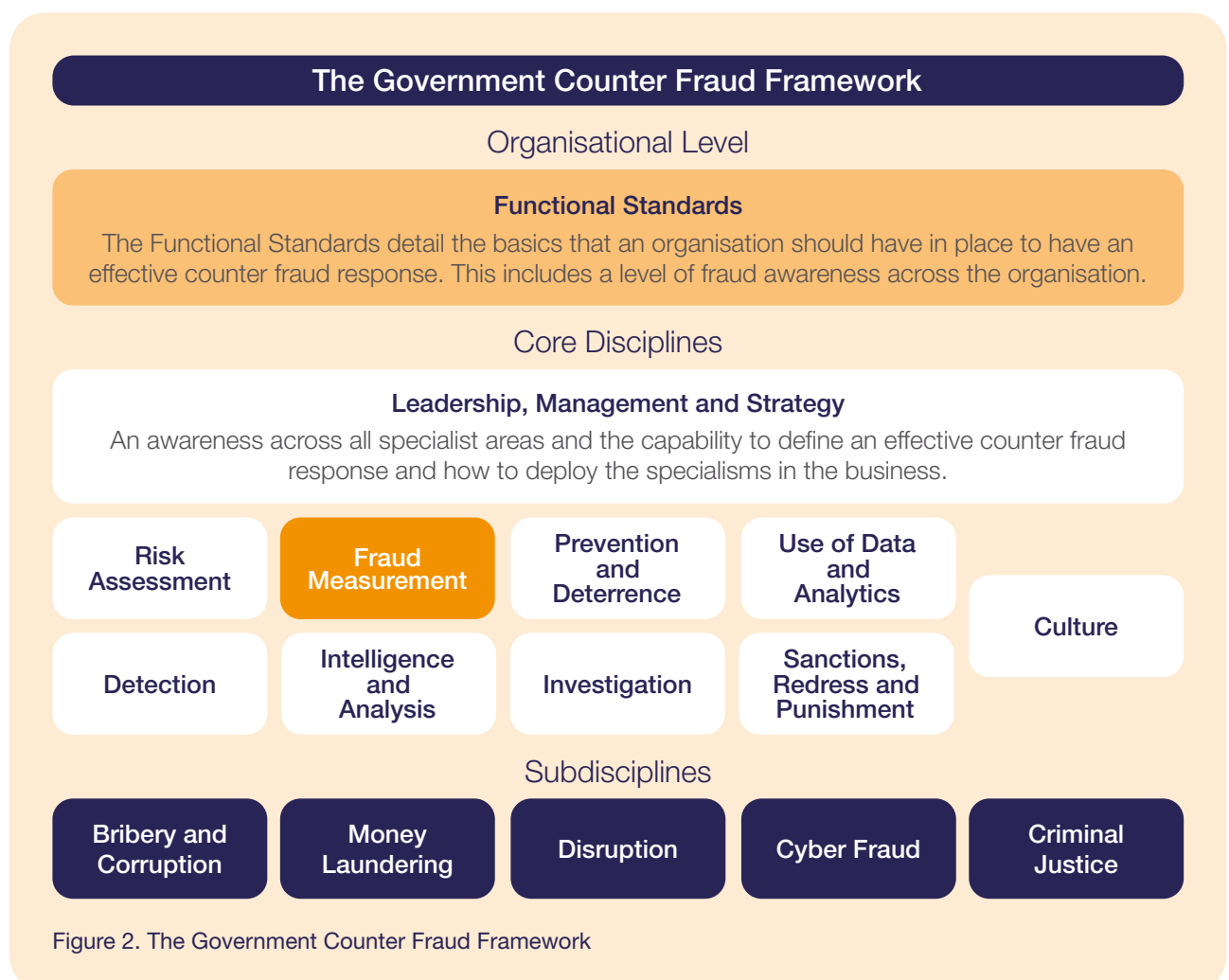
The GCFP board is supported by a Cross Sector Advisory Group (CSAG). This is made up of experts in counter fraud from a range of sectors, including academic, financial, legal and regulatory. The advisory group acts as a critical friend to the decisions made by the board.

3 <https://www.gov.uk/government/publications/public-sector-fraud-authority-mandate>

A7. Government Counter Fraud Framework

The framework covers the core disciplines and subdisciplines that a public sector organisation needs to counter fraud threat. Organisations will use these to different extents depending on the nature of their function and services, and the associated fraud threat, as assessed through their threat assessments and fraud risk assessments.

- **Organisational Level** – this is aimed at the organisation. It is covered by the [Counter Fraud Functional Standard](#). This states the basics that organisations should have in place to have an effective counter fraud response. It includes things like having a fraud risk assessment, a counter fraud policy and having fraud training and awareness across the organisation
- **Core disciplines** – the core disciplines include a functional leadership level (Leadership, Management and Strategy) for those who are responsible for co-ordinating an organisation's overall response to fraud. The main area is in the functional delivery level, this details the core disciplines that an organisation may use in an effective counter fraud response. Within these core disciplines are details of the knowledge, skills and experience needed to undertake these disciplines effectively
- **Subdisciplines** – the subdisciplines is an area of additional knowledge, skills and experience that enhance capability across a number of core disciplines.



The Fraud Control Cluster⁴

The Fraud Control cluster incorporates the Fraud Risk Assessment, Fraud Prevention, Fraud Detection, Counter Fraud Culture and Fraud Measurement disciplines enabling the development of a career pathway for the fraud control practitioner which is equitable with those of the other Government Counter Fraud Profession (GCFP) disciplines (such as Intelligence and Investigation). The cluster draws together the required knowledge, skills and experience practitioners and organisations can self assess against when building their capability. For membership of the Government Counter Fraud Profession as a Fraud Control Practitioner Member the requirement is to complete learning in the mandatory disciplines, namely Prevention and Fraud Risk Assessment and one of the elective disciplines being Fraud Measurement, Counter Fraud Culture or Fraud Detection.

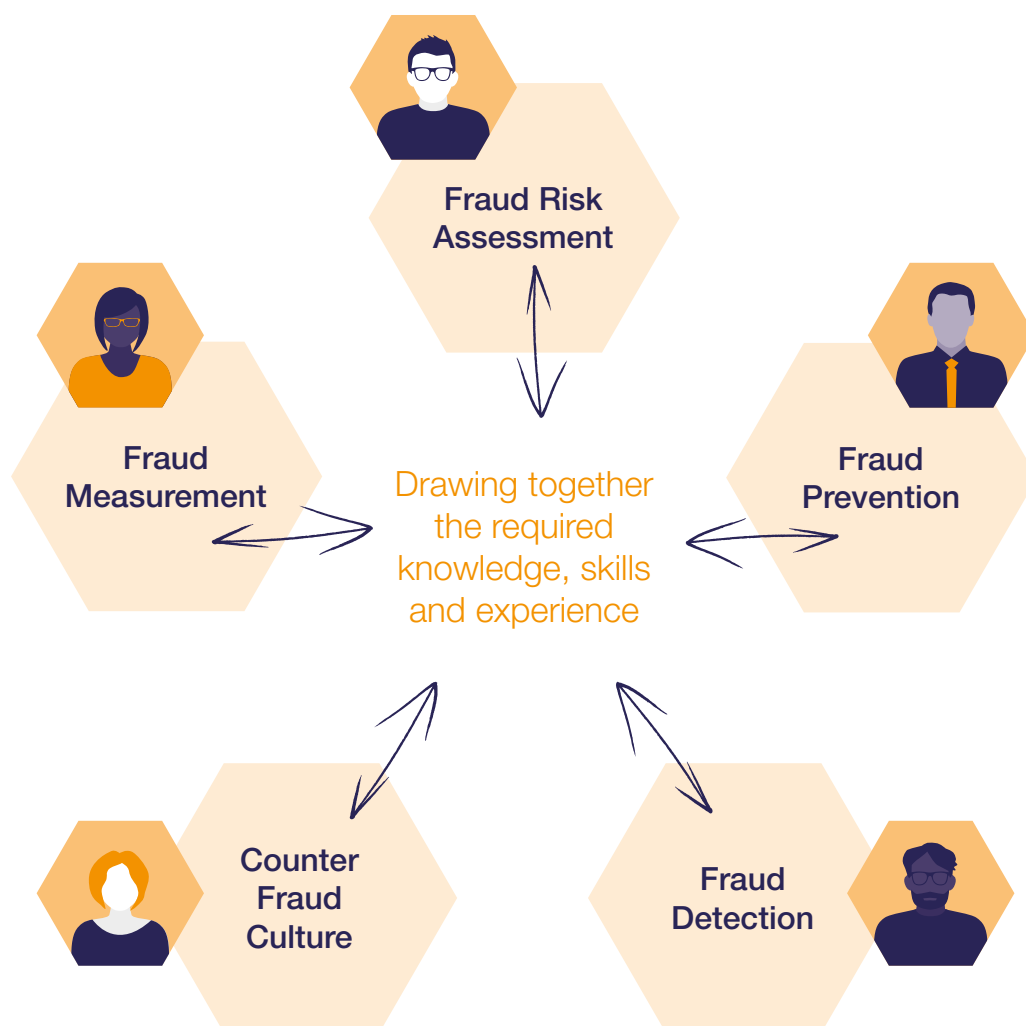


Figure 3. The Fraud Control Cluster

A8. Roles and Responsibilities

For the purposes of this standard, a practitioner will be operating within the counter fraud environment and will have the ability and opportunity to undertake and influence fraud measurement activities through the work they carry out, and in doing so produce reliable, high quality analysis that makes efficient use of resources which are value for money and improve counter fraud outcomes.

Leadership across an organisation should encourage measurement activity, seeking to find and quantify fraud in order to support effective risk management and governance, promote compliance with processes and controls, and ultimately refine and improve the overall organisational counter fraud response.

A9. Key Components Explained

Components outline at a high level the knowledge, skills and experience required for each core and subdiscipline. There are eight key components for the Practitioners Standard for Fraud Measurement. Each component has a series of elements, which are specific descriptors of knowledge, skills and experience required. These elements are then grouped into a competency framework.

Within the competency framework are two competency levels, these are Foundation and Practitioner. These levels can be used to identify progression within the standard. The framework helps to establish where your competency level is and where you have areas that you may wish to develop.





A10. Competency Levels

General rules about the competency levels are set out below

- **Foundation** is about having the knowledge
- **Practitioner** is about demonstrating the application of the knowledge.

B. Fraud Measurement Competency Framework

Practitioner Competency

The below competencies are required to attain Practitioner level. The full Fraud Measurement competency framework can be found at [Appendix 1](#). Guidance on terminology can be found in the [Glossary](#).

1. Counter Fraud, Bribery and Corruption Knowledge

- 1.1 Demonstrate and apply the relevant legislation (civil and criminal) and offences for fraud and bribery
- 1.2 Demonstrate knowledge of fraud, bribery, and corruption typologies and vulnerabilities across an organisation
- 1.3 Demonstrate knowledge of why fraud, bribery and corruption are committed across the public sector and its impact across society
- 1.4 Demonstrate knowledge of fraud landscape, scale and impact in the UK

2. Organisational Knowledge

- 2.1** Demonstrate the effective use of the different qualitative and quantitative research methods to obtain information from the organisation and its key stakeholders in order to gain an understanding of the areas at risk from fraud to inform areas of focus for fraud measurement

- 2.2** Demonstrate how to analyse and present information relevant for planning the fraud measurement programme and associated activities

- 2.3** Demonstrate an understanding of the organisational structure and responsibilities in relation to the fraud risk landscape when planning fraud measurement activities

- 2.4** Demonstrate how the Fraud Measurement programme fits into the assurance landscape of the organisation and how this relates to the role of other assurance activities

3. Fraud Measurement Planning

- 3.1 Demonstrate that the scope of the measurement programme provides assurance over the accuracy and completeness of fraud, bribery and corruption reporting
- 3.2 Demonstrate that the fraud measurement programme is aligned to the key fraud risks and main areas of spend and income for the organisation
- 3.3 Demonstrate that the fraud measurement programme is supported by an annual plan of measurement activities
- 3.4 Demonstrate the ability to establish objectives and scope for each measurement exercise ensuring the exercise is adequately resourced with appropriate skills, knowledge and expertise
- 3.5 Explain how and why each fraud measurement activity or exercise needs to be supervised and quality assured

4. Fraud Risk Assessment Skills

4.1 Demonstrate the appropriate use of fraud risk assessments in the context of both fraud measurement planning and individual measurement activities

4.2 Demonstrate how fraud measurement fits into the fraud risk management cycle in relation to reporting and monitoring prevented and detected fraud, control testing and fraud loss measurement exercises

4.3 Demonstrate how testing is focused on significant fraud risk facing an organisation

5. Statistical and Sampling Knowledge

- 5.1 Demonstrate that statistical sampling has been undertaken in the context of testing and measuring for fraud bribery and corruption
- 5.2 Demonstrate that the sample(s) selected are representative of the overall population to be tested and measured
- 5.3 Demonstrate that where a sub-population has been tested that this limits any estimate of levels of fraud, bribery and corruption to that sub-population rather than the overall population
- 5.4 Demonstrate the use of confidence levels when selecting the size of sample for testing
- 5.5 Demonstrate that test results from a sample represents a range of possible values in the total population and how the chosen sample size affects this degree of precision, or margin of error
- 5.6 Demonstrate the use of appropriate sampling methodologies within different testing scenarios

6. Identifying and Using Evidence to Test for Fraud

- 6.1** Demonstrate the use of different internal and external data sets and information to be used for comparative purposes and testing within the system/process being measured. Show how shortcomings in the data can affect subsequent testing, measurement and estimating of fraud

- 6.2** Demonstrate that a detailed test plan has been developed for each measurement exercise to be undertaken before testing takes place

- 6.3** Demonstrate consideration of the legal requirements around data handling and sharing as well as outlining the protocols and agreements needed to enable data sharing between organisations when obtaining data sets for testing

- 6.4** Demonstrate how to design individual tests within a fraud loss measurement exercise in order to determine whether or not fraud (or error), bribery or corruption has occurred

- 6.5** Demonstrate appropriate records have been designed and used for each test to demonstrate the approach taken and ensure consistency in testing

7. Estimation and Measurement

- 7.1** Demonstrate an appropriate use of testing to facilitate the measurement and estimation of fraud and error within a targeted population
-
- 7.2** Demonstrate how the results of testing have been reviewed, categorised and quantified in order to reach a conclusion as to whether fraud or error has occurred or if additional testing is required
-
- 7.3** Demonstrate that the results from fraud loss measurement testing have been used and extrapolated to measure and estimate the actual levels of fraud and error within the target population
-
- 7.4** Demonstrate the categorisation and quantifying of fraud measurement results distinguishing between detected, prevented and estimated fraud and error
-
- 7.5** Demonstrate an understanding of where benchmarking of fraud (or error), Bribery or Corruption measurement across the public sector would be helpful in putting results into context
-
- 7.6** Explain how to identify the drivers pertaining to fraud risks, how they can impact levels of fraud, and how the extent to which these drivers are increasing/decreasing can be measured through the development of fraud risk indicators
-
- 7.7** Demonstrate the calculation of ongoing savings arising from preventative action taken, using robust methodology
-
- 7.8** Explain how the effectiveness of the organisational counter fraud strategy, and related activities, is measured and monitored

8. Fraud Measurement Reporting

- 8.1 Demonstrate an understanding of the scope of fraud measurement reporting, including prevented and detected fraud, prevented savings and estimates of previously unknown fraud from control testing and fraud loss measurement exercises
- 8.2 Demonstrate that the results of fraud measurement and testing have been communicated to all key stakeholders
- 8.3 Demonstrate the ability to incorporate key findings from fraud measurement into reporting using metrics such as spend and activity levels to illustrate organisational vulnerabilities
- 8.4 Demonstrate that reporting acknowledges and recognises any limitations with estimates and measurement and where the potential for unknown fraud still exists
- 8.5 Demonstrate the establishment of a regular routine for fraud reporting, ensuring consistent updates and annual aggregation of results to monitor trends over time
- 8.6 Demonstrate how fraud measurement results are linked to the organisation's fraud appetite statement and defined tolerance levels, to support informed decision-making on control effectiveness and necessary actions to mitigate fraud risk

C. Guidance on Processes for Fraud Measurement

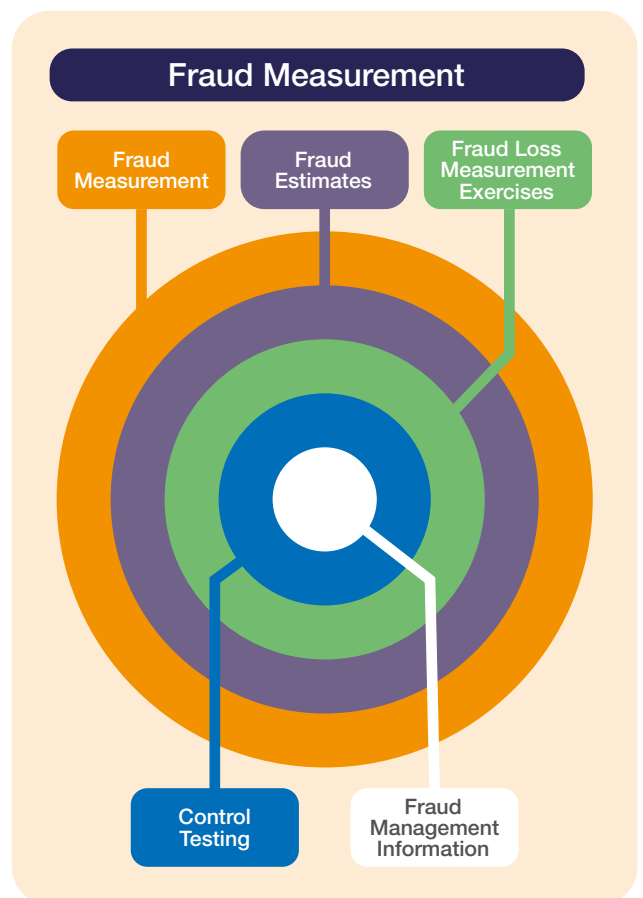
C1. Introduction

This guidance supports the standard for a fraud measurement practitioner. All processes and procedures should be regularly revised and evaluated to ensure they remain best practice. Set out below are the processes for undertaking, measuring and improving fraud measurement work. Fraud Measurement as a discipline includes Fraud Management Information, Fraud Estimate and Fraud Loss Measurement exercises as well as control testing and savings methodologies.

The scope of the Fraud Measurement discipline requires practitioners to:

- Understand the importance of measuring known fraud through the reporting of instances found through prevention and detection controls, and the estimation of the scope and level of unknown fraud
- Use fraud risk assessment knowledge and skills to understand organisational vulnerabilities to fraud by identifying key areas of fraud risk
- Understand the importance of establishing and maintaining reporting processes to collect data on instances of fraud and error found through business systems and controls, and ensure they accurately account for and report on prevented and detected fraud and error
- Run fraud testing exercises to measure and estimate levels of undetected fraud and error through fraud loss measurement exercises or control testing.

- Calculate prevented savings where new controls have been put in place
- Establish actual levels of fraud and error loss compared to sums recovered
- Understand the need for clear, accurate and persuasive reporting to communicate assessments, estimates and findings to engage with and influence senior leaders and key stakeholders about vulnerabilities to fraud.



C2. Identifying and Reporting Detected and Prevented Loss (Known Fraud)⁵

In order to understand the extent of fraud and error overall, we first need to measure the fraud and error we already know about.

Reporting of detected or prevented losses due to fraud and error is key to understanding the baseline level of known fraud faced by an organisation.

Regular fraud reporting should be established (at least quarterly) ensuring consistent updates and annual aggregation of results to monitor trends over time. A reporting process should connect all business units responsible for measuring and reporting fraud. Practitioners should ensure that reporting is comprehensive with input from all business units and activities, and that the details reported are complete, accurate and timely.

Business units should be instructed as to the types of information that needs to be collected, which as a minimum should include:

- **Numbers of cases and financial values for detected (post-payment) fraud and error losses**
- **Numbers of cases and financial values for prevented (pre-payment) fraud and error potential losses**
- **Recovery of detected fraud and error losses, including losses reported in previous periods.**

Data should be reported and collated according to a recognised fraud typology such as the one used by the Public Sector Fraud Authority to collate reported fraud across central government.⁶ Accompanying this should be a brief description of the fraud and how it happened, together with an outline of the scheme or payment/revenue stream where the fraud took place relevant to the reporting.



Reporting of detected or prevented losses due to fraud and error is key to understanding the baseline level of known fraud faced by an organisation

⁵ Also known as Fraud Management Information - see IPSFF Fraud Loss Measurement Framework

⁶ The Consolidated Data Return (CDR) mandated for central government - see [Appendix 2](#)

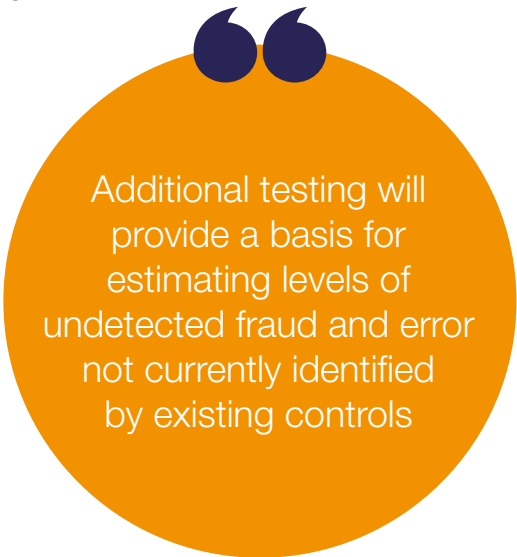
C3. Estimating Undetected Fraud and Error

Additional testing will provide a basis for estimating levels of undetected fraud and error not currently identified by existing controls.

This can be done by:

- **Fraud Loss Measurement Exercises** – testing primarily focused on residual fraud risk (and measuring associated losses) and/or;
- **Control Testing** – testing vulnerabilities in the operation of key counter fraud controls (and measuring associated losses to estimate levels of fraud and error occurring because of control failure), and/or;
- **Estimation** – using comparator data from similar schemes or data analytics (and potentially FLM results) to provide an estimation of likely losses in an area, without testing individual cases.

This is in line with the Control Evaluation and Reporting and Reviewing sections of HM Government's Fraud Risk Management Cycle.⁷



Additional testing will provide a basis for estimating levels of undetected fraud and error not currently identified by existing controls

Fraud Loss Measurement Exercises

Fraud Loss Measurement is designed to test the residual fraud risks themselves rather than the controls. Together the two types of testing complement each other as part of the control evaluation and monitoring phase of the HM Government Fraud Risk Management Cycle. However, Fraud Loss Measurement exercises will often identify control failures, and when this occurs these should be documented and fed back into the fraud risk assessment.

Where a fraud risk has been assessed and scored to have a high residual fraud risk, this implies that any controls in place are ineffective at mitigating that risk. It therefore follows that Control Testing would not be appropriate in such circumstances.

Instead, the testing needs to focus on the identified gaps and weaknesses in control in order to ascertain whether they have allowed fraud and error to occur and, if so, how much.

A fraud risk owner may seek assurance on the scale of the fraud problem caused by the identified fraud risks to ensure value for money before committing to any costly control improvements. Those commissioning and undertaking such exercises should focus on where the fraud risk assessment has identified weaknesses in control (that is, where a control is not designed, either entirely or partially, to mitigate a specific fraud risk). It is these gaps in control that are the focus of a fraud loss measurement exercise.

⁷ <https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

Reasons for Undertaking a Fraud Loss Measurement (FLM) Exercise⁸

There are three different drivers for undertaking an FLM exercise, linked to HM Government's Fraud Risk Management Cycle. We label these 'exploratory', 'performance', and 'assurance'.

Exploratory



An **Exploratory** exercise is undertaken in an area where there is high materiality (potential loss) in terms of expenditure or income collection, but where little is known about the levels of fraud, with only a minimal amount of fraud or error being detected and reported. This equates to an initial phase of the Fraud Risk Management Cycle to evaluate the effectiveness of controls against a reliable assessment of potential levels of fraud. The area selected should be one where there is considered to be a high risk of fraud and error loss, and an area that is not subject to regular "business as usual" testing that is already reported publicly, for example in published annual reports and accounts. In subsequent phases of the Fraud Risk Management Cycle estimates of unknown fraud will be revisited.

Performance



The '**Performance**' stage repeats a measurement exercise where additional controls have been implemented in response to levels of fraud found during an 'Exploratory' exercise. The purpose of a 'Performance' driven exercise is to ascertain and measure the effect those controls are having on instances of fraud.

Assurance



Once it has been demonstrated that controls are working as intended and are consistently effective, and estimates of levels of fraud are within accepted levels of tolerance, then occasional repeat Fraud Loss Measurement exercises may be undertaken as an '**Assurance**' phase to provide ongoing assurance that the risk of fraud is being contained within accepted levels of tolerance.

⁸ https://assets.publishing.service.gov.uk/media/67b85a45ba253db298782c0c/IPSFF_Fraud_Loss_Measurement_Framework_.pdf

Selecting an area for Measurement

An “area” selected for measurement activity can cover any process by which an organisation pays out expenditure or receives income. Consideration should be given to the financial size of the area, the inherent risk, whether intelligence, quality assurance work or other reporting indicates fraud and error are present, and what is known regarding the efficacy of the control framework.

An area is only suitable for selection and quantitative measurement if:

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

The process of selecting an area for measurement requires practitioners to identify areas of spend or income that are likely to present significant fraud risks. They should use either their organisation’s Enterprise or Thematic Fraud Risk Assessments or their own analysis, such as a Spend Area Assessment or similar (if necessary⁹), to identify areas where fraud is most likely to be found, and where fraud loss measurement exercises will add the most value by looking for and measuring instances of undetected fraud.

Step #1

As a **first step**, it is necessary to understand the spend/income profile of the organisation and the extent to which this is mapped onto the Enterprise FRA. It is important to recognise any significant areas of spend/income which are not represented on the Enterprise FRA and to flag these as potential gaps.

Step #2

The **second step** should be to map instances of reported fraud and error to each area of the Enterprise FRA – noting where levels of reported irregularity appear to be low or non-existent, and assessing the extent to which potential areas of undetected fraud may exist.

“Single Risk” Fraud Loss Measurement Exercises¹⁰

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 a small group of similar fraud risks (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.

Control Testing

The second half of HM Government’s Fraud Risk Management Cycle requires Fraud Risk Owners to evaluate and monitor the effectiveness of the controls in place to stop fraud from happening, or find it when it does happen.

The fraud risk assessment process will have identified relevant controls as they apply to each fraud risk identified.

Where a fraud risk has been assessed and scored to have a low residual fraud risk (but the inherent risk would be high), this implies that the controls in place have been designed to effectively mitigate that fraud risk.

However, the residual risk is only ‘low’ if the controls in place are, in practice, working effectively and correctly. In such situations, it would be advisable for testing to be undertaken to provide assurance that the controls are indeed working as intended in order to confirm the residual risk score indicated by the Full Fraud Risk Assessment.

Alternatively, a fraud risk owner might seek assurance through control testing where the fraud risk assessment has identified that certain controls had limitations which indicate that they might not always work effectively 100% of the time.

The purpose of control testing is to test the operation of key controls designed to combat fraud and assess whether they are working. This can be done at a relatively simple level whereby the control is repeated for a sample of transactions in order to test whether or not it operated correctly. This may provide suitable assurance for the fraud risk owner, **but is not of itself fraud loss measurement.**

¹⁰ https://assets.publishing.service.gov.uk/media/67b85a45ba253db298782c0c/IPSFF_Fraud_Loss_Measurement_Framework_.pdf

Fraud measurement in the context of Control Testing involves testing a statistically valid sample and quantifying and recording the instances of fraud or error, and the associated value, attributable to the control failure. This allows those results from that sample to be extrapolated to determine the effect of the control failure across the system as a whole.

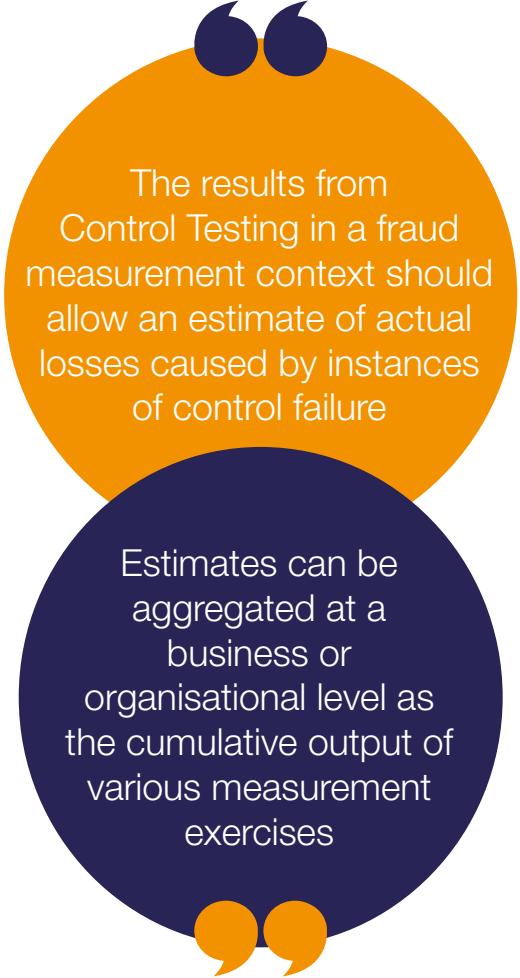
The approach taken to sampling, testing and reporting should follow the guidance outlined for Fraud Loss Measurement in

[Sections C5 \(planning\)](#); [C6 \(sampling\)](#); [C10 \(estimating\)](#) and [C12 \(reporting\)](#).

The results from Control Testing in a fraud measurement context should allow an estimate of actual losses caused by instances of control failure. The results of such testing can be used by the fraud risk owner to determine whether control improvements would be cost effective. The results of testing should also be used to update the fraud risk assessment.

Estimation

Estimation can happen at different levels. There will be the 'scheme' level where levels of fraud and error relating to specific fraud risks can be estimated from a single FLM exercise. As departments grow in fraud measurement maturity then estimates can also be aggregated at a business or organisational level as the cumulative output of various measurement exercises.



The results from Control Testing in a fraud measurement context should allow an estimate of actual losses caused by instances of control failure

Estimates can be aggregated at a business or organisational level as the cumulative output of various measurement exercises

Estimating Undetected Fraud and Error

Area selection: Indicators of good quality	Area selection: Indicators of poor quality
There will be a clear rationale to explain the selection of an area for fraud testing, including: • Being able to demonstrate why the spend area is vulnerable to fraud, not just that it is labelled 'high risk' • Reasoning, other than the size of the spend area (i.e. weak controls, lack of intelligence, high volume of fraud referrals) • Critical evaluation of the spend area against other spend areas identified • Reference to evidence or intelligence that demonstrates why spend area is high risk or a good candidate for testing in the context of the Department's Enterprise (organisational) Fraud Risk Assessment • Providing persuasive reasons why fraud and error is likely to be found.	Evidence for selection of areas for testing will be undermined by: • Describing the spend area as high risk without reasoning or justification • A failure to demonstrate why the spend area is high risk, or why the spend area is a good candidate for testing • No evaluation of other possible candidate areas • No reference to Enterprise (organisational) Fraud Risk Assessment.

C4. Carrying Out and Adapting a Full Fraud Risk Assessment

A Full Fraud Risk Assessment (Full FRA) is key to understanding how fraud could happen within the target area for which fraud measurement and assurance is required.

This might be through a failure in the operation of controls or flaws in the design of the controls when applied to specific fraud risks. Section C3 outlines how both Fraud Loss Measurement and Control Testing play an important role in providing assurance and measuring the extent to which undetected fraud and error are occurring.

In relation to Fraud Loss Measurement, understanding how fraud can occur (the fraud risks) helps identify particular fraud risk exposures (residual risks) that might have been exploited. Testing of those exposures will then build understanding by enabling measurement of levels of underlying and previously undetected fraud resulting from those residual fraud risks.

It is therefore essential that a good quality, up to date, Full FRA is available before a Fraud Loss Measurement or Control Testing exercise commences.

The process for producing the Full FRA is the same as is described in the GCFP Standard for Fraud Risk Assessment^{11 12}

1. Understand the organisational landscape
2. Research to identify known risks
3. Identify, categorise, and define risks
4. Identify risk owner and evaluate inherent risk
5. Identify controls, assess their effectiveness, and evaluate residual risk
6. Prioritise residual risks against fraud risk appetite.

However when building a Full FRA for the purposes of Measurement, you also need to consider:

- How the identified risks can be tested to see if fraud has occurred
- What evidence is available to enable this testing to happen.

When building a Full FRA consider the following:-

Identifying fraud risks

View the target spend area through different perspectives to help provide a comprehensive list of fraud risks to identify how fraud could happen.

One perspective could be identifying risks from each of the following three lenses:

- The eligibility criteria for making a payment or receiving an income
- All the individuals involved, both internally and externally
- Each step of the process from end to end.

Another perspective could be to consider how different fraud offences could occur, such as:

- Information that could be misrepresented
- Information that might not be declared when there is a responsibility to do so
- Positions of responsibility that could be abused for fraudulent purposes.

These identification processes should be creative, considering all the different ways in which someone committing fraud might operate, and remembering that different individuals can act fraudulently at different points in the process, including those applying for funding, employees, contractors, suppliers, etc.¹³

11 <https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

12 <https://www.gov.uk/government/publications/full-fraud-risk-assessment-practice-note>

13 <https://www.counterfraud.gov.au/learn-about-fraud/types-fraudsters>

The process should also be collaborative, involving those who understand the relevant policies, processes, systems and behaviour of individuals and teams involved. Collaboration can also help spark ideas about ways in which the scheme could be defrauded.

Defining the fraud risks

A Full FRA requires descriptions of identified risks to be very specific about how individual instances of fraud could occur, rather than generalised statements about fraud happening.

For each risk, the Actor, Action, and Outcome must be clearly defined and articulated. This identifies who commits the fraud (actor), how they do it (action) and what the impact is (outcome), which ensures clarity and avoids overly generic risk descriptions. Outcome should consider all relevant factors, such as social impacts, physical impacts, reputational impacts etc. and not just financial impacts.

The more specific the risk description is, the easier it is to identify associated controls and the remaining residual risk, and also determine how testing could show if that risk has occurred.

Identifying controls

A control refers to any action that could mitigate against a specific fraud risk either through prevention or detection activities. Be sure to identify how the control affects or could affect the fraud risk.

Ensure that the type and action of any relevant control is assessed in relation to a specific fraud risk, with a clear explanation of how and the extent to which each control is designed to mitigate the risk in question.

This may include the absence of one or more types of control, for example controls that would prevent or detect fraud that have not been implemented, or flaws in the operation of implemented controls that mean that it may have limited effectiveness in controlling a specific fraud risk.

Identifying residual risk

Residual risk refers to the risk that remains after controls have been applied, that is, how fraud can still happen even with the current controls in place.

It is important to describe the specific ways in which the fraud risk could still occur, and how the limitations of existing controls could enable the fraud to happen.

For the purposes of fraud measurement, describing the residual risk specifically and in detail will help to later identify evidence that could be used for testing to indicate whether the fraud is occurring.

Assessing the quality of a Full Fraud Risk Assessment

In some instances, practitioners undertaking a Fraud Loss Measurement exercise may be given a pre-existing Full FRA completed by someone else. A Full FRA informs the design of effective tests to find previously undetected fraud so, if the Full FRA is vague, incomplete, or of poor quality, any subsequent testing will be unfocused and unlikely to successfully identify or accurately measure the true level of fraud loss. Practitioners should be able to assess the quality of an FRA before commencing a Fraud Loss Measurement exercise.^{14 15}

14 <https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

15 <https://www.gov.uk/government/publications/full-fraud-risk-assessment-practice-note>

Carrying out a Full Fraud Risk Assessment for measurement

Consideration	Fraud risk assessment: Indicators of good quality	Fraud risk assessment: Indicators of poor quality
Defining the fraud risks To identify associated controls and the remaining residual risk, and to determine how testing could show if that risk had occurred.	Fraud risk is clearly described and can be understood by a non-expert and details specifically: who could commit the fraud, how the fraud could take place, and the consequences (i.e. actor, action, outcome).	Fraud risk outlined is not clear to a non-expert, or is a business/compliance risk rather than a fraud risk.
Identifying controls	The control can be understood by a non-expert, and terms, roles and documents are explained.	The control is not clear to a non-expert or does not explain how it affects the fraud risk.
	Controls are described in terms of the fraud risk and are specific about how they affect the fraud risk.	
Identifying residual risk Help to later identify evidence that could be used for testing to indicate whether the fraud is occurring.	Identifies specific actions that could allow fraud to take place even with the control in place, in significant detail, and describes the full extent of the limitations of controls in relation to the fraud risk.	Does not cover how fraud could still be committed even with the control in place, or uses one-word descriptors (e.g. low/medium/high).
	Residual risk explained in detail, and relates back to the control and to the specific fraud risk.	
	Terms, roles or documents referred to are explained as to what their function is in relation to the residual risk.	

After the Full FRA - Additional Stages for Fraud Loss Measurement (FLM):

Stage #1

Categorise the internal and external evidence or comparator data available for testing

Once the fraud and error risks have been assessed, the extent to which these risks can be measured must be determined. This will depend on what comparator data exists to provide evidence of fraud and its availability, completeness and quality.

Comparator data is data which can be used to validate existing data and identify non-matching attributes and anomalies which indicate if fraud or error has occurred.

Existing controls might use comparator data as part of the authorisation or approval process. Such data would seek to validate information provided by an applicant or claimant (for example). It is useful to understand this so that FLM testing can go beyond anything the control currently does.

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 is external to or not used in the decision process or at payment
- External data or evidence independent to the organisation not used in the decision process or at payment.

Once identified, comparator data must be evaluated in terms of its availability, quality and completeness. The evidence may be stored elsewhere, collected and held by another organisation, or may have been discarded or lost. A fraud measurement practitioner must consider the quality of the data, its accuracy, age, reliability and how it is compiled and stored in order to understand the limitations this may have when undertaking testing.

If the evidence is out of date, collected in an unreliable way, or too ‘high level’ to be useful, it is unlikely to produce a reliable estimate of levels of fraud and error.

This categorisation informs risk selection and feasibility. For the detailed process of identifying and validating the actual evidence to be used in testing, refer to Section C8.

Identification of evidence or comparator data available for testing:

Availability of comparator data: Indicators of good quality	Availability of comparator data: Indicators of poor quality
The possible range of evidence has been researched and is clearly explained, including explaining terms, roles and documents so that their function is understood.	The range of possible evidence available for testing is limited, or is vague and not clearly explained (for example listing sources of data such as ‘contract’, ‘application form’ without specifying what that data is).

Stage #2**Select fraud risk(s) to test**

Once all of the fraud risks have been identified and the associated controls, residual risk and potential evidence and comparator data available for fraud testing have been identified, the next step is to select which fraud risks to test.

The number of risks selected should be based on the type of testing proposed and the resource available. The fraud measurement practitioner must document the reasons why a fraud risk has been selected for testing. Relevant factors would include the residual risk score and the extent to which comparator data is available for testing fraud occurring through that residual risk.

It is also important to consider whether the evidence available is likely to allow you to reach a conclusion on whether an individual case has had fraud or error occurring.

It is important to consider whether the evidence available is likely to allow you to reach a conclusion on whether an individual case has had fraud or error occurring

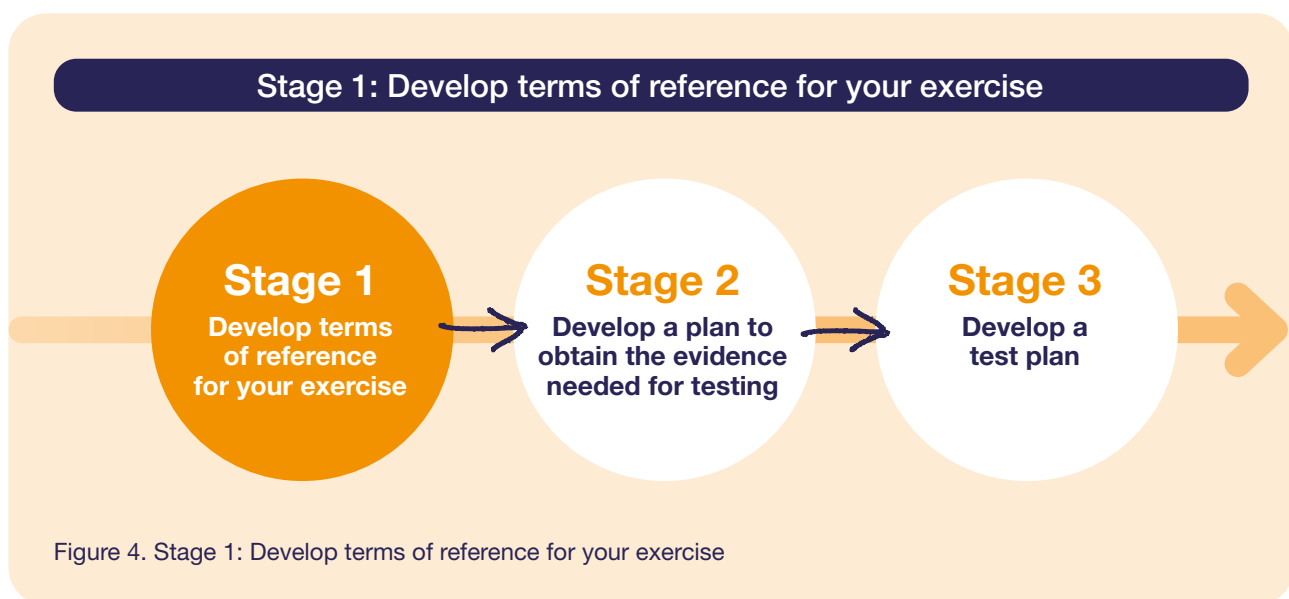
Selecting a fraud risk to test for Fraud Loss Measurement

Fraud risks selected for testing: Indicators of good quality	Fraud risks selected for testing: Indicators of poor quality
Use a Full Fraud Risk Assessment that has identified and assessed a wide range of fraud risks.	Significant areas of fraud risk have not been included, or the specific items are not understandable as fraud risks.
An achievable number of appropriate risks have been chosen for testing, and it is clear what evidence can be used for testing.	Too many or too few risks have been chosen for testing and it is not clear how they will be tested for fraud.
There is a clear, evidence based rationale for the selection of the fraud risks to be tested.	There is no explanation why fraud risks have been selected for testing, or the explanation is not supported by evidence.
Evidence chosen for testing is likely to allow conclusions to be drawn about whether fraud or error has taken place.	It is not clear how the evidence will be used to identify if fraud or error has taken place.

C5. Planning Fraud Loss Measurement

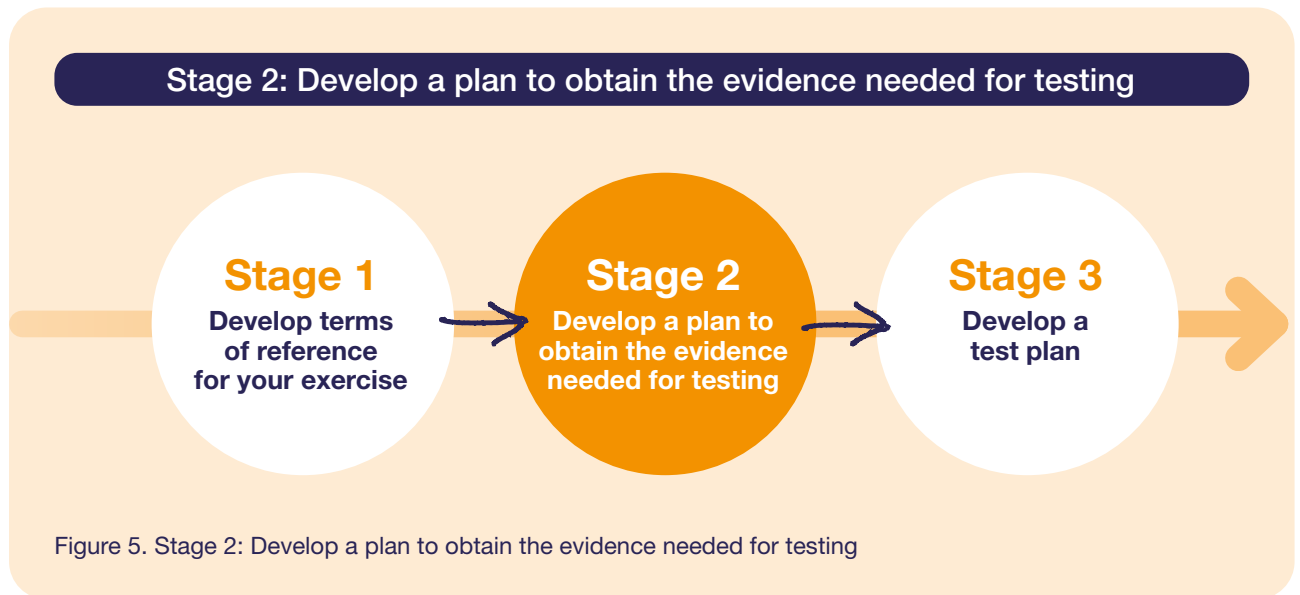
Following the identification of areas of high residual fraud risk, a decision will need to be taken about whether the cost of conducting a bespoke fraud measurement exercise is justified. An outline plan of the testing requirements should be produced to inform that decision. This should consider the proportionality of the cost of undertaking the exercise versus the assurance to be gained. Once approval is given, then a more detailed test plan will be required to ensure that tests undertaken will be fully effective and find fraud if it is present.

The following stages should be covered when planning a fraud measurement exercise:



The terms of reference should:

- Have a clear objective:- to find and measure fraud
- Cover the scope of the exercise
- Describe the resource requirements including the amount of time it is likely to take to collect data/information from third parties and undertake testing
- Secure an appropriate Senior Responsible Officer for the exercise who has the authority to agree and secure necessary resources, review progress and sign off on decisions.



Research to identify external evidence that could be used as comparator data. Sources of data¹⁶ or information¹⁷ that might be available for testing include:

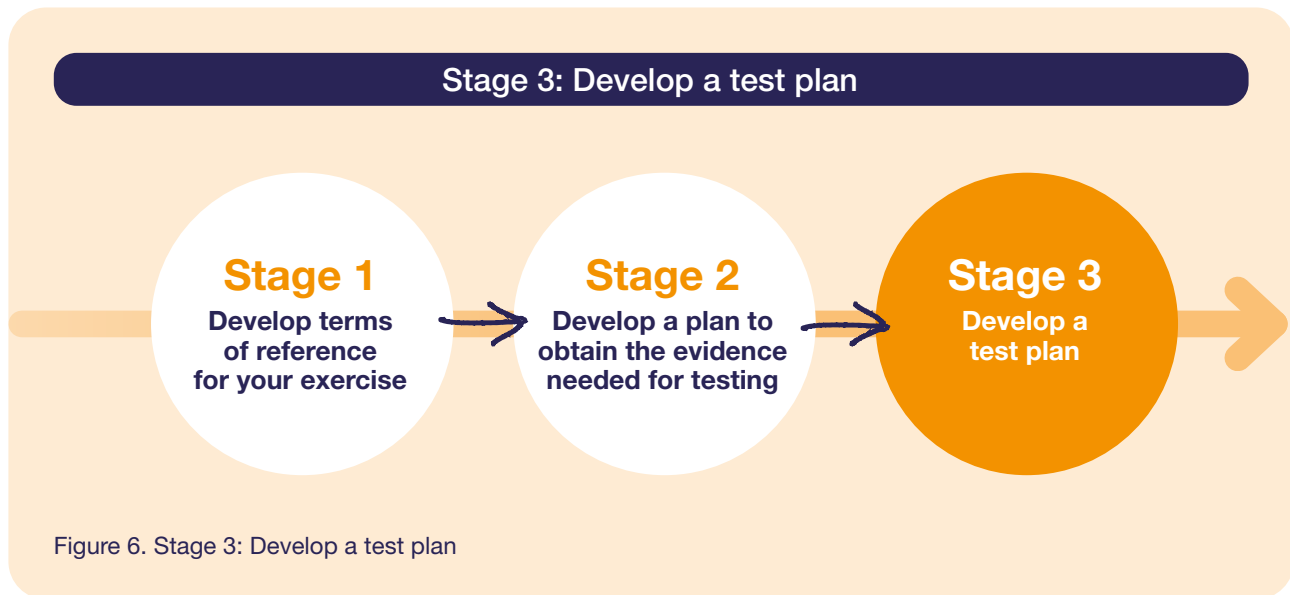
- Internal data/information held within the scheme or process being tested
- Internal data/information held elsewhere within the organisation
- Data/information that can be self-generated through analysis or through an inspection or site visit
- Open-source data/information
- External data/information held by other public sector bodies and/or private companies. For this, there will be a need to arrange a data share agreement with the third-party organisation(s).

Key steps to consider for data sharing

- Identify the source for data sharing
- Refer to the Full FRA to help identify the intended use of data
- Contact the Departmental Data Protection Officer for help in completing a Data Protection Impact Assessment (DPIA)
- Use the source for the data and the intended use to inform and implement a data sharing agreement
- Make use of the Digital Economy Act 2017, which provides a legal basis for data sharing.

¹⁶ Data can be defined as facts and statistics collected together for reference or analysis.

¹⁷ Information can be defined as the giving or receiving of knowledge and can be written, spoken or communicated by conduct.



The test plan should scope and document the following:

- Each fraud risk to be tested
- Rationale for testing a specific risk
- Consideration of how the test population of spend or income will be sampled, to ensure the sample is representative of that population
- An outline of how each fraud risk will be tested
- Ensure planned testing goes beyond testing controls and will enable any fraud or error found to be quantified
- Consider the use of data analytics packages to identify irregularity and assist with estimating fraud losses, particularly in areas where fraud measurement is more difficult and resource intensive
- The evidence to be used to reach a conclusion on whether the transaction was correct or fraud or error.

C6. Choosing Statistically Valid Samples for Testing

When testing for instances of fraud, ideally, the entire population would be examined. Advancements in technology, such as data analytics, are increasingly making this possible. However, if this approach is impractical or too resource-intensive, statistical sampling offers an effective alternative.

In statistical sampling, a subset (the 'sample') is drawn from the wider, entire population in a way that represents as closely as possible the population from which it was drawn.

The results from testing a sample are then applied and interpreted to the population from which the sample was drawn.

Therefore, the sample must be selected using a methodology that allows it to be representative of the target population. It 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 with defined possible margins of error.

All methodologies must:

- 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

Note – Non-probability sampling is not an acceptable sampling method.

This means that unlike probability sampling, sampling is based on subjective judgement, such as what the tester thinks a typical sample would look like, or selecting sampling units which are the easiest to obtain or test (for example convenience sampling). If there is no random selection, then the probability of any unit being chosen is unknown, so it would be impossible to calculate sampling error or extrapolate results to the wider population.

Step #1

Determine the sampling methodology

Different sampling methodologies can be used. Different options may be less or more suited to a particular exercise depending on the characteristics of the area being tested, and the resources available for testing. In choosing a sampling methodology it is important to consider the advantages and disadvantages of each methodology and to select a methodology most suited to the characteristics of the target population and the testing that is to be carried out.

Acceptable sampling methodologies are:

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.

Advantages:

- Easy to implement
- Each member of the population has an equal chance of being chosen
- Free from bias

Disadvantages:

- A complete list of the population may not be available
- Smaller subgroups within the population may not be present in the sample
- Testing may be difficult and resource intensive if, for example, site visits are required where the population has a wide geographic spread.

Systematic sample

For this sampling method, all data is sequentially numbered and every nth piece of data is chosen. The number n is chosen by:

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

Advantages:

- Easy to select sample
- Evenly spread over entire population.

Disadvantages:

- May be biased when the pattern used for the samples coincides with a pattern in the population.

Stratified Random 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, transaction size or approved suppliers.

Within the strata, a random sampling method such as Simple Random Sampling is used to choose the sample within each stratum. It is important that the sample selected for each stratum is weighted to reflect the size of that stratum in relation to the rest of the strata. For example, if the strata are geographical regions and region A has 100 transactions, and region B has 50 transactions then the sample for Stratum A would be twice the size of the sample for Stratum B.

The choice and selection of strata is based on a belief or 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 pre-conceived 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. This means 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 be taken to ensure that test results are interpreted for each stratum first before aggregating to reflect the overall population.

Advantages:

- Strata can be proportionally represented in the final sample
- It is easy to compare subgroups
- Can be used to target sub-population for testing, however care should be taken when estimating fraud levels for the population if 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.

Disadvantages:

- Information must be gathered before being able to divide the population into subgroups.

Monetary Unit Sample

Monetary Unit Sampling (MUS) is based on attribute sampling techniques and each test seeks to identify samples that can be placed into one of two classifications: 'exception' (e.g. an instance of fraud or error) or 'no exception'. It turns monetary amounts into units for example, a grant payment of £50.00 contains 50 sampling units.

Once the size of the sample has been determined, the selection is made by dividing the total value of the population by the sample size. This will give an interval of 'n' £ (pounds). The population is then arranged into a logical order (usually by date). Selection is made by working through the population by cumulative value to identify each occurrence of the "n'th" £(pound) which represents the sampling unit at each of the pre-determined intervals. The claim, payment or invoice to which this 'n' £(pound) belongs is then selected for testing.

In populations where there is a relatively low number of units (such as a programme containing a small number of large projects) then consideration should be given to using the transaction level as the sampling unit in order to have a sufficient sample size.

Advantages:

- MUS is a value-weighted selection whereby sample size, selection and evaluation will result in a conclusion in monetary amounts.

Disadvantages:

- MUS will not be suitable for areas where the fraud risk is higher for small payments rather than larger payments such as a grants programme where large grants may be tightly controlled, but there is lots of residual risk exposure around small grants (e.g. if based on self-declaration).

Cluster sample

In cluster sampling, the population is divided into naturally occurring groups (clusters) of individuals, such as those in a geographic region, cities, schools, age demographic or households. Random sampling is then used to select one or more of those clusters from the collection of entire clusters. For example, if the cluster was geographic regions then the sample might be based on one or two of those regions. Testing would then either select every individual within that cluster or, if that would be too many, randomly select some of the individuals within the chosen cluster(s) to represent the whole population.

Advantages:

- Cuts down the cost and time by collecting data from only a limited number of groups
- Can show grouped variations.

Disadvantages:

- It is not a genuine random sample
- The sample is less likely to be representative of the population.



Cluster sampling cuts down the cost and time by collecting data from only a limited number of groups

Step #2**Determine the size of the sample**

In determining the size of the sample to be selected, there are two considerations. Firstly, the degree of confidence that the sample selected accurately reflects the population from which it is drawn. Secondly, 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.

The degree of confidence that the sample represents its parent population is known as the Confidence Level and is expressed as a percentage. For example, a 95% Confidence Level that the sample selected accurately represents the parent population.

The degree to which test results accurately represent the actual rate of error or incidence of fraud within the population is known as the Margin of Error (or confidence interval). This is expressed as the percentage by which the 'true' rate of error may differ (plus or minus) from the actual rate of error found from testing the sample. For example, a sample with test results showing a level of fraud of 5% with a margin of error of $\pm 2\%$ will mean that the 'true' rate of fraud within the parent population is expected to be within the range of 3% - 7%.

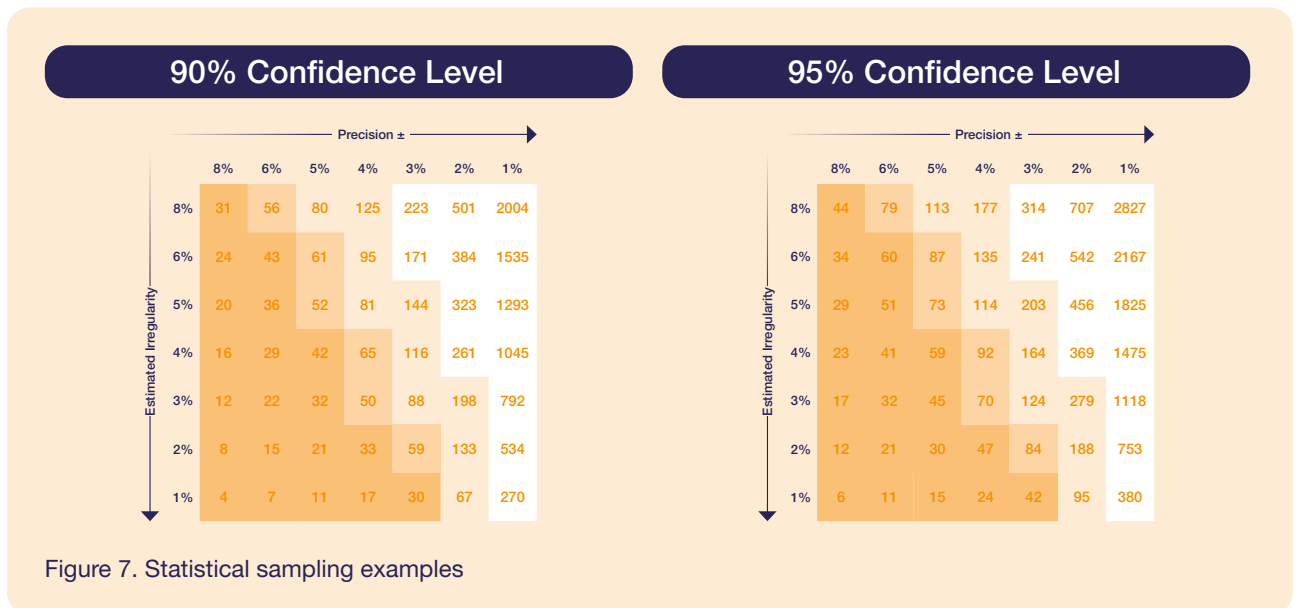
Step #3**Determining the desired confidence level and margin of error**

Fraud measurement practitioners should aim to achieve the highest statistical precision possible within the resources available. A 95% Confidence Level and a Margin of Error (or confidence interval) of $\pm 1\%$ is generally considered best practice in fraud and error measurement. Dropping the confidence level as low as 80% and the margin of error to $\pm 2.5\%$ is acceptable.

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

Depending on the type of sampling selected different formulas can be used, but the table below (based on the simple random sampling for attributes in the NAO Sampling guide)¹⁸ gives an idea of different sample sizes required.

18 <https://webarchive.nationalarchives.gov.uk/ukgwa/20170207052351/https://www.nao.org.uk/wp-content/uploads/2001/06/SamplingGuide.pdf>



The above samples are targeted at identifying whether an attribute is present in a population, rather than the frequency of its occurrence. The advantage of this is that it will give sample sizes that will be more manageable for departments. The disadvantage is that the samples at the lower end of the spectrum will be less able to be extrapolated across the overall population to demonstrate the spread of irregular spending. As an example, using the recommended attribute of 5% irregularity, the sample size for 90% confidence and a precision of +/- 2% would be 323 items.

This approach sets sample sizes based on the likelihood of irregularity, regardless of the size of the population that is being tested.

Statistical sampling: Indicators of good quality	Statistical sampling: Indicators of poor quality
Methodology of choosing the sample is clearly described, can be demonstrated to be appropriate to the population being sampled, and is understandable to a non-expert.	Methodology for choosing the sample is not clearly described and understandable to a non-expert, or has not been recorded.
Clear articulation of how the sample represents the overall population, including any exclusions and the reasons for exclusion.	Unclear or no explanation of how the sample chosen reflects the overall population.
If the sample includes different categories (for example low/high risk, or low/medium/high value), then the process for deciding the categories is explained, and how it impacts the irregularity rate being applied to the overall population and spend area.	If the sample includes different categories (for example low/high risk, or low/medium/high value), but the process for deciding on these categories is not clearly explained, and/or the impact on the irregularity rate being applied to the overall population and spend area is not considered.
The sample size is sufficient to allow statistically meaningful and valid conclusions to be drawn from the results of testing.	An insufficient sample size that does not allow any meaningful interpretation and extrapolation of the results from testing.

C7. Other Sampling Methods

For a Fraud Loss Measurement exercise we use random based sampling methods that are statistically valid in terms of confidence levels and precision. Without this it is not possible to extrapolate the results across the wider population to estimate levels of fraud and error.

However, it is recognised that such methods may not be possible or the most appropriate in certain circumstances. It will sometimes be more appropriate to test using a risk based sample rather than a random based sample, particularly if the alternative would be to not test at all. However in these cases the results cannot be used and extrapolated outside of the test sample.

For example, benchmarking is a more appropriate method for measuring the effectiveness of a Counter Fraud Strategy, by comparing its outputs and outcomes with other organisations (and equally random sampling is not appropriate in this context). Similarly, modelling is an alternative way of measuring levels of fraud by combining data from various sources with assumptions to produce an estimate of the possible range of fraud and error. For example, some public bodies model income evasion by comparing actual receipts from customers against the receipts they would expect to receive based on other information sources.¹⁹



Evidence is essential to fraud measurement

C8. Identifying and Selecting Evidence/Test Data

Evidence is essential to fraud measurement in order to check the validity of each attribute or item within the sample.

Each sample needs to be rigorously investigated, by examining all the information that can be lawfully and appropriately accessed, in order to verify and validate data and information held within the area of spend or income being reviewed and measured.

This requires comparator data – data which can be used to validate existing data and identify non-matching attributes and anomalies which indicate if fraud or error has occurred.

Identifying comparator data to be used as evidence in testing for fraud:

To identify suitable comparator evidence as test data, it is necessary to consider all the information that may be available (both internal and external to the organisation) to help determine the presence of correctness, error or fraud. Engaging with those who work in the area being tested can be a useful way of identifying potential evidence.

19 <https://www.nao.org.uk/wp-content/uploads/2025/02/estimating-and-reporting-fraud-and-error.pdf>

Evidence can therefore fall into two categories:

- **Firstly**, data or evidence collected or held by the organisation and used within the particular process or scheme being tested. For example: data used to decide on the eligibility of someone to be accepted as an employee, supplier or recipient of a grant or benefit, or in order to make a payment.
- **Secondly** data which is outside of this process or scheme which can be used for testing purposes and help verify and validate the accuracy of the data already held. This second group of data can fall into three categories:
 - **Internal:** data or evidence collected or held by the organisation but not used in the decision process or at payment
 - **Internal (or external):** data which can be generated through carrying out, for example, a physical check, a site visit or an inspection
 - **External:** data or evidence external to the organisation not used in the decision process or at payment. This may be open-source data, or data with restricted access that is owned by another organisation.

The fraud measurement practitioner should seek to identify and document all the possible sources of data that might be used to test for incidences of fraud or error.

It is important that testing involves using evidence from the second group that is outside the scheme or process being tested. Otherwise if only data that is internal to that scheme or process is used it is likely that testing will be focussed on testing controls and not looking for evidence that indicates that fraud has taken place. The next stage is to consider the availability of each possible data source, in other words who owns the data and what steps would be necessary to obtain it.

This could include the need to consider data sharing agreements and use of legislation such as the Digital Economy Act 2017 to obtain the data. Consideration should also be given as to what data products may already be available that could be used to validate whether fraud or error has occurred, such as the National Fraud Initiative.

Example: In the first category, an individual might claim an age-related benefit by providing a date of birth. The original process might validate the claim on the basis of whether the date of birth makes them eligible. However, there is a possibility that the date of birth could have been misdeclared. So, comparator data from the second category might seek to validate this. This might include other data held internally which provides details of that individual; use of an inspection to generate comparator data by asking to see valid ID documentation; or access to data sets held by other organisations which would include details of age and date of birth.

Evaluating Comparator Data

Once identified, it is necessary to evaluate the format and quality of the data to be used and how this could affect the quality and results of testing. This includes ascertaining the data fields available, the reliability of the collection method, and how recent, accurate and complete it is likely to be. If the evidence is out of date, collected in an unreliable way, or too 'high level' to be useful, it is unlikely to produce a useful estimate of fraud and error levels.

Evaluating comparator data: Indicators of good quality	Evaluating comparator data: Indicators of poor quality
Available comparator data is clearly documented and explained, including how it could be used to test for fraud.	Comparator data is not clearly documented or explained, or does not describe how it could be used to test for fraud.
A wide range of external comparator data has been considered and obtained for testing comparators held within the organisation but not used in the decision or at payment, as well as evidence held by external organisations.	Only internal comparator data (already held and used as part of the decision or at payment) has been considered.

C9. Testing

The testing itself will be unique to each exercise, so this standard does not describe this element of the process in detail.

However, it will usually be a case of taking each sampling unit and assessing it against processing criteria, controls and evidence and determining whether:

1. The payment or transaction item is correct and valid or;
2. Whether fraud or error has occurred.

It can be useful to start with the premise that every unit in the sample is fraud or error, and then seek to find sufficient proof that they are not, and if not continue to consider them potential fraud or error with additional testing required. If no further tests can be identified and we still cannot make a decision whether the payment was regular, the sample item should be classified as 'unresolved'.

It is common that testing will conclude on cases where we have enough evidence to know the payment should not have been made, but insufficient evidence to confirm whether it was due to fraud or due to error.

Different levels of testing are required to be able to definitively classify a case as fraud or error. Testing of the sample might find some cases 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 need to 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 the testing into distinct phases, where a provisional classification is made and revisited at each subsequent phase:

Phase 1 – Internal evidence review

Phase 2 – Internal and external comparator evidence review

Phase 3 – Further review based on cases where further evidence is needed

Phase 4 – Final review and determination.²⁰

It is important to update the FRA with the insights generated from the testing. As well as influencing risk scoring updates, this may include the identification of new fraud risks that had not been considered before. This is a common occurrence as the FLM exercise improves our understanding of how a programme can be defrauded.

Ensuring Consistency

It is important to ensure consistency in testing, particularly where this is being done across different geographical locations by different individuals. Ways of achieving consistency should include:

- Training of staff undertaking measurement activities
- Providing written guidance
- The use, and design of, documents which outline the tests to be performed and provide contextual information about expectations for how they will be performed
- Supervision and quality assurance reviews.

²⁰ <https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/fraud-loss-measurement-framework-html>

Testing: Indicators of good quality	Testing: Indicators of poor quality
Evidence sources are clearly described and understandable to a non-expert.	Significant areas of fraud risk have not been included, or the specific actions are not understandable as fraud risks.
Evidence sources provide new information that was not used in the original decision making/payment process, or such evidence used is looked at in a new way, using new techniques.	Too many or too few risks have been chosen for testing and it is not clear how they will be tested for fraud.
The limitations of evidence considered when deciding whether fraud or error has occurred.	It is not clear how the evidence will be used to identify if fraud or error has taken place.
The evidence sources allow a decision on whether fraud or error has occurred.	The evidence sources do not allow a decision on whether fraud or error has occurred.
Testing focuses on finding fraud and error.	Testing focuses on non-compliance, or something other than fraud.
The evidence used clearly demonstrates that the testing has gone beyond checking that the controls have been applied.	Evidence uses only checks that the controls have been applied.
Decisions made during testing show that the purpose of the exercise was to find and measure levels of fraud.	Decisions made during testing show an approach focused on something other than finding fraud.
Testing covers the risks previously selected to be tested, with reasonable justification as to why other risks selected were not tested.	Testing does not cover all the risks previously selected and it is unclear why all risks were not tested.

Different levels of testing are required to be able to definitively classify a case as fraud or error

It is important to ensure consistency in testing

C10. Estimating and Measuring Levels of Fraud and Error Losses

Once testing for fraud and error has been completed the next step is to interpret the results by:

- 1 **Grouping the findings**
- 2 **Calculating the precision or margin of error**
- 3 **Making calculated estimations**
- 4 **Expressing the degree of confidence given to those estimations**

1. Grouping the findings

The **first step** is to **group the findings** and actual results from fraud and error testing using the following categories:

- Regular (or correct) transactions
- Transactions not determined as regular (or correct), which are further classified into the following:
 - Fraud
 - Error
 - Indicators of fraud (identified as irregular but unable to determine if fraud or error)
 - Unresolved transactions (testing has not been able to confirm regularity or determine irregularity).

This should include the number of instances out of the sample attributed to each category and also the monetary value. Definitions for these categories can be found in section D2 of this Standard.

The fraud measurement practitioner analysing the results of testing within a FLM exercise should consider the following:

Firstly, from the test results, is there sufficient evidence to prove on the balance of probabilities that the transaction is correct? If yes, then no further action is required and the result will be recorded as showing no fraud or error.

If there is not sufficient evidence to determine correctness, then **secondly** it is necessary to decide (on the balance of probabilities) whether it represents either: (a) fraud; (b) error; (c) is almost certainly incorrect (rather than correct) but there is not enough evidence to make the fraud/error distinction - this is what we call an Indicator of fraud (irregularity) - we can show it is wrong but cannot (yet) say if it is fraud or error; or (d) there are 'unresolved' cases. This is where there is currently insufficient evidence to determine whether the transaction is correct or incorrect.

For (c) and (d) it is necessary to decide whether further testing should be undertaken in order to achieve a more conclusive result.

2. Calculating the precision or margin of error

The **second step** is to **calculate the precision or margin of error** for the sample and to use this to calculate the possible range for each of the categories of findings.

For example, a finding of 3% fraud and error by monetary value within the sample with a precision of $\pm 1\%$ allows an estimation that the 'true' value of fraud and error within the overall population is within the range of 2% - 4%. Similarly, if these results from the same sample showed that this monetary amount of fraud and error came from 5% of the number of cases sampled then the 'true' incidence of fraud and error within the population can be estimated to be within a range of 4% - 6% of the overall numbers of transactions.

3. Making calculated estimations

The **third step** is to make **calculated estimations** as to 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 rate of monetary value rate of fraud and error 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 either fraud or error can be estimated to be between 400 to 600 items.

4. Expressing the degree of confidence given to those estimations

The **fourth step** is to **express the degree of confidence** that can be given to the calculated estimations. This is dependent upon the sample size and the degree to which it provided confidence that it accurately reflected the overall population. Thus, a confidence level in the representativeness of the sample of 95% would provide 95% confidence in the accuracy of the estimated range of fraud and error.

Care needs to be taken when using sampling methodologies to ensure that the estimated results accurately reflect the population.

For example, in stratified sampling, results and estimations should be calculated for each strata. The results for the overall population should then be calculated on the basis of the percentage of the overall population that each strata represented.

Similarly care needs to be taken if the sampled population is drawn from a sub-set of a larger population. For example, a particular grant scheme out of a population of several grant schemes. In this instance,

although the findings and results will reflect the grant scheme that was tested, it only has limited value in providing an estimation of likely levels of fraud and error within the wider population.

C11. Methodology for Calculating Savings

Types of savings generated

There are three types of savings generated from fraud/error cases detected as a result of fraud loss measurement exercises, where appropriate action has been taken:

1. **Prevented loss:** whereby payment has been stopped from being processed due to the fraud/error being detected. This includes prevention of payments anticipated to be processed in the future (depending on the payment structure of the sample item tested), as well as payment(s) scheduled to be processed that have been stopped from being processed due to the fraud/error being detected.²¹
2. **Recovered:** where money is in the process of being reclaimed or has been reclaimed on payment(s) processed as a result of fraud/error being detected.
3. **Detected loss:** the potential for savings through recoveries and against which actual recoveries should be measured.

There is a further distinction on the type of savings, whether they are generated by detected fraud and error in the exercise itself ("tactical") or whether they are based on changes to the control framework based on insights generated in the initial exercise ("strategic").

21 <https://www.gov.uk/government/publications/fraud-prevention-savings-framework>
<https://www.gov.uk/government/publications/government-counter-fraud-profession-standards-and-guidance>

Different types of savings measures

There are different types of measures that can be applied to calculating savings, each of which has a different level of certainty attached in relation to the values calculated and reported.

1. **Actual measures:** Actual savings are the amounts that have been proven to be recovered from detected fraud/error or payments proven to have been prevented from being processed due to the detection of fraud/error.
2. **Estimated measures:** Estimated projections or forecasts of future savings based upon evidenced assumptions from existing data, in relation to the future pattern and frequency of payments that can be presumed to have taken place if the fraud/error had not been detected or fraud controls had not been changed.

Identifying and calculating Preventative savings

Preventative savings are generated when payment has been stopped from being processed due to fraud or error being detected. There are three points for calculating different Preventative savings measures:

1. Prevented Actual

This saving is from loss prevented at the point where fraud or 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 as a (“tactical”) **actual measure**.

2. Future Loss Prevented

‘Future Loss Prevented’ can be generated from both Prevented loss cases and Detected loss cases. These savings occur where it can be evidenced that, had the fraud or error not been detected by the measurement activity, then it would have been more probable than not that it would

have continued for a period of time resulting in subsequent financial loss.

Such savings are based upon evidenced and agreed assumptions on the basis of the business process and policy area. 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.

Given the evidence for this measure is based on assumptions which are subject to a level of uncertainty, this measure is attributed to the exercise as a (“tactical”) **estimated measure**.

3. Upstream Prevention

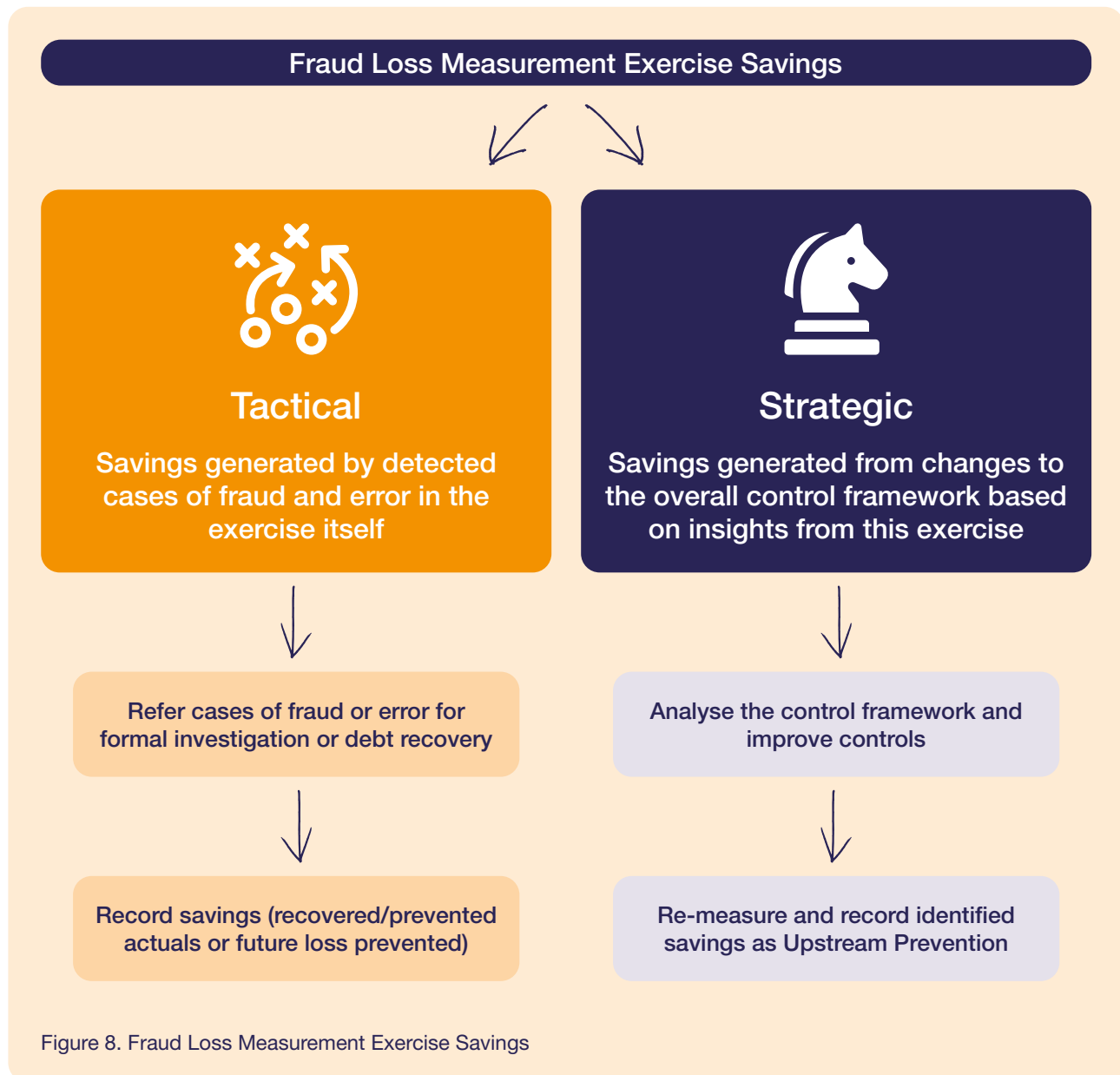
For both Prevented loss and Detected loss cases, improvements in processes resulting from the measurement exercise may generate ‘Upstream Prevented Savings’. These savings are generated from process changes arising from the detected fraud/error that prevent subsequent fraud/error within the wider population.

In addition, savings may include the application of the test parameters to the wider population to identify similar, existing, cases of fraud/error. The level of these savings will reduce over a period of time as behaviours subsequently change once awareness of the process changes has become common knowledge.

Such savings will be calculated on the basis of awareness of the level of fraud/error in the general population from post and pre-implementation of the additional application of control measures. These are attributed to the exercise as a (“strategic”) **estimated measure**.

Fraud Loss Measurement Exercise Savings

The diagram below illustrates the different savings generated from Fraud Loss Measurement Exercises.



Agreeing a methodology for calculating prevented savings

The methodology used to calculate prevented savings must be evidence based and consistent with similar methodologies used across government. The Public Sector Fraud Authority within the Cabinet Office hosts the cross government Prevention Panel that assesses and approves methodologies for calculating prevented savings. Once a methodology has been approved it is then authorised for use in similar circumstances.

C12. Reporting on Fraud Testing and Estimation

The results from fraud control testing and measurement exercises should be reported individually for each exercise and collectively to show the results and impact of the fraud measurement programme.

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

- The instances of fraud and error found and the respective values
- The number and values of sample items that were verified as being correct
- The number and values of sample items which remain 'unresolved' in that a decision on correctness or irregularity could not be determined
- Outline any bias, uncertainty or limitations within the underlying data or methodology.

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 statistical analysis of the results and any interpretations extrapolated over the total population.

The fraud measurement practitioner should draw statistically valid 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.

When reporting results within an exercise or across a programme of exercises be careful to avoid double counting. For example, this can happen when testing more than one fraud risk and fraud is found against each risk. If this would render the payment invalid it is important not to include the value twice, otherwise reported fraud would exceed the value of the transaction.

Where appropriate recommendations should be made in relation to additional control requirements and updated actions for the counter fraud strategy.

Reporting: Indicators of good quality	Reporting: Indicators of poor quality
Reasoning for decisions on whether fraud or irregularity has occurred is clearly outlined and understandable to a non-expert.	Reasoning for decisions on whether fraud or error have occurred are not clear .
Decision-making process for reaching conclusions on fraud or irregularity is applied consistently.	Decisions on whether fraud or error have occurred do not appear to have been applied consistently.
The process undertaken for testing is clearly described and understandable to a non-expert.	The process undertaken for testing is not clearly described, or is not understandable to a non-expert .
A comprehensive report that measures and culminates in conclusions about levels of fraud and error within the area of spend, and sets out limitations of testing .	No reporting of measurement of levels of fraud or inability to provide evidence based conclusions of actual levels of fraud within area of spend.
Report provides details of improvements to controls resulting from the exercise which are shown to be an appropriate and proportionate response.	Report fails to consider improvements to control framework.

C13. Managing Instances of Fraud and Error

The primary aim of fraud measurement and control testing exercises is to ascertain the overall level of fraud in a given area. However, such exercises may uncover particular and specific instances of fraud or error that need to be addressed.

Organisations should therefore have appropriate procedures and reporting routes in place to ensure that suspicions of fraud arising from fraud measurement activity are acted on and managed appropriately.

Similarly, when errors are uncovered, there should be mechanisms in place to communicate these to the relevant team or department to rectify the issue, cleanse organisational data, and prevent future false positives.



The primary aim of fraud measurement and control testing exercises is to ascertain the overall level of fraud in a given area

Organisations should have appropriate procedures and reporting routes in place

D. Guidance on Products for Fraud Measurement Practitioners

D1. Introduction

This guidance covers what good quality products should look like when undertaking fraud measurement. The design and content of these products may be unique to the organisation's activities, internal and external context, the size and complexity of the organisation, geographical location of these activities and the breadth and depth of its supply chain. A suitably trained and skilled person should undertake the design and maintenance of these products.

D2. Fraud Reporting – What to Include in the Reporting of Known Fraud and Error Found Through the Operation of Existing Controls

For an action to be strictly classified as “fraudulent”, there needs to be sufficient evidence to prove beyond reasonable doubt that a fraud related offence was committed.

However, it is recognised that proving fraud to the criminal standard is not possible or practical in every case.

Therefore, for the purposes of recording fraud, a pragmatic approach is taken by central government by using the civil standard of proof.

Cases should be recorded as fraud where the organisation considers that it was more likely than not that an action or inaction was taken with the intention of defrauding the organisation or public funds, in other words that on the balance of probabilities, fraud occurred.

This also means that instances of irregularity should be recorded and reported as fraud, bribery or corruption at the point at which it is identified, not the point at which the fraud took place. Fraud is a hidden crime, which may lie undetected for a period of time. Therefore, the reporting of cases of irregularity as fraud should not be reliant upon a prosecution being taken or civil sanction imposed, either of which could take months or years to conclude.

When reporting fraud, organisations should consider all areas of spend including income/revenue, benefits, procurement, grants, and payroll. The identification of fraud and its component elements should be disaggregated by area of fraud.

Categories

For the purpose of central government reporting, counter fraud management information/cases of irregularity are broken down into the following categories:

- ✓ **Detected Fraud**
- ✓ **Prevented Fraud**
- ✓ **Error**
- ✓ **Recovery of Losses**

Categories of Reporting²²

Detected Fraud

Detected fraud includes instances of identified fraud where, post-payment, it was decided that on the balance of probabilities the intention was to defraud.

Include:

- The number of cases of detected fraud which have been discovered in the time period
- The financial losses to the organisation resulting from each case. The gross loss should always be recorded, and not the net loss, if recovery action has already successfully returned monies to the organisation
- Include instances where the investigation may still be active, provided the organisation has determined within the reporting period that there is a case to answer for dishonesty
- Sometimes the actual loss is not known but an estimate should be provided. This should be recorded as an estimate with a note given about the method of calculation
- The spending area within the organisation that the fraud occurred in
- The person or organisation that committed the fraud
- The type of fraud detected according to the Fraud Act 2006 (false representation, failure to disclose information or abuse of position)
- The specific method by which the fraud was committed
- If applicable any known enablers, such as bribery or a conflict of interest.

Exclude:

- Costs associated with investigating a case.

Prevented Fraud

Include:

- Any incidents of fraud that have been prevented in the reference period from specific fraud prevention processes
- Transactions identified as being fraudulent before payment was made
- In the case of stopping an ongoing series of fraudulent payments, include the total value of payments for the relevant reference period
- Examples of the type of prevention activities that can be measured include the deployment of real time transaction checking systems, pre-payment fraud checks, or the use of data sets to check entitlement in application processes.

Exclude:

- Further payments that were due to be made in subsequent periods should not be included
- Do not include an estimate of fraud deterred through publicity or warnings to potential fraudsters of the controls in place.

Reporting Error

In reporting error, organisations should consider all areas of spend including income/revenue, benefits, procurement, grants, and payroll.

The point at which error should be referenced is the point at which the error is identified – not when the error took place. Error may lie undetected for a period of time, and can be defined in two categories:

1. **Customer/Supplier Error:** This occurs where the customer or supplier has provided inaccurate or incomplete information, or failed to report a change in their circumstances, but there is no suggestion of any fraudulent intent. For the purpose of recording error the 'customer' should be seen as any third party outside of government with whom there is a financial relationship of any kind.
2. **Official Error:** This occurs where the correct information has been provided by the customer but this information has been incorrectly processed by the organisation. Where possible, organisations should be able to distinguish whether an error is due to the actions of a customer or official.

Detected Error

Detected error includes all errors (both customer and official) which were confirmed in the specified reference period and resulted in a financial loss to the department.

When calculating value, include the gross value of errors which caused a financial loss whether or not any monies were subsequently recovered.

Include:

- All financial losses to the organisation resulting from each error.

Recovery of Losses

Where fraud or error has resulted in losses to the organisation, the extent to which these have been recoverable should be reported.

Reporting should show the following:

- Unrecovered losses due to (i) fraud; (ii) error brought forward from the previous reporting period
- Additional losses due to (i) fraud; (ii) error discovered within the reporting period
- Losses recovered within the reporting period
- Losses written off as unrecoverable within the reporting period
- Adjustments to previously reported losses (e.g. revision of previous calculations)
- Net amount of unrecovered losses carried forward to the next reporting period
- The method by which the fraud or error was recovered, such as civil or criminal proceedings.

D3. Fraud Loss Estimation and Measurement – Outputs from Fraud Measurement Exercises

The key output from a fraud measurement exercise is a report which outlines the approach taken, details the findings and results, and provides overall conclusions about estimated levels of fraud and error within the wider population.

As a minimum, the report of a single fraud measurement exercise should contain the following sections:

- An introduction to explain the spend area tested
- The sample methodology used and sample size
- The approach taken to testing
- The results from testing, and the amount of fraud and error found within the sample
- Recognition of any limitations or uncertainty in relation to the data used, sampling or testing
- Actions and recommendations for controls and future measurement in that specific area
- Conclusions about estimated levels of fraud and error within the wider population.

Where an organisation judges that it has an area of high fraud risk but that a fraud measurement exercise is not justified, in certain circumstances it could be acceptable to develop an estimate of fraud and error loss. This can be done by using the results from an exercise performed on a similar profile of expenditure elsewhere in the business, or even carried out by another organisation, providing the fraud risk profile (see FRA standard) is sufficiently similar.

The findings and results from fraud and error testing should be grouped and reported using the following categories:

- Regular transactions
- Irregularity, which can be further categorised as cases of:
 - Fraud
 - Error
 - Indicators of fraud
- Unresolved cases.



The key output from a fraud measurement exercise is a report which outlines the approach taken, findings and results and overall conclusions

Definitions of reporting categories

Regular transactions	There is sufficient evidence to be able to demonstrate that the transaction within the sample was entirely 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 probabilities, evidence that a case or transaction is irregular through dishonesty and fraudulent intent then it should be recorded as fraud.
Error	Where there is evidence of irregularity but sufficient evidence on the balance of probabilities that there was no intent to defraud, then this should be classified as 'error'.
Indication of fraud	Where 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.
Unresolved	Where there is no available evidence to determine the correctness of a case or payment, or the evidence indicates a case of payment may be irregular but this cannot be positively determined. Fraud measurement exercises may tend to report more error, as often a full fraud investigation would be required to prove the necessary intent to determine the loss as fraud, which will not be within the scope of a sampling exercise aimed at measuring losses.

Reporting findings from fraud measurement exercises

[Appendix 5](#) provides example templates for reporting these categories of findings.

The actual findings from the testing should be interpreted in relation to the overall population from which the sample was drawn. This involves using the calculated rate of precision (or margin of error), which is calculated from the size of the sample in relation to the overall population. This is then used to predict the minimum and maximum extent to which a level of fraud or error exists within the overall population, in terms of both monetary value and numbers of transactions.

D4. Calculation of Savings Generated Through a Fraud Loss Measurement Programme

The calculations of savings generated by fraud loss measurement activities can be used to assess the success and financial impact of an organisation's counter fraud strategy and controls.

Repeated measurement is key to demonstrating this. Initial exercises will be undertaken in an area where Fraud Loss Measurement has not been done before. Depending on what is found this might lead to new control interventions to bring down the levels of fraud. A subsequent (repeat) exercise would measure whether the new controls have had an effect. Any reduction in levels of fraud and error can be shown as prevented savings - this is upstream prevention - a **strategic** output from the exercise.

Quantifying these savings also allows the organisation to demonstrate the cost effectiveness of undertaking the measurement activities, and calculating the value of fraud and error prevented at different points in time. This includes future (prevented) savings resulting from improved controls, or the introduction of new controls and processes.

D5. Updating Full Fraud Risk Assessments

A Full Fraud Risk Assessment should be produced for each specific area targeted for testing and measurement. This assessment must adhere to the Fraud Risk Assessment Standard²³ and incorporate the considerations and additional elements for measurement outlined in the process guidance in section C4 of this document (Carrying out and adapting a Full Fraud Risk Assessment).

The additional considerations for the purposes of Measurement are:

Evidence available to facilitate testing for fraud

Identification of relevant information that is held within the area, process, scheme etc. being examined.
Identification of 'comparator data' that could be used to validate the authenticity of information submitted by a potential fraudster or used to identify missing information that has not been declared. This could be held elsewhere within the organisation or externally in another organisation or via open-source data.

Alternatively, comparator data can be generated through physical inspections, site visits etc.

Whether the fraud risk will be included within the scope of the test plan

A 'Yes'/'No' decision of whether the fraud risk will be tested. Decisions should be based upon the extent to which fraud exposures have been identified within the residual risk and also the availability of evidence that can be used to test if the fraud has happened.

Findings from measurement activities should then be fed back into the fraud risk assessments as part of the Fraud Risk Management Cycle.

23 <https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

E. Guidance for Organisations

E1. Introduction

The objectives of Fraud Measurement are:

1. To establish the vulnerabilities of the organisation to fraud.
2. To be able to identify, quantify and report instances of fraud and error being prevented and detected through the business processes and controls operated by the organisation.
3. To test for and estimate levels of undetected fraud and error to gain additional insights into, and assurance over, current estimated levels of fraud and error across the organisation.
4. To be able to calculate the value of fraud and error prevented, including future savings from the implementation of additional controls or ways of working.
5. To enable more informed and transparent conversations within the organisation on its fraud risks and the material nature of the threat they present to the organisation.
6. To measure the effectiveness of the organisation's counter fraud strategy.

The guidance set out below is the approved professional practice for public sector organisations to support measurement practitioners in implementing effective fraud measurement within their organisations.

In the United Kingdom this includes aspects of mandated steps for government organisations as per the Government Functional Standard GovS 013: Counter Fraud and the Public Sector Fraud Authority (PSFA) Mandate²⁴. Where steps are mandated, this is clearly signposted.

The Government Counter Fraud Functional Standard GovS013²⁵ states:

“Organisations should undertake activity to try and detect fraud, bribery and corruption in high-risk areas where little or nothing is known of fraud, bribery and corruption levels. This activity should include using loss measurement activity (fraud measurement and assurance) where suitable.”

“Proactive detection activity can include fraud, bribery and corruption measurement and assurance activity, or the use of data sharing and/or data analytics to attempt to find fraud in a specific business area, based on a good understanding of the risks in that area.”

“Organisations should define the outcomes they are seeking to achieve that year, and should have metrics to measure whether the targeted outcome has been achieved.”

²⁴ <https://assets.publishing.service.gov.uk/media/63207cd68fa8f51825582b2f/3042-PSFA-Mandate-V4-final.pdf>

²⁵ GovS013 is mandatory for government departments and their arm's-length bodies. Other public sector organisations, devolved or local, might find this standard useful.

Executive Boards in every organisation should plan to measure or estimate the extent to which fraud is impacting the organisation, in proportion to its size and fraud risk profile. This should encompass measurement and reporting of the amount of fraud being prevented or detected by existing control frameworks, and testing to determine previously undetected fraud losses in order to estimate the level of loss that the organisation is potentially exposed to.²⁶

Accountability and responsibility for a programme of fraud measurement and reporting at board level should be clearly defined. The counter fraud functional lead should seek the sponsorship of the fraud measurement programme at the highest level of the organisation.

The organisation should support a counter fraud culture. An effective culture is fostered through a cycle of education, measurement, monitoring and improvement. A strong counter fraud culture is essential to effectively deal with fraud. There are different approaches that can be deployed to evaluate a counter fraud culture.²⁷ Fraud Measurement practitioners must be able to robustly withstand challenge while exercising objective professional judgement to promote and demonstrate the value of fraud measurement. This includes when organisations, business units or activities regularly fail to find or report fraud or error.

In the same way that organisations should demonstrate that they are managing risks within their spend, scheme or project, an organisation should consider how it measures the success of its counter fraud strategy. This should also include measuring the counter fraud culture as part of the organisation's counter fraud response and effectiveness as well as the cost/benefit of its counter fraud controls.

This will entail capturing the value of the operation of those controls through determining the levels of fraud or error actually prevented, or detected and recovered. However, this alone does not provide a view on how effective those controls are in practice in managing all attempts at fraud. Therefore, fraud loss measurement exercises, focussing on testing losses arising from residual risk (the fraud risk exposure not fully covered by the controls) is necessary.

HM Treasury in their publication 'Managing Public Money'²⁸ also advises that effective management of the risk of fraud includes evaluating the scale of fraud risk and measuring the effectiveness of the counter fraud strategy. If an organisation is unaware of the potential losses to fraud and error it faces then it will be unable to put in place an effective strategy, controls and resources to tackle and reduce the level of losses it faces.

Fraud measurement therefore lies at the heart of an effective counter fraud response.

26 https://assets.publishing.service.gov.uk/media/67b85a45ba253db298782c0c/IPSEFF_Fraud_Loss_Measurement_Framework_.pdf

27 <https://www.gov.uk/government/publications/government-counter-fraud-profession-standards-and-guidance-standard-for-counter-fraud-culture-practitioners>

28 https://assets.publishing.service.gov.uk/media/684ae4c6f7c9feb9b0413804/Managing_Public_Money.pdf

E2. Mapping and Understanding Assurance Requirements

Accounting Officers rely on assurances from others within the organisation to give independent insight into the organisation's performance (including their responsibility to prevent and detect fraud and error). This may include programmes of assurance activity (for example Internal Audit).

Therefore, an organisation must be able to understand the areas where it is exposed to a risk of fraud or error. Organisational (Enterprise) FRAs coupled with Thematic (Grouped) FRAs help to identify and map those areas on which assurance activity may be needed.

Once the fraud and error risks have been comprehensively assessed, it is important to identify assurance requirements in respect of those risks and develop a fraud and error risk assurance map for the organisation.

An Assurance Map that focuses on fraud and error should include:



Effective Reporting Process which captures instances of fraud and error within each of the areas of the organisation where fraud exists and reports these to the central counter fraud function. This allows an organisation to measure the amount of fraud and error that is being discovered through the operation of controls in particular areas of the organisation.

It is important to continuously ensure that reporting on fraud and error is thorough. This helps the organisation understand how much fraud and error is detected by its control measures. Assurance processes should include comparing levels of fraud and error across different areas of the organisation and questioning why there are few or no reported cases in some parts.



Assurance on the Operation of Key Controls for Fraud and Error Prevention. The assurance requirement should include the measurement of the level of losses resulting from controls failing to operate correctly. This normally will involve internal or external audit. This will involve sample-based testing that is statistically significant and allows the amount of fraud and error being missed through controls not being applied correctly to be identified as well as assurance on the correctness of values of fraud and error being reported through the application of those controls.



Identify Residual Risk. Identify areas of the organisation where significant residual fraud risks remain and where testing through fraud loss measurement can provide assurance on levels of fraud that are currently undetected.

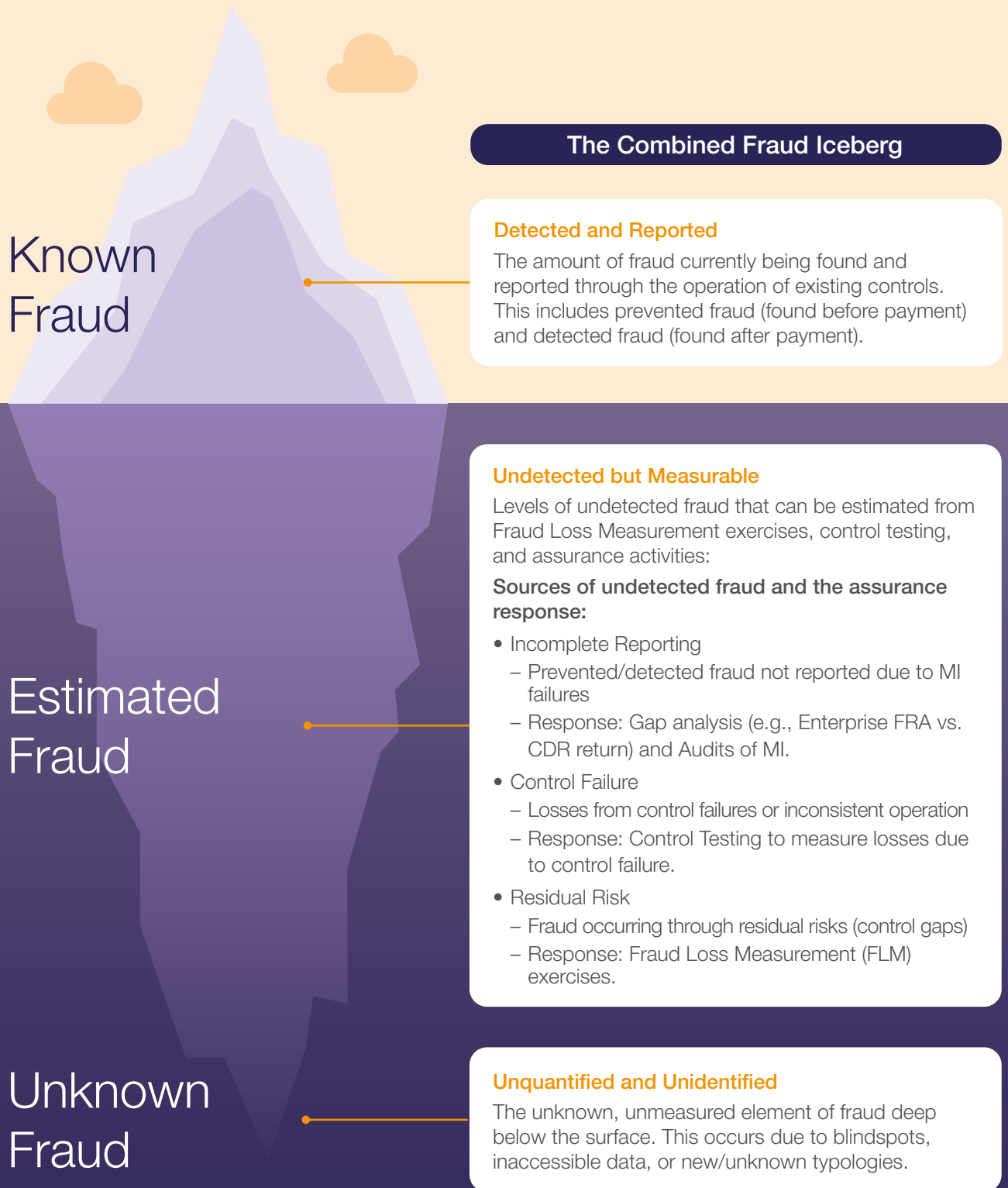
Example Assurance Map

The below example is for illustrative purposes only as a generic example at a basic level, it is not a template. It is crucial for practitioners and organisations to build their own scoring matrix with a defined scoring criteria which is meaningful and appropriate to their organisational setting.

Department for Fictional Objectives of Fraud and Error Assurance activity: Confidence in effectiveness of Governance, Risk Management and Control.	Desired/ Required Amount of Assurance	Amount of Assurance				Current Amount of Assurance
		Management:	Counter Fraud Function:	Independent (Internal Audit):	Counter Fraud Function External Review (PSFA):	
		First line	Second line	Third line	Fourth line	
Schemes and Processes						
Objective of Assurance activity – confidence in exposure to fraud risk is understood and being acted upon						
Free prescriptions	High	High	Medium	High	Medium	High
Free eyesight and hearing tests	Medium	Low	Low	None	None	Low
Free travel to hospital appointments	Medium	Medium	Low	None	None	Low
Winter fuel payment	High	Medium	Medium	Low	Low	Medium
Stairlift scheme	High	Low	Low	Low	None	Low
Mobility scooter scheme	High	Low	Low	Low	None	Low
Grants for local social activities	Low	None	None	None	None	None
Payroll and expenses	Medium	Medium	Low	High	Low	Medium

Figure 9. Example Assurance Map

The purpose of delivering assurance activities in relation to fraud and error is to provide a greater in-depth understanding of the volume and values of irregularity that the organisation faces. The overall objective is therefore to reveal more of the “fraud iceberg” through those activities as illustrated in the diagram below²⁹:



29 https://assets.publishing.service.gov.uk/media/67b85a45ba253db298782c0c/IPSFF_Fraud_Loss_Measurement_Framework_.pdf

Fraud and error – organisational assurance requirements

Fraud and error reporting

Assurance that reporting covers all business areas/key organisational fraud risks and that reporting of instances of fraud and error is accurate, complete and timely.

Key counter fraud controls and counter measures

Testing of key controls to assess the extent to which they are working and to measure the level of resulting losses where they have failed to operate correctly.

Undetected and unknown fraud

Testing areas where there is a residual exposure to the risk of fraud to see if undetected fraud has materialised and/or is being contained within accepted levels of tolerance.

Assurance should also include the provision of benchmarking between different parts of the organisation as well as with other organisations on the levels of fraud and error being discovered within similar areas. This should facilitate challenge where little or no cases of fraud and error are being found.

E3. Building a Fraud Measurement Programme within the Organisation

Organisations should develop a fraud measurement programme to meet the assurance requirements identified in respect of organisational fraud and error risks, and provide measurement on all key areas of the business within the organisation.

The scope of the fraud measurement programme should include:

- Regular reporting of known fraud and error as prevented/detected by existing controls
- The measurement of fraud and error losses arising from vulnerabilities in controls which have resulted in them not working as intended. (Where it is identified that an individual has not operated a control correctly an assessment should be made as to whether this was done deliberately to either cause a loss to the organisation and/or a gain to themselves or someone else)
- The measurement and estimation of undetected fraud through undertaking fraud loss measurement exercises
- Calculating and reporting recoveries of detected fraud, including cumulative, multi-annual, figures on recoveries, losses still to be recovered and losses that have been written off as unrecoverable
- Calculating ongoing savings of prevented fraud where new additional controls have been implemented, including those implemented as a result of previous measurement activity.

E4. Developing and Implementing an Annual Plan as Part of the Ongoing Fraud Measurement Programme

The fraud measurement programme should be implemented through an annual measurement plan which carry out fraud measurement activities within the scope of the fraud measurement programme. This could be a standalone plan for fraud measurement or form part of the annual action plan as required by GovS013. The annual measurement plan should also ensure

that activities are carried out to provide the assurance requirements detailed in the assurance map for fraud and error risks.³⁰

Some activities will be continuous business as usual activities, such as collecting and reporting instances of fraud and error discovered through routine business operations. Others, such as fraud loss measurement exercises, will be time limited exercises targeted at specific areas of the business where it is considered that there remains a risk of undetected fraud and error.

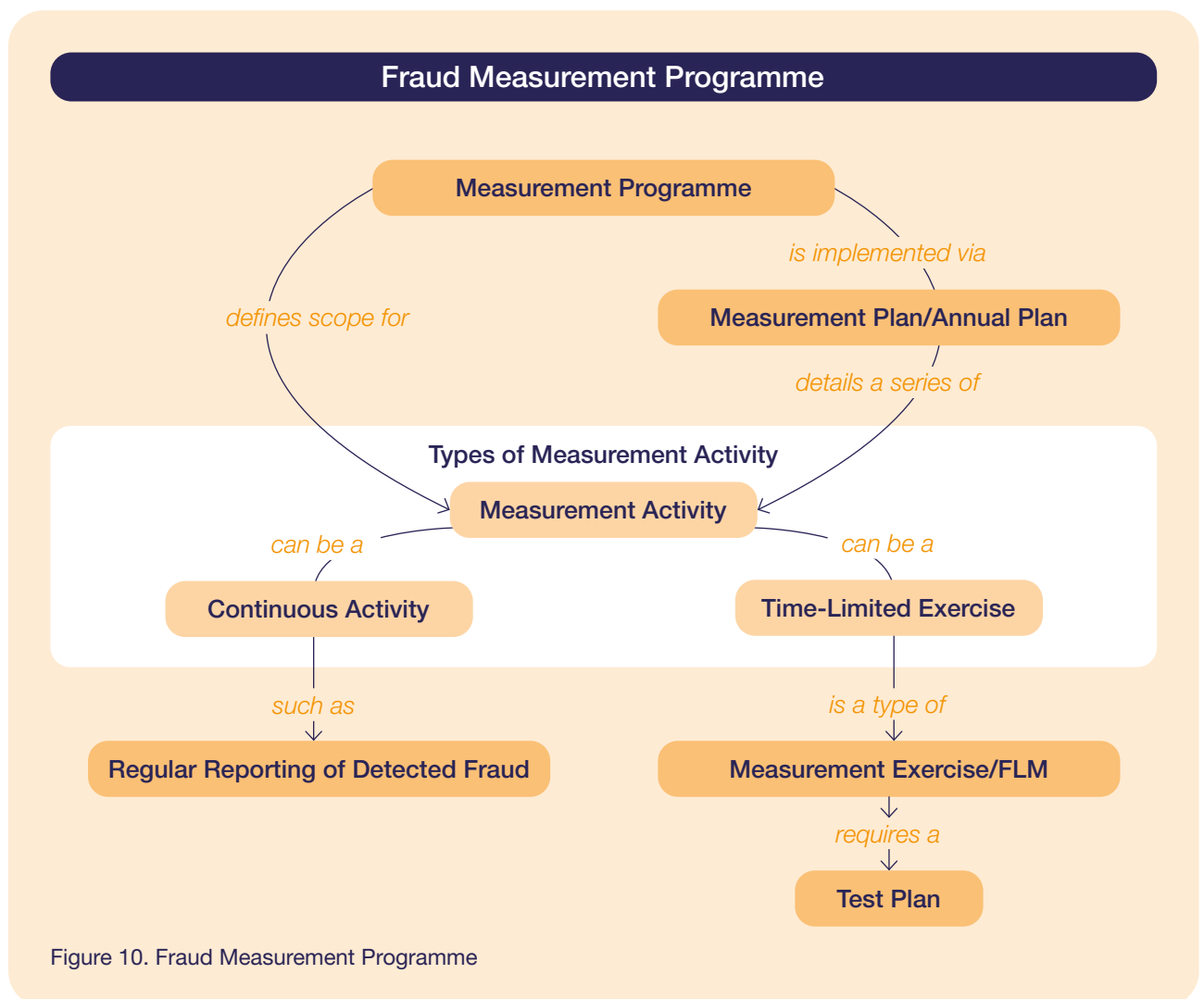


Figure 10. Fraud Measurement Programme

30 Larger organisations might have a standalone Fraud Measurement Plan

Fraud Measurement as part of HMG Fraud Risk Management Cycle

The diagram below illustrates control evaluation and monitoring and reporting where fraud measurement activities take place.

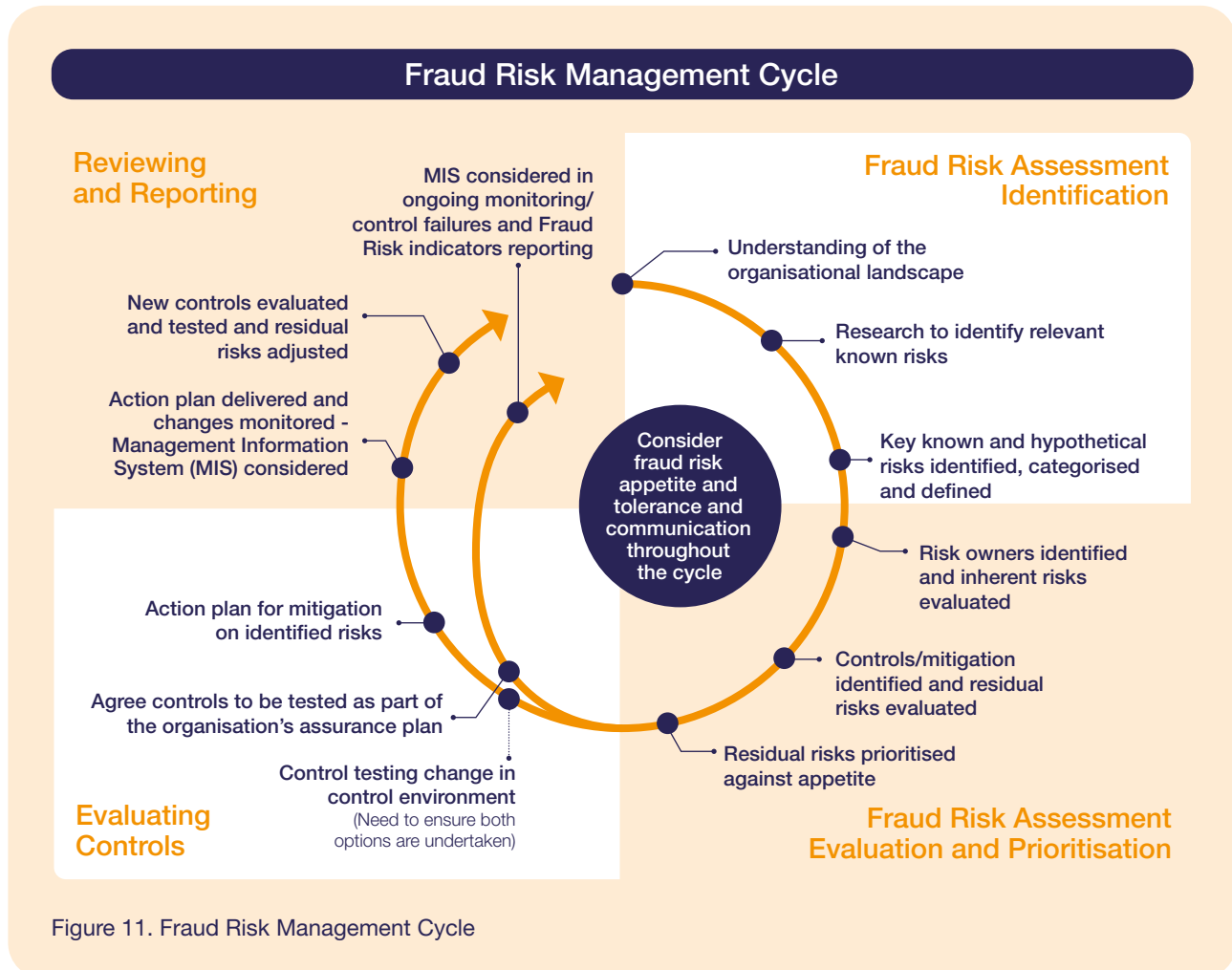


Figure 11. Fraud Risk Management Cycle

E5. Governance and Oversight of the Fraud Measurement Programme

The fraud measurement programme should be a key component of an organisation's assurance landscape and be owned and signed off by the board-level individual who is accountable for managing fraud and error risks.

The fraud measurement programme should be built into the organisation's counter fraud strategy, and the results of the programme should inform the future revisions of that strategy.

Key governance structures, such as the organisation's equivalent of an Audit and Risk Committee, should have oversight of the fraud measurement programme and the development of the annual fraud measurement plans that implement it.

The counter fraud lead should prepare associated annual plans to implement the programme and ensure these are agreed by the equivalent of an Audit and Risk Committee and signed off by the board-level individual responsible for the organisation's response to fraud and error risks. This sign-off should also include the provision of adequate resources to achieve the annual plan and fulfil the overall fraud measurement programme. Resourcing should include the provision of staff who are proficient in fraud

reporting and measurement.

The creation of fraud measurement processes and standard operating procedures should be considered to achieve the objectives for fraud measurement. Different standard operating procedures could be considered for different fraud types. All processes and procedures should be regularly reviewed and evaluated to ensure they are of the required standard and remain current.

E6. Measuring the Effectiveness of the Counter Fraud Strategy

The counter fraud strategy should include arrangements to measure the effectiveness of the strategy and its delivery.³¹ This could include the development of:

- **Key Performance Indicators and Metrics** – to measure the effectiveness of activities within the strategy (including fraud measurement), to find or prevent fraud and error, and to demonstrate the achievement and success of key activities within the counter fraud strategy, including informing the setting of, and assessing progress made against financial outcome targets
- **Key Fraud Control Indicators** – which facilitate regular measurement and monitoring of the performance of key controls that mitigate key fraud risks

- **Key Fraud Risk Indicators** – indicators which assess and measure factors that increase the likelihood of particular fraud risks materialising – and the extent to which the counter fraud strategy is responsive to adapting to these indicators. For example, increased numbers of transactions, new areas of spend, turnover of staff, identified new threats, increased instances of particular frauds across the public sector.

HM Treasury in their publication 'Managing Public Money' advises that effective management of the risk of fraud includes measuring the effectiveness of the counter fraud strategy.³² If an organisation is unaware of the potential losses to fraud and error it faces then it will be unable to put in place an effective strategy, controls and resources to tackle and reduce the level of losses it faces.

This aligns to GovS013 which states that the strategy should be maintained for relevance and its implementation monitored and measured.³³

For further information on strategy see the Building a Counter Fraud Strategy Practice Note produced by the GCFP.³⁴

31 <https://www.gov.uk/government/publications/building-a-counter-fraud-strategy-practice-note>

32 https://assets.publishing.service.gov.uk/media/684ae4c6f7c9feb9b0413804/Managing_Public_Money.pdf

33 <https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud>

34 <https://www.gov.uk/government/publications/building-a-counter-fraud-strategy-practice-note>

F. Further Guidance

F1. Further Information

This Professional Standards and Guidance has been created in order to align counter fraud capability across government.

You can learn more about the Public Sector Fraud Authority and the Government Counter Fraud Profession via:

<https://www.gov.uk/government/organisations/public-sector-fraud-authority>

Alternatively, the Counter Fraud and Investigation Team in the Government Internal Audit Agency (GIAA) provides a range of services defined in the Government Counter Fraud Framework. They can be contacted to discuss how they are able to assist you to meet your requirements at:

Correspondence@giaa.gov.uk

For further information on the Government Counter Fraud Profession, or to view the other Professional Standards and Guidance available, please visit the Government Counter Fraud Profession page at:

<https://www.gov.uk/government/groups/counter-fraud-standards-and-profession>

If you have any questions surrounding the Government Counter Fraud Profession, and how you can get yourself and your department involved, please contact:

GCFP@cabinetoffice.gov.uk

F2. Functional Standards³⁵

Functional Standards	Standard Number
 Government Functions – sets expectations for the direction and management of functions across government	GovS 001
 Project Delivery – sets expectations for the direction and management of portfolios, programmes and projects in government	GovS 002
 People – sets expectations for the leadership and management of human resources across government	GovS 003
 Property – sets expectations for the management of corporate functions across government	GovS 004
 Digital – sets out how all digital, data and technology work and activities should be conducted across government	GovS 005
 Finance – sets expectations for the effective management and use of public funds	GovS 006
 Security – sets expectations for the planning, delivery and management of government security activities	GovS 007

Functional Standards	Standard Number	
	Commercial and Commercial Continuous Improvement Assessment Framework – designed to help drive continuous improvement in commercial practices across the public sector	GovS 008
	Internal Audit – sets the expectations for internal audit activity to enhance the effectiveness and efficiency of governance, risk management and control in government organisations	GovS 009
	Analysis – sets expectations for the planning and undertaking of analysis to support well-informed decision making	GovS 010
	Communication – sets expectations for the management and practice of government communication in order to deliver responsive and informative public service messaging	GovS 011
	Counter Fraud – sets the expectations for the management of fraud, bribery and corruption risk in government organisations	GovS 013
	Debt – part of a suite of standards to guide people working in and with the UK government	GovS 014
	Grants – promotes efficiency and effectiveness in grant making across all government departments and arm’s-length bodies	GovS 015

F3. Further Reading

Enterprise Fraud Risk Assessment

<https://www.gov.uk/government/publications/enterprise-fraud-risk-assessment-practice-note>

Initial Fraud Impact Assessment

<https://www.gov.uk/government/publications/initial-fraud-impact-assessment-practice-note>

Full Fraud Risk Assessment

<https://www.gov.uk/government/publications/full-fraud-risk-assessment-practice-note>

Professional Standards and Guidance for Fraud Risk Assessment in Government

<https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

Fraud Prevention Standard for Counter Fraud Professionals

<https://www.gov.uk/government/publications/government-counter-fraud-profession-standards-and-guidance>

Government Counter Fraud Profession Standards and Guidance, Standard for Counter Fraud Culture Practitioners

<https://www.gov.uk/government/publications/government-counter-fraud-profession-standards-and-guidance-standard-for-counter-fraud-culture-practitioners>

Government Counter Fraud Profession Practitioners Standard for Fraud Detection

<https://www.gov.uk/government/publications/practitioners-standard-for-fraud-detection>

Government Counter Fraud Function and Profession Guidance and regulation

<https://www.gov.uk/search/guidance-and-regulation?order=updated-newest&organisation%5B%5D=public-sector-fraud-authority&page=1&parent=public-sector-fraud-authority>

International Public Sector Fraud Forum Guidance (including on Fraud Loss Measurement and Controls Testing)

<https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance>

Glossary



Glossary

Term	Definition
Ability	Skill/proficiency in a particular area.
Actor, Action, Outcome	The three specific components required to clearly define a fraud risk: identifying who commits the fraud (Actor), how they do it (Action), and what the impact is (Outcome).
Actual Measure	The amounts that have been proven to be recovered from detected fraud/error or payments proven to have been prevented from being processed due to the detection of fraud/error.
Apply	Make use of a skill/knowledge.
Awareness	Knowledge of a fact.
Bribery	Offering, promising or giving a financial or other advantage to induce or reward improper performance or the request or receipt of such an advantage. It includes the corporate offence of failing to prevent bribery.
Categories	Defined combinations of elements, which show the expected knowledge, skills and experience for each core discipline. These enable a common assessment of skills and draw a distinction of those with a level of skill, and those without.
Cluster Sample	A sampling method where the population is divided into naturally occurring groups (clusters), such as geographic regions, and specific clusters are randomly selected for testing.
Comparator Data	Data used to validate existing data and identify non-matching attributes and anomalies which indicate if fraud or error has occurred.
Competency Framework	Group of elements found in core or subdisciplines. Grouped together, with varying levels of knowledge, skills and experience required.
Competency Levels	Used to identify progression within the standards and competencies. The competency levels are Foundation and Practitioner.
Confidence Interval (Margin of Error)	The degree to which test results accurately represent the actual rate of error or fraud within the population (e.g. $\pm 1\%$).
Confidence Level	The degree of confidence, expressed as a percentage (e.g. 95%), that the sample selected accurately represents the parent population from which it was drawn.

Term	Definition
Control Testing	Testing the operation of key controls to see if they are working. Unlike Fraud Loss Measurement, it focuses on losses caused by control failure rather than residual risk.
Core Components	Behind each core and subdisciplines there are components outlining knowledge, skills and experience required.
Core Disciplines	Areas of expertise, knowledge, skills and experience that are needed for an effective counter fraud response. They are not people role or category specific.
Corruption	The abuse of entrusted power for private benefit that usually breaches laws, regulations, standards of integrity and/or standards of professional behaviour.
Demonstrate	Show something and explain how it works.
Describe	Give a report on how something is done or what something is like.
Design	Make or draw plans for something.
Detected Fraud	Includes instances of identified fraud where, post-payment, it was decided that on the balance of probabilities the intention was to defraud.
Detected Loss	Instances of fraud or error found after payment has been made (post-payment), representing a potential for savings through recovery.
Discuss	Consider and offer an interpretation or evaluation of something or give a judgement on the value of arguments for and against something.
Error	Is a similar occurrence to fraud, but where the elements of dishonesty or intent (see definition of fraud) are missing or cannot be proved. However, error also results in losses to public funds and for the purposes of this standard, is considered alongside fraud.
Estimated Measure	Projections or forecasts of future savings based upon evidenced assumptions from existing data, in relation to the future pattern and frequency of payments that can be presumed to have taken place if the fraud/error had not been detected or fraud controls had not been changed.
Evaluate/Assess	Judge or calculate the quality, importance, amount, or value of something.
Explain	Make something easier to understand by giving information about it and/or give a reason for an action.
Extrapolation	The process of interpreting results from a sample to apply them across the overall population.

Term	Definition
Fraud	Defined in the Fraud Act 2006. The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position.
Fraud Control Cluster	The Fraud Control cluster incorporates the Fraud Risk Assessment, Fraud Prevention, Fraud Detection, Counter Fraud Culture and Fraud Measurement disciplines enabling the development of a career pathway for the fraud control practitioner.
Fraud Deterrence	The act of discouraging fraud by being clear of consequences. Sending out the message that committing fraud has adverse consequences for fraudsters, victims and society.
Fraud Iceberg	A visual metaphor describing the total landscape of fraud, consisting of 'Known Fraud' (visible), 'Estimated Fraud' (measured but undetected), and 'Unknown Fraud' (unquantified and hidden).
Fraud Loss Measurement (FLM)	Exercises designed to test residual fraud risks (where controls are weak or absent) to estimate the level of undetected fraud and error in a specific area.
Fraud Measurement	The process of quantifying and estimating the extent of fraud and error within a specific area or across the organisation using data analysis, sampling, and modelling.
Fraud Prevention	To stop the likelihood and reduce the impact of fraud. To create an anti-fraud culture in which people and processes work together to minimise fraud risk.
Fraud Risk Assessment	A process aimed at proactively identifying and addressing an organisation's vulnerabilities to both internal and external fraud. It is an essential element of an effective counter fraud response and whilst it should be integrated into the organisation's overall risk management approach, it requires specific skills, knowledge, processes and products.
Full Fraud Risk Assessment (Full FRA)	A comprehensive assessment required before testing, which identifies specific fraud risks, evaluates controls, and determines the residual risk that needs to be measured.
Horizon Scanning	Exploring what the future might look like to understand uncertainties better. Horizon scanning helps organisations analyse whether it is adequately prepared for potential opportunities and threats. This helps ensure that policies are resilient to different future environments.
Identify	Recognise a problem, need, fact, or other item and show that it exists.

Term	Definition
Indicator of Fraud (irregularity)	A classification for a transaction where evidence suggests it is irregular and potentially fraudulent, but the evidence is not yet sufficient to meet the 'balance of probabilities' test.
Inherent Risk	Also defined as gross risk, is the risk to an organisation assuming there are no controls in place.
Know/ Knowledge	Provide evidence of factual information or awareness gained through experience or education.
Monetary Unit Sample (MUS)	A value-weighted sampling technique where each monetary unit (e.g., £1) is treated as a sampling unit, and selection is based on cumulative value intervals.
National Audit Office (NAO)	The UK's independent public spending watchdog. The NAO supports Parliament in holding the government to account and in helping improve public services through high-quality audits.
Non-probability Sampling	A sampling method based on subjective judgement (e.g. convenience) where the probability of selection is unknown. Results from this method cannot be extrapolated to the wider population.
Population	The wider, entire group of data or transactions from which a sample is drawn.
Potential Measure	A savings measure showing the value of detected loss cases where recovery has not yet happened and may not be fully realised.
Precision	The range of accuracy (e.g. $\pm 1\%$) calculated from the sample size to predict the minimum and maximum levels of fraud in the overall population.
Prevented Loss	A savings category where payment is stopped before it is processed because fraud or error was detected.
Probability Sample	A sample where any unit within the population has a known, non-zero chance of being chosen, allowing for the calculation of sampling error and extrapolation.
Recognise	Show from knowledge.
Regular Transaction	A transaction where testing has provided sufficient evidence to demonstrate that it is entirely valid and contains no fraud or error.
Residual Risk	Also defined as net risk, or fraud risk exposure, it is the risk remaining once the risk response has been conducted including controls that are in place and identifies how fraud can still happen.
Risk	The possibility of an adverse event occurring or a beneficial opportunity being missed. If realised, it may have an effect on the achievement of objectives and can be measured in terms of likelihood and impact.

Term	Definition
Risk Appetite	The amount of risk the organisation is willing to accept at the enterprise level, which manifests itself in the type and number of activities and associated risks that the organisation is willing to undertake.
Risk Tolerance	The threshold levels of risk exposure and target levels of incidences and losses that, with appropriate approvals, can be exceeded but which, when exceeded, will trigger some form of response for example, reporting the situation to senior management.
Sample	A subset drawn from the wider entire population in a way that represents the population as closely as possible.
Simple Random Sample	A sampling method where each member of the population has an equal chance of being chosen, typically using random number generation equal to the desired sample size.
Spend Area Assessment	A basic risk assessment performed in the absence of a Full FRA to prioritise areas for measurement, scoring them against financial, reputational, inherent and control risks.
Stratified Random Sample	A method where the population is divided into sub-populations (strata) based on specific characteristics (e.g., value or region), and random samples are taken from each stratum.
Subdisciplines	Areas of additional knowledge, skills and experience that enhance capability in those areas across a number of core disciplines.
Summarise	A brief statement of the main points.
Systematic Sample	A sampling method where data is sequentially numbered and every nth piece of data is chosen based on a calculated interval.
Threat	A person or group, object or activity that has the potential to cause harm to the achievement of the organisation's objectives. It takes into account capability and intent to do so.
Understand/ Interpret	Provide the intended meaning or cause of something.
Unresolved (Case)	A classification for a transaction where testing has not been able to confirm if it is correct (regular) or incorrect (irregular) due to insufficient evidence.

Appendices



Appendix 1 – Full Competency Framework

1. Counter Fraud, Bribery and Corruption Knowledge

Foundation

Practitioner

1.1	Explain the relevant legislation (civil and criminal) and offences for fraud and bribery.	Demonstrate and apply the relevant legislation (civil and criminal) and offences for fraud and bribery.
1.2	Explain different fraud, bribery, and corruption typologies and vulnerabilities across an organisation.	Demonstrate knowledge of fraud, bribery, and corruption typologies and vulnerabilities across an organisation.
1.3	Summarise why fraud, bribery and corruption are committed across the public sector and its impact across society.	Demonstrate knowledge of why fraud, bribery and corruption are committed across the public sector and its impact across society.
1.4	Describe the fraud landscape, scale and impact in the UK.	Demonstrate knowledge of fraud landscape, scale and impact in the UK.

2. Organisational Knowledge

Foundation

Practitioner

2.1	Explain the various research methods used to obtain information from an organisation and its key stakeholders gain an understanding of the areas at risk from fraud to including the advantages and disadvantages of each approach.	Demonstrate the effective use of the different qualitative and quantitative research methods to obtain information from the organisation and its key stakeholders in order to gain an understanding of the areas at risk from fraud to inform areas of focus for fraud measurement.
2.2	Explain the need to analyse and present information relevant for planning the fraud measurement programme and associated activities.	Demonstrate how to analyse and present information relevant for planning the fraud measurement programme and associated activities.
2.3	Explain the importance of understanding the organisational structure and responsibilities in relation to the fraud risk landscape when planning fraud measurement.	Demonstrate an understanding of the organisational structure and responsibilities in relation to the fraud risk landscape when planning fraud measurement activities.
2.4	Explain the key parts of the organisational assurance landscape, including the role of internal audit, and the distinction between this and fraud measurement activities.	Demonstrate how the Fraud Measurement programme fits into the assurance landscape of the organisation and how this relates to the role of other assurance activities.

3. Fraud Measurement Planning

Foundation

Practitioner

- | | |
|--|--|
| <p>3.1 Explain how the scope of the measurement programme provides assurance over the accuracy and completeness of fraud, bribery and corruption reporting.</p> | <p>Demonstrate that the scope of the measurement programme provides assurance over the accuracy and completeness of fraud, bribery and corruption reporting.</p> |
| <p>3.2 Explain the need for the fraud measurement programme to cover all significant areas of spend and income within the organisation.</p> | <p>Demonstrate that the fraud measurement programme is aligned to the key fraud risks and main areas of spend and income for the organisation.</p> |
| <p>3.3 Explain how the fraud measurement programme is supported by an annual plan of measurement activities.</p> | <p>Demonstrate that the fraud measurement programme is supported by an annual plan of measurement activities.</p> |
| <p>3.4 Explain how to establish the objectives and scope for each measurement exercise.</p> | <p>Demonstrate the ability to establish objectives and scope for each measurement exercise ensuring the exercise is adequately resourced with appropriate skills, knowledge and expertise.</p> |
| <p>3.5 Explain how and why each fraud measurement activity or exercise needs to be supervised and quality assured.</p> | |

4. Fraud Risk Assessment Skills

Foundation

Practitioner

4.1	Explain the differences between and appropriate use of the three different levels of fraud risk assessment in the context of both fraud measurement planning and individual measurement activities.	Demonstrate the appropriate use of fraud risk assessments in the context of both fraud measurement planning and individual measurement activities.
4.2	Explain how fraud measurement fits into the fraud risk management cycle in relation to reporting and monitoring prevented and detected fraud, control testing and fraud loss measurement exercises.	Demonstrate how fraud measurement fits into the fraud risk management cycle in relation to reporting and monitoring prevented and detected fraud, control testing and fraud loss measurement exercises.
4.3	Explain how testing can be focussed on most significant fraud risk facing the organisation.	Demonstrate how testing is focused on significant fraud risk facing an organisation.

5. Statistical and Sampling Knowledge

Foundation

Practitioner

5.1	Explain the rationale of statistical sampling in the context of testing and measuring for fraud (and error).	Demonstrate that statistical sampling has been undertaken in the context of testing and measuring for fraud bribery and corruption.
5.2	Explain the importance of samples being representative of the overall population that you intend to test and measure.	Demonstrate that the sample(s) selected are representative of the overall population to be tested and measured.
5.3	Explain the significance of sub-populations and the implications for measuring and estimating if testing is solely focussed on one or more sub-population.	Demonstrate that where a sub-population has been tested that this limits any estimate of levels of fraud, bribery and corruption to that sub-population rather than the overall population.
5.4	Explain what confidence levels are and how sample size affects this.	Demonstrate the use of confidence levels when selecting the size of sample for testing.
5.5	Explain what precision is, what this means in terms of a range of possible results, and how sample size affects this.	Demonstrate that test results from a sample represent a range of possible values in the total population and how the chosen sample size affects this degree of precision, or margin of error.
5.6	Explain the differences between different sampling methodologies, their strengths and limitations when applied to different testing scenarios.	Demonstrate the use of appropriate sampling methodologies within different testing scenarios.

6. Identifying and Using Evidence to Test for Fraud

Foundation

Practitioner

6.1	Explain the use of various internal and external data sets for comparison and testing in the system or process being evaluated. Explain how issues in the data can impact testing, measurement, and estimating fraud.	Demonstrate the use of different internal and external data sets and information to be used for comparative purposes and testing within the system/process being measured. Show how shortcomings in the data can affect subsequent testing, measurement and estimating of fraud.
6.2	Explain what a test plan for a fraud measurement exercise should include.	Demonstrate that a detailed test plan has been developed for each measurement exercise to be undertaken before testing takes place.
6.3	Explain how the data needed for test purposes will be obtained, including recognition of legal requirements and protocols such as data protection or data sharing agreements.	Demonstrate consideration of the legal requirements around data handling and sharing as well as outlining the protocols and agreements needed to enable data sharing between organisations when obtaining data sets for testing.
6.4	Explain how to design individual tests within a fraud loss measurement exercise in order to determine whether or not fraud (or error) has occurred.	Demonstrate how to design individual tests within a fraud loss measurement exercise in order to determine whether or not fraud (or error), bribery or corruption has occurred.
6.5	Explain why it's important to keep appropriate records for each test.	Demonstrate appropriate records have been designed and used for each test to demonstrate the approach taken and ensure consistency in testing.

7. Statistical and Sampling Knowledge

Foundation

Practitioner

7.1	Explain how testing for instances of fraud can be used to measure and estimate levels of fraud and error within the targeted population.	Demonstrate an appropriate use of testing to facilitate the measurement and estimation of fraud and error within a targeted population.
7.2	Explain how to decide whether each item reviewed within a test sample indicates fraud, error, how this can be categorised, and if additional testing is required to reach a decision.	Demonstrate how the results of testing have been reviewed, categorised and quantified in order to reach a conclusion as to whether fraud or error has occurred or if additional testing is required.
7.3	Explain how to apply the results obtained from testing for fraud and how these can be interpreted and extrapolated within the population being reviewed.	Demonstrate that the results from fraud loss measurement testing have been used and extrapolated to measure and estimate the actual levels of fraud and error within the target population.
7.4	Explain the difference between detected fraud and error, prevented fraud and error, and estimated fraud and error.	Demonstrate the categorisation and quantifying of fraud measurement results distinguishing between detected, prevented and estimated fraud and error.
7.5	Explain the benefits of comparison to other public sector organisations to validate findings and the levels of irregularity measured and estimated.	Demonstrate an understanding of where benchmarking of fraud (or error), bribery or corruption measurement across the public sector would be helpful in putting results into context.
7.6	Explain how to identify the drivers pertaining to fraud risks, how they can impact levels of fraud, and how the extent to which these drivers are increasing/ decreasing can be measured through the development of fraud risk indicators.	
7.7	Explain the benefits of calculating ongoing savings through prevention and the need to have a robust methodology for calculating these savings.	Demonstrate the calculation of ongoing savings arising from preventative action taken, using robust methodology.
7.8	Explain how the effectiveness of the organisational counter fraud strategy, and related activities, is measured and monitored.	

8. Identifying and Using Evidence to Test for Fraud

Foundation

Practitioner

8.1	Explain the scope of fraud measurement reporting, including prevented and detected fraud, prevented savings and estimates of previously unknown fraud from control testing and fraud loss measurement exercises.	Demonstrate an understanding of the scope of fraud measurement reporting, including prevented and detected fraud, prevented savings and estimates of previously unknown fraud from control testing and fraud loss measurement exercises.
8.2	Understand why fraud measurement and testing results should be communicated to key stakeholders.	Demonstrate that the results of fraud measurement and testing have been communicated to all key stakeholders.
8.3	Explain how to incorporate key findings from fraud measurement into reporting.	Demonstrate the ability to incorporate key findings from fraud measurement into reporting using metrics such as spend and activity levels to illustrate organisational vulnerabilities.
8.4	Explain the importance of recognising and reporting any limitations with estimates and measurement of levels of fraud, including untested areas.	Demonstrate that reporting acknowledges and recognises any limitations with estimates and measurement and where the potential for unknown fraud still exists.
8.5	Explain how a regular routine for fraud reporting provides the ability to monitor trends over time.	Demonstrate the establishment of a regular routine for fraud reporting, ensuring consistent updates and annual aggregation of results to monitor trends over time.
8.6	Explain how fraud measurement results are linked to the organisation's fraud appetite statement and defined tolerance levels and support informed decision-making on control effectiveness and necessary actions to mitigate fraud risk.	Demonstrate how fraud measurement results are linked to the organisation's fraud appetite statement and defined tolerance levels to support informed decision-making on control effectiveness and necessary actions to mitigate fraud risk.

Appendix 2 – Fraud Reporting Categories and Typologies

Category	Definition
Prevented	Fraud or error stopped before it occurred. Sub-categories • Prevented actual: Value of prevented loss is known • Future loss prevented (fraud): Estimated ongoing prevented fraud loss • Future loss prevented (error): Estimated ongoing prevented error loss • Upstream Prevention: Controls implemented to reduce fraud/error rates.
Detected	Fraud or error identified after it happened. Sub-categories • Detected fraud: Loss due to fraud • Detected error: Loss due to a mistake • Detected bribery: Public sector bribe.
Recovered	Losses that have been successfully recouped. Sub-categories • Recovered fraud: Funds recovered from a fraud • Recovered error: Funds recovered from an error.
Typology Field	Every available value/option
Business Area	Benefits, Charges and other non-tax income, Grants, Licences and permits, Loans and credit guarantees, Personnel, Procurement, Special payments, Subsidies, Tax and duties.
Nature of Deception	Abuse of position: Allowances, Application for employment, Asset misappropriation, Contract rigging, Falsified application, Insider theft of assets, Mandate fraud, Misuse of purchasing card, Payment fraud Failure to declare/disclose: Abuse of working hours, Allowances, Application for employment, Asset misappropriation, Change of circumstances, Charge evasion, Expense claims, Misuse of funding. False representation: Abuse of working hours, Allowances, Application for employment, Asset misappropriation, Charge evasion, Expense claims, Falsified application, Falsified invoice, Impersonation of purchasing cardholder, Mandate fraud, Misuse of funding, Product substitution or misselling. Unknown: Unknown.

Category	Definition
Fraud Enabler	AI (artificial intelligence), Bribery, Coercion, Collusion, Conflict of interest, False identity, Phishing, Vishing and SMSing, Social media.
Who Committed Fraud	Contingent labour, Hostile third party, Members of the general public, Other public servants, Private sector (company, partnerships, or self-employed), Public sector employees, Public sector organisations, Third sector organisations, Unknown.
Error Origin	Customer, Official, Supplier, Unknown.
Prevention Activity	Automated compliance checks, Behavioural insights, Biometrics, Cyber security, Eligibility criteria and rules, External audit or review, Governance, Manual compliance checks, Risk scoring and Enhanced due diligence, Training and Awareness.
Recovery Type	Fraud: Indemnity, Offsetting, Through civil proceedings, Through criminal proceedings, Unknown, Covid Commissioner voluntary repayment scheme, Voluntary repayment . Error: Indemnity, Offsetting, Through civil proceedings, Unknown, Covid Commissioner voluntary repayment scheme, Voluntary repayment.
Counter Fraud Involvement	Counter fraud delivered, Counter fraud influenced, No counter fraud involvement.
COVID-19	Yes, No.

Appendix 3 – Spend Area Assessment

In the absence of an Enterprise Fraud Risk Assessment, a Spend Area Assessment may be undertaken to prioritise areas for loss measurement activity.

This is **not** the recommended approach to take and should only be done if necessary and only for exploratory exercises. Practitioners should adhere to the Fraud Risk Assessment Standard.

Creating a Spend Area Assessment requires practitioners to identify key areas of spend/income and then assess each area in order to identify: (a) areas most likely to be susceptible and vulnerable to the risk of fraud; (b) where testing is most likely to find previously unknown fraud and therefore (c) where a fraud loss measurement exercise would add the most assurance value.

In the basic risk assessment, the practitioner should score each area against four key risk factors:

- **Annual gross financial risk** – the materiality of each area (potential loss)
- **Reputational risk** – the extent to which fraud could have other consequences for the organisation besides financial
- **Inherent risk** – the extent to which levels of fraud within the area are currently understood, measured and reported, and if there is a strong possibility of additional undetected fraud. For example the risk might be considered higher if little or no fraud is being detected in this area and/or levels of reported fraud are less than 0.5% of expenditure
- **Control/residual risk** – the extent to which there is assurance that the controls within a particular area are well-designed and operating as intended. For example, the risk might be considered higher if controls do not cover all the fraud and error risk, or it is not known how well-designed or operationally effective the controls are.

Appendix 4 – Fraud Prevention Savings Framework³⁶

Savings Term Fraud Measurement Standard	Savings Term Fraud Prevention Savings Framework
(Prevented Actual) Point of Interdiction	Point of Intervention
Future Loss Prevented	Secondary Prevention
Upstream Prevention	Primary Prevention
N/A	Primordial Prevention (prevention from controls built into new spend from outset)
Recovered Losses	Tertiary Prevention

36 <https://www.gov.uk/government/publications/fraud-prevention-savings-framework>

Appendix 5 – Reporting Findings From Fraud Measurement Exercises

Template for reporting findings from fraud measurement exercises [D3]

[illegible]

Template for estimating, interpreting and extrapolating results

[illegible]



Public Sector
Fraud Authority

