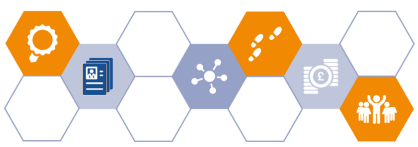
Government
Counter Fraud
Profession

Government Counter Fraud Professional Standards and Guidance

Fraud Measurement Core Discipline

January 2021



Crown copyright disclaimer

Contents

A. Introduction to the Fraud Measurement Discipline

A1. Purpose

A2. Aims

A3. Note on using these Standards and Guidance

A4. How this document is structured

A5. Feedback and Further Information

B. Introduction to the Government Counter Fraud Profession

B1. Government Counter Fraud Function

B2. Governance of the Government Counter Fraud Profession

B3. Government Counter Fraud Disciplines Framework

C. Professional Standards and Competencies

C1. Introduction to the Fraud Measurement Professional Standards and Competencies

C2. Scope

C3. General Principles for Fraud Measurement Professionals

C4. Structure of the Fraud Measurement Competency Framework

C5. The Fraud Measurement Competency Framework

D. Guidance for Professionals - Process

D1. Introduction

D2. Process for capturing and reporting detected loss and prevented loss due to fraud

D3. Identifying areas vulnerable to fraud and selecting areas for measurement

D4. Carrying out a detailed Fraud Risk Assessment

D5. Planning and undertaking testing to find fraud and error

D6. Choosing statistically valid samples for testing

D7. Identifying and selecting evidence / test data

D8. Estimating and measuring levels of fraud and fraud losses

D9. Methodology to follow for calculating prevented savings

D10. Reporting on the results of fraud testing and estimation.

E. Guidance for Professionals - Products

E1. Introduction

E2. Fraud reporting – details of requirements to include in the reporting of fraud or error found through the operation of existing business controls

E3. Detailed fraud risk assessments of targeted areas

E4. Fraud loss estimation and measurement – outputs from fraud measurement exercises

E5. Calculation of savings generated through a fraud measurement exercise including future (prevented) savings resulting from improved controls or the introduction of new controls and processes

F. Guidance for Organisations

F1. Introduction

F2. Mapping and understanding assurance requirements in relation to fraud risks to quantify associated fraud risk exposures and resulting losses

F3. Building a fraud measurement programme within the organisation

F4. Developing and implementing an annual plan as part of the ongoing fraud measurement programme

F5. Governance and oversight of the fraud measurement programme

F6. Measuring the effectiveness of the counter-fraud strategy

F7. Continuing Professional Development

G. Glossary

G1. Glossary

Annex A: Typology used to report fraud and error in Central Government

A. Introduction to the Fraud Measurement Discipline

A1. Purpose

This document contains the agreed professional standards and guidance for the implementation of a consistent approach for the measurement of fraud, and error, in central government. This document is part of the wider government Counter Fraud Standards and Guidance, covering all the core disciplines and sub disciplines in the government Counter Fraud Framework. This document is intended to reflect the position in England and Wales.

The standards are designed to facilitate a consistent cross-government approach to counter fraud, raise the quality of organisations' counter fraud work and the skills of individuals working in counter fraud.

A2. Aims

The professional standards and guidance's aim is threefold:

- to describe the knowledge, skills and experience (professional standards and competencies) for those working in Fraud Measurement. These are detailed in the competency framework, outlining how someone can progress through this standard;
- to provide guidance on the processes and products individuals will use to deliver the core discipline and what they should seek to put in place in the organisation to achieve this; and
- the 'Organisational Guidance' to consider what individuals' should put in place in an organisation applicable to the core discipline. These should be read in conjunction with the HMG Functional Standards.

A3. Note on using these Standards and Guidance

The extent to which central government bodies utilise these professional standards and guidance will vary and develop according to their assessment of fraud risk, which will drive their counter fraud strategy and their investment in counter fraud activities.

Some organisations will have established specialist counter fraud teams and these standards are designed to enable those teams to develop their capability in a consistent way across government that will, over time, increase the ability of these organisations to share resources and practice under a common understanding.

For organisations that make use of more ad-hoc resource for fraud measurement, the intention is for this resource to develop to meet the standards within this document, if they do not already.

These standards will form the basis of the Fraud Measurement part of the Counter Fraud Profession that is being established within government. To be acknowledged as a Counter Fraud Professional in Fraud Measurement, these standards will have to be met.

For further guidance on these standards please contact the Counter Fraud Centre of Expertise at the Cabinet Office, which coordinates standards activity, or the Counter Fraud and Investigations Service in Government Internal Audit Agency (GIAA). Contact details are provided in section A5.

A4. How this document is structured

This document contains the following:

- The Competency Framework outlining the knowledge, skills and experience required by those undertaking fraud measurement to operate effectively, and how these develop through the competency framework levels Trainee, Foundation and Practitioner.

- Guidance for Professionals includes:
  - Process guidance describing the recommended processes for organisations to correctly implement fraud measurement processes;
  - Product guidance setting out guidance on developing good quality outputs in relation to reporting and measuring fraud and error; and
  - Organisation guidance outlining the key considerations for an organisation in relation to fraud measurement and reporting.

The Standards have been created, reviewed and agreed by the Government Counter Fraud Profession Board, the body with oversight of the Profession, and responsibility for the development and maintenance of the Counter Fraud Professional Standards and Guidance. The board has been assisted by an expert Cross Sector Advisory Group (CSAG).

A5. Feedback and Further Information

The Government Counter Fraud Professional Standards and Guidance have been created in order to align counter fraud capability across government.

If you have any questions surrounding the Government Counter Fraud Profession, and how you can get yourself and your organisation involved, or if you would like to provide feedback on the Government Counter Fraud Professional Standards and Guidance please contact GCFP@cabinetoffice.gov.uk

Alternatively, the Counter Fraud and Investigation Team in the Government Internal Audit Agency (GIAA) provide 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

B. Introduction to the Government Counter Fraud Profession

B1. Government Counter Fraud Function

The Counter Fraud Function is one of government's fourteen functions. The aim of the Functions is to develop the Civil Service to evolve and be even more efficient. The Counter Fraud Function brings together over 15,000 public servants who work to find and fight fraud across the public sector, including those who focus on understanding and mitigating fraud risks. Although new, the Counter Fraud Function has already published a Functional Standard, a Strategy and launched the first Counter Fraud Profession. The vision of the Counter Fraud Function 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, and these teams make up the wider government function, supported by expertise in other public bodies and the functional centre. The Counter Fraud Centre of Expertise (CoEx) at the Cabinet Office is responsible for overall leadership of the function, including overseeing the strategy, defining standards and monitoring performance. Within the Functional Standards for Counter Fraud, there is a clear ask of organisations in relation to finding previously unknown fraud, measuring and estimating levels of fraud and error, and reporting instances of fraud prevented and detected.[1]

B2. Governance of the Government Counter Fraud Profession

The Government Counter Fraud Profession has a clear governance structure, established in 2015. The Government Counter Fraud Profession 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 the Counter Fraud, but all have an equal vote on the Board. The key principles when developing the Profession, as agreed by the Board are Collaboration, Choice, Empowerment and Pace.

[1] Functional Standard 8: Report identified loss from fraud, bribery, corruption and error, associated recoveries, to the centre in line with the agreed government definitions.
Functional Standard 10: Undertake activity to try and detect fraud in high-risk areas where little or nothing is known of fraud, bribery and corruption levels, including loss measurement activity where suitable.

The Board is supported by a cross sector advisory group. This is made up of experts in counter fraud from a range of sectors, including academic, financial, legal and regulatory. The advisory group act as a critical friend to the decisions made by the Board.

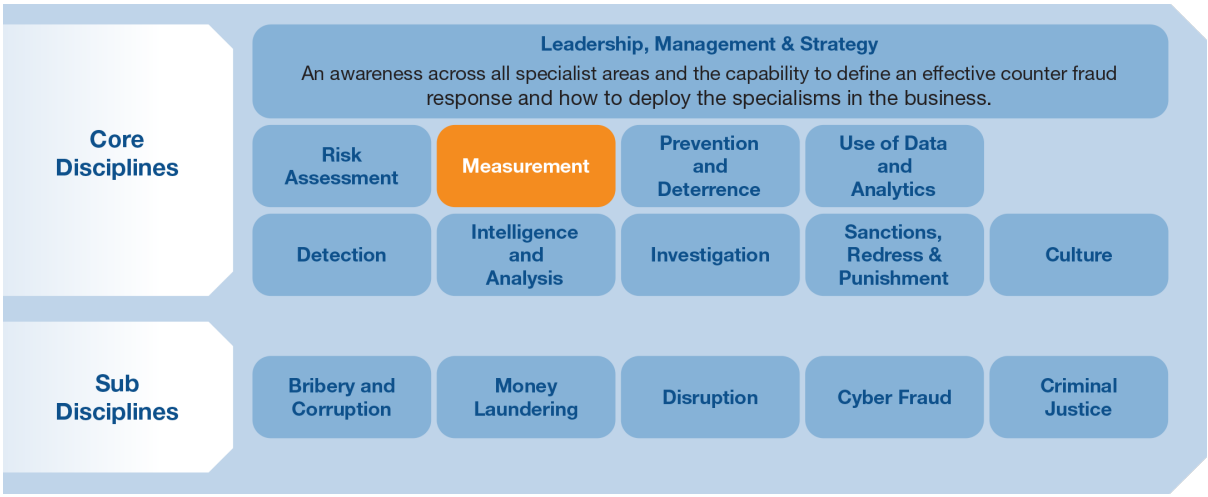
The Profession is built by experts, for experts. The products of the Profession derive from collaboration across the public sector and beyond. Many organisations have invested resource into developing standards and guidance for the Profession. They have also offered support to the Advisory Panels (that review applications for Collective Membership) and the Learning Groups (who advise on training or development related decisions for the Profession).

B3. Government Counter Fraud Disciplines Framework

This document covers the Fraud Measurement Core Discipline of the Government Counter Fraud Framework.

The Framework below covers all of the core disciplines and sub-disciplines that organisations need to call upon to deal with the threat of fraud. Organisations will call on these to differing extents depending on the nature of their business, services and the associated fraud threat, as assessed through fraud risk assessment.

Government Counter Fraud Profession Standards



Core Disciplines: The core disciplines include a functional leadership level (Leadership, Management, Strategy) for those that are responsible for coordinating an organisation's overall response to fraud and economic crime. 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.

Sub Disciplines: The sub disciplines are areas of additional knowledge, skills and expertise that enhance capability across a number of core disciplines. For instance, knowledge, skills and experience in Bribery and Corruption will help Counter Fraud

professionals undertake more effective risk assessments and investigations (depending on their role).

C. Professional Standards and Competencies for the Fraud Measurement Discipline

C1. Introduction to the Fraud Measurement Professional Standards and Competencies

The Professional Standards and Competencies for the Fraud Measurement Discipline identify the knowledge, skills and experience required when measuring and estimating levels of fraud and error and reporting instances of prevented and detected fraud and error. Individuals can use the Standards to measure and develop their skills, not only within this discipline but also in others. This information is then helpful to target learning and development, and assist career planning.

Standards and competencies also help individuals within organisations identify the research, training and resources needed to develop capability further, and identify skill gaps and how to address them.

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. They are living documents, owned by the Profession Board and will be maintained and updated as applicable.

C2. Scope

This document focuses on individuals' capability to measure, estimate, and report instances of fraud and error. The scope of this Standard covers the following activities:

- Reporting of instances of fraud or error as detected / prevented by existing controls (including for government departments reporting to the centre via the Consolidated Data Request), which provides baselining 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 control.
- Calculating and reporting recoveries of detected fraud.
- Using methodologies for calculating ongoing savings of prevented fraud and error.

This discipline is therefore focused on the practical application of fraud measurement and reporting. It includes many factors, such as:

- An understanding of counter fraud context, including knowledge of types of fraud, and how the organisation may be vulnerable to each fraud type;
- Skills needed to design and deliver a Fraud Measurement programme.
- The process and techniques for effective measurement of fraud risk exposures.
- Communicating assessed vulnerabilities to fraud, including ensuring that there is accurate and complete reporting of estimated fraud and instances of detected and prevented fraud and error.

In undertaking testing to find and measure previously undetected fraud, this standard draws upon and uses elements from other counter fraud disciplines such as Fraud Risk Assessment and the use of Data and Data Analytics. Whilst this standard covers the requirements relevant to the delivery of the Fraud Measurement discipline, it does not seek to replace other standards. Where it is appropriate, reference, and adherence should be maintained with Standards covering other Counter Fraud disciplines.

These Professional Standards and Competencies specify the skills that are required by those involved in fraud measurement and reporting.

The skill competence levels required are at an increasing level of expertise; from Trainee to Foundation, and then Practitioner (see section C4 for further explanation of the competency levels).

C3. General Principles for Fraud Measurement Professionals

Staff engaged in Fraud Measurement and Reporting are expected to display the highest standards of professionalism as reflected in the GCFP Code of Ethics: integrity, honesty, objectivity and impartiality; with specific behaviours demonstrated of being courageous, challenging, collaborative and objective. The conduct of all activity will abide by these principles and if a conflict of interest exists, staff will disclose this fact at the earliest opportunity.

Those engaged in applying this Fraud Measurement Standard should;

- **Use fraud measurement to improve counter fraud outcomes**:
  - Continuously consult, engage and work with others in the counter fraud function, to ensure that fraud reporting, associated analysis, measurement and estimation provide useful insight for counter fraud decision making, including informing the counter fraud strategy, and help the achievement of counter-fraud outcomes.
  - Produce analysis that has impact, and understand the effect of their impact on others in the counter fraud area.
  - Promote the application of fraud measurement for counter fraud purposes, and demonstrate to other counter fraud professionals the value it has to help understand and focus on fraud problems.

- Understand the constantly evolving nature of fraud, and seek out innovative ways of testing for fraud, including applications of data analytics and analysis, to address new challenges, whilst recognising the need for proportionality of resource.

➢ **Be impartial and ethical when using data**:
- Understand and implement necessary data governance and ethics legislation, principles and practices when handling, sharing and using data, such as the Data Protection Act, Digital Economy Act and Freedom of Information Act.

➢ **Produce reliable, high quality analysis:**
- Ensure knowledge of related GCFP Standards such as those for Fraud Risk Assessment and Data Analytics & Analysis, and the counter fraud context in which they are being applied, are up to date. Recognise and meet gaps within this knowledge.

➢ **Produce analysis and outputs that make efficient use of resources and are value for money:**
- Testing for undetected fraud, and associated measurement, should focus on those areas of the organisation where there is significant risk of fraud, or where there is considerable spend and activity and levels of fraud and error are currently unknown.
- The outputs from fraud measurement activity should be a key driver in setting the future direction and strategy for counter-fraud activities.

➢ **Undertake activity that is consistent with the Civil Service values and behaviours, diversity and equality policy**
- In accordance with individual organisations' code of conduct, practices and procedures, recognising when legislation, policies and procedures need reviewing or updating.

C4. Structure of the Fraud Measurement Competency Framework

The information on the next page explains the structure of the Competency Framework and how it can be utilised by members of the Profession.

C4.1 Key Components Explained

Components outline at a high level, the knowledge, skills and experience required for each core & sub discipline. There are 8 key components for the Fraud Measurement Discipline. 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 (see page 17).

Counter Fraud Knowledge
Developing knowledge of the fraud landscape within the organisation, the public sector, the UK, and internationally across a range of specialisms.

Business knowledge
Skills and experience in utilising a range of research methods to gain knowledge of the organisation's structures and business activities.

Measurement Assurance Planning
Planning annual programmes of measurement activity to provide assurance to the organisation on the scale of its vulnerability to fraud and error and associated losses.

Risk Assessment Skills
Understanding the fraud risk profile of an organisation and developing experience and skills to evaluate the effectiveness of existing controls and assess residual risk.

Statistical and Sampling Techniques
Knowledge of statistics and understanding and implementing various sampling techniques appropriate to the analysis and measurement required.

Identifying and using evidence to test for fraud
The skills needed to identify, collect, record and store data and evidence in a correct and lawful manner and designing tests to use this data to test for whether fraud has occurred.

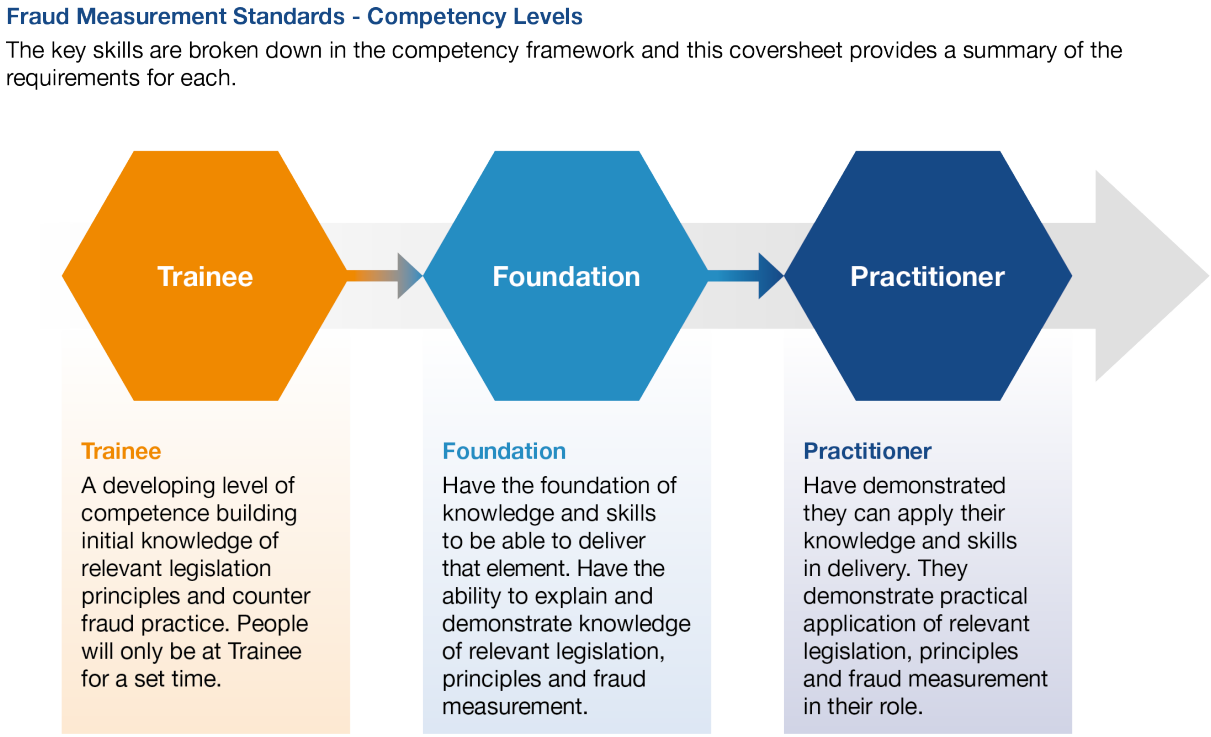
Estimation and Measurement
Understanding various techniques to estimate and measure instances of fraud and error, including methodologies to calculate future savings.

Stakeholder engagement and reporting
Reporting the outcome of measurement activity including the capture of what is already known and detected; actual losses and what has been recovered or prevented.

Within the Competency Framework are three **Competency Levels**. These range from **Trainee, Foundation to Practitioner**. These 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.

General rules about the **Competency Levels** are set out below:

- **Trainee** is about developing introductory knowledge;
- **Foundation** is about having the knowledge;
- **Practitioner** is about demonstrating the application of the knowledge.



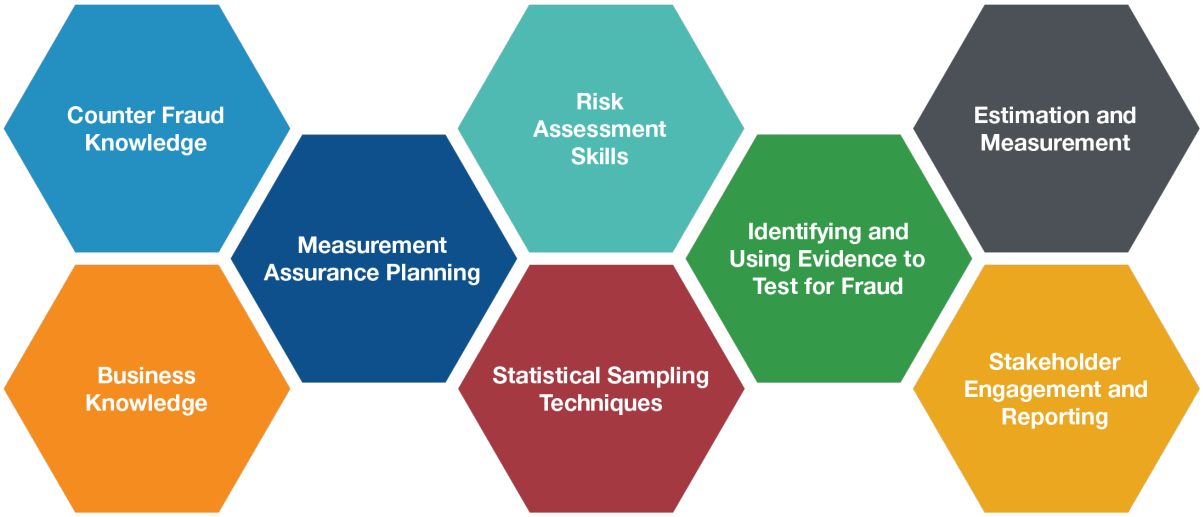
Advanced Practitioner works differently to the other levels as there are no predetermined categories for this level. Instead, members can select individual or groups of elements they have a particular interest or focus in, to demonstrate their skills, knowledge and experience. The knowledge skills and experience for an Advanced Practitioner level within the Fraud Measurement discipline will be determined at a later stage.

C4.3 Understanding Categories

Categories recognise and provide for specialisation within the discipline and will be developed at a later stage if required. The initial version of this Standard is intended to publish a recognised standard for fraud measurement across government. The next stage of agreeing a process to on-board individuals to this discipline will also consider the need for 'Categories'.

C4.4 Competency Framework

Below you will find a detailed competency framework outlining the knowledge, skills and experience required for the fraud measurement discipline. Within each of the eight key components (see diagram below) you will find descriptors of the elements required at each level, from trainee to practitioner level.



Counter Fraud Knowledge
Developing knowledge of the fraud landscape within the organisation, the public sector, the UK, and internationally across a range of specialisms.

Business knowledge
Skills and experience in utilising a range of research methods to gain knowledge of the organisation's structures and business activities.

Measurement Assurance Planning
Planning annual programmes of measurement activity to provide assurance to the organisation on the scale of its vulnerability to fraud and error and associated losses.

Risk Assessment Skills
Understanding the fraud risk profile of an organisation and developing experience and skills to evaluate the effectiveness of existing controls and assess residual risk.

Statistical and Sampling Techniques
Knowledge of statistics and understanding and implementing various sampling techniques appropriate to the analysis and measurement required.

Identifying and using evidence to test for fraud
The skills needed to identify, collect, record and store data and evidence in a correct and lawful manner and designing tests to use this data to test for whether fraud has occurred.

Estimation and Measurement
Understanding various techniques to estimate and measure instances of fraud and error, including methodologies to calculate future savings.

Stakeholder engagement and reporting
Reporting the outcome of measurement activity including the capture of what is already known and detected; actual losses and what has been recovered or prevented.

C5. The Fraud Measurement Competency Framework

Competency 1: Counter Fraud Knowledge

13 elements:

1.1	Statutory frameworks
1.2	Professional standards
1.3	Defining fraud
1.4	Data handling and sharing
1.5	Motivation of fraudsters
1.6	People who commit fraud
1.7	Victims of fraud
1.8	Fraud typologies
1.9	Fraud controls and prevention tools
1.10	Fraud in the public sector
1.11	Fraud risk management
1.12	Role of different business units in combatting fraud
1.13	Bribery and corruption

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
1.1 Counter Fraud Knowledge – **Statutory Frameworks**	Identify the key legislation making up the statutory framework that is relevant to fraud measurement and reporting activity, including those covering fraud and bribery and data handling and sharing.	Explain how the statutory framework is relevant for measuring and reporting fraud to help bring these to life for those engaging in the process.	Demonstrate the application of the statutory framework in the discussion of fraud measurement and reporting to help bring these to life for those engaging in the process.
1.2 Counter Fraud Knowledge – **Professional Standards**	Identify that there are several relevant professional standards, associated guidance materials, including the GCFP Code of Ethics and Civil Service Code, and regulatory requirements.	Explain the relevant professional standards, associated guidance materials, including the GCFP Code of Ethics and Civil Service Code, and regulatory requirements.	Demonstrate the application of the relevant professional standards, associated guidance materials, including the GCFP Code of Ethics and Civil Service Code, and regulatory requirements.
1.3 Counter Fraud Knowledge – **Define Fraud**	Identify the principle fraud offences within the Fraud Act 2006, Theft Acts 1968, Proceeds of Crime Act 2002 and other relevant legislation.	Explain the principle fraud offences within the Fraud Act 2006, Theft Acts 1968, Proceeds of Crime Act 2002 and other relevant legislation.	Demonstrate and apply knowledge of the principal fraud offences within the Fraud Act 2006, Theft Acts 1968, Proceeds of Crime Act 2002 and other relevant legislation.
1.4 Counter Fraud Knowledge **–** **Data handling and sharing**	Identify the relevant legislation including the General Data Protection Act and the Digital Economy Act	Explain the main principles for handling and sharing data as outlined in the General Data Protection Act and the Digital Economy Act.	Demonstrate the practical application of handling and sharing data in compliance with the General Data Protection Act and Digital Economy Act.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
1.5 Counter Fraud Knowledge – **Motivation of Fraudsters**	Identify the theories regarding the motivation of fraudsters and the elements of fraud such as the Fraud Triangle/Diamond, Rational Choice, Routine Activity Theory, Differential Association and the Fraud Scales Model.	Explain the theories regarding the motivation of fraudsters and the elements of fraud such as the Fraud Triangle/Diamond, Rational Choice, Routine Activity Theory, Differential Association and the Fraud Scales Model.	Demonstrate the application of theories regarding what motivates fraudsters and the elements of fraud such as the Fraud Triangle/Diamond, Rational Choice, Routine Activity Theory, Differential Association and the Fraud Scales Model.
1.6 Counter Fraud Knowledge**- People who commit fraud – fraud personas**	Identify that there are a variety of types of people who commit fraud from inside the organisation and/or externally with different motivators.	Explain who fraudsters are, the range of people who commit fraud from inside the organisation and/or externally and the different motivators, including organised crime and terrorist financing. Explain the different personas of those who commit fraud.	Demonstrate and apply knowledge of the range of people who commit fraud from inside the organisation and/or externally and the different types of fraud personas. Understand the motivators for fraud, including organised crime and terrorist financing, as well as the relationship between different fraudsters and organisations.
1.7 Counter Fraud Knowledge**– Victims of Fraud**	Identify that there are a range of people and organisations that may be victims of fraud and name a number of victim organisations and demographic groups.	Explain who the victim of fraud is in a range of scenarios (e.g. governmental organisation, financial services institute, other organisations, individuals) and explain the potential impacts on the victims e.g. - financial, physical,	Demonstrate and apply knowledge of who the victim of fraud may be in a range of scenarios (e.g. governmental organisation, financial services institute, other organisations, and individual) and the impacts on the victims e.g. - financial, physical, social, reputational and potential

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
		social, reputational and potential national security issues.	national security issues.
1.8 Counter Fraud Knowledge – **Fraud Typologies**	Identify the various ways to categorise fraud into types e.g. by functions and processes (such as types of procurement or grant fraud); by modus operandi (misappropriation of assets, financial statement fraud, and bribery) or by victim.	Explain the various fraud types that exist (by functions or processes, modus operandi, and victim).	Demonstrate the ability to apply knowledge of the various fraud types whilst categorising fraud risks in the context of fraud measurement.
1.9 Counter Fraud Knowledge– **Fraud Controls and Prevention Tools**	Identify that there are a variety of different controls used to deter, prevent, detect and disrupt fraudsters and name a few key concepts e.g. segregation of duties, policy frameworks and freezing assets.	Explain how organisations, including your own, use key fraud controls and mitigations to prevent, detect, deter and disrupt fraud and that technology has a huge impact in this area.	Demonstrate and apply an understanding of a range of fraud controls and mitigations used to deter, prevent and detect fraud and how current trends and technology impact this area.
1.10 Counter Fraud Knowledge– **Fraud in Public Sector**	Identify a few types of fraud across different sectors and those within public sector including, procurement fraud,	Explain the types of fraud seen across the public sector including, procurement fraud, corruption, and grant fraud.	Demonstrate and apply an understanding of the different types of fraud across the public sector including, procurement fraud, corruption, and grant fraud.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
	corruption, and grant fraud.		
1.11 Counter Fraud Knowledge– **Fraud Risk Management**	Identify the elements of the fraud risk management cycle.	Explain the elements of the fraud risk management cycle and the need for ongoing assurance and evaluation over fraud risk exposures.	Demonstrate and apply an understanding of the elements of the fraud risk management cycle, in particular the need for ongoing assurance and evaluation over fraud risk exposures.
1.12 Counter Fraud Knowledge – **Role of different business units in combatting fraud**	Identify all the business units with responsibility for different aspects of fraud risk management.	Explain the role of the business units in managing fraud risk e.g., Policy, Operations, Finance, Legal, HR, Risk Management, Internal and External Audit (NAO) and other relevant business units.	Demonstrate and apply an understanding of how different business units manage the risk of, and the response to, fraud. Also apply an understanding of the roles of various BUs in this process e.g. such as Finance, Legal, HR, Risk Management, Internal and External Audit (NAO) and other relevant business units.
1.13 Counter Fraud Knowledge– **Bribery and Corruption**	Identify that there are differences in how bribery and corruption are defined and how it is carried out.	Explain the modus operandi of bribery and corruption and provide examples for each, together with the potential impact - financial, physical and reputational.	Demonstrate and apply knowledge of the various elements of bribery and corruption relating to the assessment of the fraud risks an organisation faces, together with the potential impact - financial, physical and reputational.

Competency 2: Business Knowledge and Skills

6 elements:

1.1 Research methods

1.2 Qualitative and Quantitative techniques

1.3 Using management information

1.4 Review of relevant information

1.5 Contractual points

1.6 Understanding the assurance landscape and role of related assurance activities

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
2.1 Business Knowledge & Skills – **Research Methods**	Identify various research methods used to obtain information from an organisation and its key stakeholders in order to gain an understanding of the organisation, its strategy, structure, key objectives, delivery targets, key financial systems, policies and processes. This could include, but is not limited to, desk-based research, interviews, surveys, process walkthroughs, workshops, meetings, focus groups, and document review.	Explain the various research methods used to obtain information from an organisation and its key stakeholders including the advantages and disadvantages of each approach.	Demonstrate the effective use of the different qualitative and quantitative research methods used to obtain and analyse information from the organisation and its key stakeholders in order to gain an understanding of the organisation and the areas at risk from fraud which will inform areas of focus for fraud measurement. This will include its strategy and policy objectives, all aspects of its operations, delivery targets and associated mechanisms.
2.2 Business Knowledge & Skills - **Qualitative and Quantitative Techniques**	Identify, in general terms, the employees, stakeholders, business processes and documentation that are essential to the development of a successful programme of fraud and error measurement and reporting.	Explain the qualitative and quantitative techniques that may be applied to this data to plan and produce an effective programme of fraud and error measurement and reporting.	Demonstrate the ability to use the appropriate qualitative and quantitative techniques to effectively obtain and analyse all the information needed to identify, categorise and classify those fraud risks to which the organisation is, or may be vulnerable which will direct fraud and error measurement and reporting activities.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
2.3 Business Knowledge & Skills – **Management Information**	Identify that management information (MI) has a key role to play in the assessment and monitoring of fraud reporting and measurement.	Explain the role of MI in supporting fraud measurement and reporting and how recent, current and future changes in processes or systems within an organisation might impact on the quality of the MI.	Demonstrate the use of quality MI to assess and fraud risks to identify areas for measurement, whilst successfully influencing other parts of the organisation to provide more effective MI to identify and manage fraud risks.
2.4 Business Knowledge & Skills - **Review of Relevant Information**	Identify the types of information that should be reviewed when planning a fraud measurement programme and associated activities, including, but not limited to, strategy documents, governance arrangements (structures, delegations and accountabilities), business plans and objectives, deliverable products and services, available technologies, organisational culture, risk management processes and outputs and control frameworks.	Explain the need to review and précis relevant information to the person responsible for the fraud measurement programme and how this will aid measurement activities and exercises.	Demonstrate and systematically assimilate complex information to extract that which is relevant for planning the fraud measurement programme and associated activities.
2.5 Business Knowledge & Skills - **Contractual Points**	Identify the relevance for understanding fraud risks in identifying customer contact points within the delivery of government services; or the	Explain the importance of understanding how an organisation's services are delivered for identifying fraud risks. These could include where	Demonstrate the application and understanding of how an organisation's services are delivered. These could include where accountability rests throughout a customer's journey for

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
	parties to a contract and the key contractual points throughout a supply chain.	accountability rests throughout an overall customer journey for government services; or within a supply chain, for the quantity and quality of goods or services, the nature of contractual relationships and the capability of the team managing the contract to hold the supplier to account with appropriate checks and balances.	government services; or within a supply chain, the nature of contractual relationships and the capability of the team managing the contract to hold the supplier to account/put in place appropriate checks and balances.
2.6 Business Knowledge & Skills – **Understanding the assurance landscape and role of related assurance activities**	Identify the key components of an organisation's assurance model, including how these map onto a 3 lines of defence model. Identify how fraud measurement fits into this assurance landscape.	Explain the key parts of the organisational 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 the role of other assurance activities, such as internal audit, in providing assurance over the quality and operation of controls compared to the particular focus in measuring fraud on residual risk and testing to see if gaps and weaknesses in controls have been exploited by fraudsters.

Competency 3: Measurement Assurance Planning

10 elements:

1.1	Communication and facilitation skills – engagement for developing a fraud measurement programme	1.6	Identifying priorities for inclusion in the annual plan
1.2	Scope of activities to include in a fraud measurement programme	1.7	Reviewing and adjusting the annual plan
1.3	Meeting assurance needs through the coverage of a fraud measurement programme	1.8	Determining objectives and scope for each activity
1.4	Engagement for developing an Annual Plan of measurement activities	1.9	Resourcing the annual plan
1.5	Organisational awareness	1.10	Supervision

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
3.1 Measurement Assurance Planning **- Communication and Facilitation Skills – engagement for developing a fraud measurement programme**	Identify the importance of communicating confidently to all levels of an organisation the need for an ongoing programme of fraud measurement.	Explain the process of engaging with a range of people in an organisation to develop an ongoing programme of fraud measurement as a key element of the counter fraud strategy.	Demonstrate engagement with a range of stakeholders across the organisation in order to achieve recognition of the importance of the fraud measurement programme as a key of the organisation's counter fraud strategy.
3.2 Measurement Assurance Planning **– scope of activities to include in a fraud measurement programme**	Identify the key areas of scope within a programme of fraud measurement including reporting of actual cases; estimation and measurement of additional undetected losses; measurement of recoveries compared to losses; and prevented savings.	Explain how an ongoing programme of fraud measurement should include within its scope the following activities: reporting of fraud and error as prevented / detected by existing controls; measurement and estimation of undetected fraud and error through fraud loss measurement exercises; calculating and reporting recoveries of detected fraud and error; calculating methodologies for capturing ongoing savings of prevented fraud and error.	Demonstrate that the scope of the measurement programme can provide assurance over the accuracy and completeness of reporting of detected fraud and error; measurement of underlying levels of undetected fraud and error losses; recovery of losses; and prevented savings.
3.3 Measurement Assurance Planning **– meeting assurance needs through the coverage**	Identify the need for the fraud measurement programme to be aligned to key fraud risks and	Explain how the scope of the coverage of the programme of fraud measurement must ensure it covers	Demonstrate that all the activities within the fraud measurement programme, including fraud loss measurement

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
of a fraud measurement programme	main areas of spend / income for the organisation.	all significant areas of spend / income within the organisation as well as all the fraud risks captured on the organisation's high-level fraud risk assessment.	exercises, cover all significant areas of spend / income within the organisation as well as coverage of all fraud risks identified on the high-level fraud risk assessment.
3.4 Measurement Assurance Planning **– engagement for developing an Annual Plan**	Identify that the programme for fraud measurement should lead to, and be supported by, an annual plan of measurement activities and exercises.	Explain the process of engaging with a range of people in an organisation to develop an annual plan of fraud measurement activities to provide an achievable annual plan in support of the overall programme of fraud measurement.	Demonstrate that the overall fraud measurement programme is supported by an annual plan of measurement activities and exercises and that this has support throughout the organisation, achieved through engagement with relevant stakeholders.
3.5 Measurement Assurance Planning **– organisational awareness**	Identify the need for the annual plan for fraud measurement activities needs to be set within a context of what the organisation seeks to deliver and how fraud could undermine this.	Explain how in developing the annual plan for fraud measurement it is necessary to understand the organisation's strategies, key business objectives, associated fraud risks, and fraud risk management processes.	Demonstrate the annual plan for fraud measurement reflects the organisation's strategies and business objectives and considers how associated fraud risks could undermine those strategies and objectives.
3.6 Measurement Assurance Planning **- identifying priorities for inclusion in the annual plan**	Identify that in scoping an annual plan for fraud measurement activity, a range of activities should be considered that are prioritised to reflect organisational and	Explain how to identify priorities for an annual plan for fraud measurement so that it contains a series of fraud and error loss measurement activities and exercises that align to areas representing key fraud risks to the	Demonstrate that the annual plan was developed from a range of possible activities that have been prioritised to reflect the best coverage of key fraud risks, aligning with the organisation's counter fraud strategy.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
	counter fraud priorities.	organisation. This should be consistent with the organisation's counter fraud strategy.	
3.7 Measurement Assurance Planning **– reviewing and adjusting the annual plan**	Identify the need to keep annual plans, such as for fraud measurement, under review with the facility to adjust if required to reflect changing priorities.	Explain how the annual plan for fraud measurement must be reviewed and adjusted as necessary in response to changes in the organisation's business, operations, programmes, systems, and associated fraud risks.	Demonstrate that the annual plan has been kept under review and adjusted where appropriate to reflect changed priorities for the organisation.
3.8 Measurement Assurance Planning **– determining objectives and scope for each measurement activity**	Identify the need for the objectives and scope for every activity and exercise within the annual fraud measurement plan to be clearly established.	Explain how objectives should be established for each fraud measurement exercise, with an established scope that is sufficient to achieve the objectives of the exercise.	Demonstrate the relevance of the objectives and scope established for every activity and exercise within the annual fraud measurement plan through supporting analysis of the probability of significant exposure to fraud or error within areas of associated processes, schemes or systems.
3.9 Measurement Assurance Planning **– resourcing the annual plan**	Identify that resourcing of fraud measurement activities is an important consideration that takes into account knowledge, skills and expertise.	Explain how it is necessary to quantify resources needed as well as the mix of knowledge, skills, and other expertise to successfully achieve the objectives of a fraud measurement activity or exercise.	Demonstrate that each fraud measurement activity or exercise has been adequately resourced with appropriate levels of knowledge, skills and expertise in order to achieve its objectives.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
3.10 Fraud Measurement Assurance Planning **– Supervision**	Identify the importance of supervision to ensure that fraud measurement activities are kept on track to deliver to time and quality.	Explain how each fraud measurement activity or exercise needs to be properly supervised to ensure that objectives are achieved, work is quality assured against recognised quality criteria, and facilitating the development of those participating.	Demonstrate appropriate supervision of fraud measurement activities and exercises through facilitating the development of staff engaged whilst ensuring that objectives were delivered on time and in accordance with recognised quality criteria.

Competency 4: Fraud Risk Assessment skills

8 elements:

1.1	Use of fraud risk assessments	1.5	Identification of controls
1.2	Levels of Fraud Risk Assessment (High, Intermediate and Detailed)	1.6	Evaluation of the effectiveness of controls
1.3	Use of detailed fraud risk assessments	1.7	Assessment of residual risk
1.4	Describing and recording fraud risks	1.8	Using residual risk to target areas for testing

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
4.1 Fraud Risk Assessment Skills – **Use of fraud risk assessments**	Identify the need for fraud measurement activities to be informed by fraud risk assessments undertaken in accordance with the Fraud Risk Assessment Standard.	Explain how the overall fraud measurement programme and annual plan of activities must be based on a documented high-level fraud risk assessment that covers the entire organisation and is updated at least annually. The input of senior management and the board must be considered in this process.	Demonstrate how the overall fraud measurement programme and annual plan of activities have been informed by a documented, and current, high-level fraud risk assessment that covers the entire organisation. There should be evidence of input from senior management and the board in this process.
4.2 Fraud Risk Assessment Skills- **Levels of Fraud Risk Assessment (High, Intermediate & Detailed)**	Identify the differences between the three different levels of fraud risk assessment - High (Board) - Intermediate - Detailed	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: - High (Board) - Intermediate - Detailed	Demonstrate the appropriate use of fraud risk assessments in the context of both fraud measurement planning and individual measurement activities at the three different levels: - High (Board) - Intermediate - Detailed
4.3 Fraud Risk Assessment Skills- **Use of a detailed fraud risk assessment**	Identify that a fraud loss measurement exercise needs to be informed by a detailed fraud risk assessment.	Explain how a detailed fraud risk assessment is used in the context of a fraud loss measurement exercise to identify areas of residual risk that may be resulting in undetected fraud or error.	Demonstrate the use of a detailed fraud risk assessment in the context of a fraud loss measurement exercise to identify priority areas of residual risk for testing that may be resulting in undetected fraud or error.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
4.4 Fraud Risk Assessment Skills- **Describing and recording fraud risks**	Identify the need for accurately describing and recording risks using the Actor, Action, & Outcome model or other similar structure in a fraud context.	Explain how in the context of a fraud measurement exercise to accurately describe and record fraud risks using the Actor, Action, & Outcome model or other similar structure in a fraud. Explain why it is important to identify each element in the context of fraud measurement testing.	Demonstrate the accurate description and recording of risks using the Actor, Action, & Outcome model or other similar structure in a fraud measurement context.
4.5 Fraud Risk Assessment Skills- **Identification of Controls**	Recognise the need to identify and record relevant prevention and detection controls to mitigate risk.	Explain how, in the context of a fraud measurement exercise, to identify and record relevant prevention and detection controls to mitigate risk.	Demonstrate, in the context of a fraud measurement exercise, the identification and recording of relevant prevention and detection controls to mitigate the fraud risk being assessed.
4.6 Fraud Risk Assessment Skills- **Evaluation of effectiveness of Controls**	Identify the need to effectively assess controls including their ability to detect instances of fraud and limitations that would still allow fraud to happen.	Explain how to assess the effectiveness of identified controls including their ability to prevent or detect instances of fraud and how to identify weaknesses and limitations that could still allow fraud to happen.	Demonstrate the ability to evaluate the effectiveness of controls including showing how they would prevent or detect instances of fraud in relation to a particular fraud risk. This should include a description of what the identified controls actually do to mitigate the fraud risk and what they don't do, in order to be able to understand the weaknesses and limitations that could still allow fraud to happen and what the resulting impact

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
			might be.
4.7 Fraud Risk Assessment Skills- **Assessment of Residual Risk**	Identify the need to assess, describe and prioritise residual risk in a fraud measurement context.	Explain the assessment, description and prioritisation of residual risk in the context of a fraud measurement exercise in order to understand how fraud can still happen with the identified controls in place and how this will direct and focus testing.	Demonstrate the assessment, description and prioritisation of residual risk in the context of a fraud measurement exercise to show how fraud could still happen with the identified controls in place and that this understanding has directed the design of the tests undertaken.
4.8 Fraud Risk Assessment Skills- **Using residual risk to target areas for testing.**	Identify the need for fraud loss testing to focus on finding fraud rather than testing the application of controls.	Explain why a fraud loss measurement exercise needs to focus on testing the extent to which the residual risk of fraud has resulted in fraud rather than testing the application of controls.	Demonstrate that fraud loss measurement exercises have focussed on finding fraud through testing to see if the residual risk of fraud has resulted in instances of fraud rather than testing the application of controls.

Competency 5: Statistical and Sampling Knowledge and Techniques

6 elements:

1.1 The purpose of sampling

1.2 Understanding a total population

1.3 Understanding sub-populations

1.4 Understanding confidence levels

1.5 Understanding precision and margins of error

1.6 Understanding different sampling methodologies

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
5.1 Statistical and Sampling Knowledge **– The purpose of Sampling**	Identify the role of statistical sampling in the context of testing and measuring for fraud and irregularity within a target area of spend / income.	Explain the rationale of sampling in the context of testing and measuring for fraud and error within a target population of spend / income.	Demonstrate that a practical application of sampling has been undertaken in the context of testing and measuring for fraud and error within the target population of spend / income.
5.2 Statistical and Sampling Knowledge **– understanding a total population**	Identify the importance of understanding the characteristics of the overall target population when selecting samples for testing.	Explain the importance of samples being representative of the overall population that you intend to test and measure.	Demonstrate that the characteristics of the target population have been identified and are understood, including its spread, geographic distribution, uniformity etc. And how this has been considered when selecting samples to ensure that they are representative of the overall population to be tested and measured.
5.3 Statistical and Sampling Knowledge **– understanding sub-populations**	Identify that total populations may be made up of discrete sub-populations that may each have different fraud risk characteristics.	Understand and explain the significance of sub-populations and the implications for measuring and estimating by focussing testing on one or more sub-population.	Demonstrate that sub-populations within the overall population being targeted for fraud testing and measurement have been identified and their respective fraud risks understood; but recognising the limitations this brings in relation to estimates of levels of fraud within the overall target population.
5.4 Statistical and Sampling Knowledge **– understanding confidence levels**	Identify that a sample size needs to be sufficiently large to provide confidence that any test results will be representative of	Explain what confidence levels are and how sample size affects this.	Demonstrate that the size of a sample for testing has been selected to represent the overall target population to a stated degree of confidence

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
	the target population being tested.		
5.5 Statistical and Sampling Knowledge **– understanding precision and margins of error**	Identify that where sampling is employed, the test results only provide an indication of the underlying rate of fraud and error within the target population and that the possible range for error should be recognised.	Explain what precision is, what this means in terms of a range of possible results, and how sample size affects this.	Demonstrate the possible range of the rate of fraud or error that has been determined from a test sample and how the chosen sample size affected the degree of precision, or margin of error, achieved over the scale of this range.
5.6 Statistical and Sampling Knowledge **– understanding different sampling methodologies**	Identify that sampling can take different forms and name the most common methodologies.	Explain the differences between different sampling methodologies; their strengths and limitations when applied to different testing scenarios.	Demonstrate that an appropriate sampling methodology has been chosen where a sample is selected to undertake a test for fraud.

Competency 6: Identifying and using evidence to test for fraud

7 elements:

1.1	Identifying internal data sets for the area being tested	1.5	Understanding requirements for obtaining test data
1.2	Identifying external data sets that can be used for testing	1.6	Designing individual tests
1.3	Developing terms of reference for a measurement exercise including objectives and scope	1.7	Designing working papers to provide an evidence trail
1.4	Scoping a test plan		

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
6.1 Identifying and using evidence to test for fraud – **identifying internal data sets for the area being tested**	Identify that each area to be measured for fraud will collect or generate data that could potentially be used for testing purposes.	Explain how to identify different data sets and information that can be used for comparative purposes and testing within the system / process being measured. Understand how shortcomings in the data can affect subsequent testing, measurement and estimating of fraud.	Demonstrate that all the data collected or generated by the system /process to be measured for levels of fraud is understood and has been captured /mapped to facilitate a full range of testing / measurement possibilities. Show that any limitations in the data that would affect the testing, measurement and estimation of fraud has been recognised and documented.
6.2 Identifying and using evidence to test for fraud – **identifying external data sets that can be used for testing**	Identify that successful testing for incidences of fraud or error is likely to be dependent upon the identification and use of data that is external to that held within the target system or process which can be used to compare and test against internal data.	Explain how to identify other sources of data that can be used for testing that are outside of the system / process being measured, whether internal or external to the organisation. Understand how shortcomings in the data can affect subsequent testing, measuring and estimating of fraud.	Demonstrate that a full range of data sources has been considered for testing purposes, including: data held elsewhere within the organisation; open source data; data held by other organisations and public bodies; and data generated by undertaking physical checking such as site visits. Show that any limitations in the data that would affect the testing, measurement and estimation of fraud has been recognised and documented.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
6.3 Identifying and using evidence to test for fraud – **developing terms of reference for a measurement exercise including objectives and scope**	Identify that it is important to be able to demonstrate the success of a measurement exercise through setting clear objectives and scope at the outset.	Explain how to scope the testing phase of a measurement exercise; developing terms of reference, including objectives and scope; and an outline of the specific fraud risks that will be tested to see if the identified residual risk has resulted in occurrences of fraud or error.	Demonstrate that for each measurement exercise that terms of reference have been developed that include the objectives and scope of the activity, including an outline of the specific fraud risks to be tested.
6.4 Identifying and using evidence to test for fraud – **Scoping a test plan**	Identify the need for testing for fraud and error to be planned and informed in advance through the development of a test plan.	Explain what a test plan for a fraud loss measurement exercise should include.	Demonstrate that a detailed test plan has been developed for each measurement exercise to be undertaken before testing takes place.
6.5 Identifying and using evidence to test for fraud – **understanding requirements for obtaining test data**	Identify that when data is obtained to enable testing for fraud and error that it is necessary to comply with data sharing and handling legislation; and that appropriate protocols and data sharing agreements are integral to achieving this.	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 that a plan has been developed to obtain all the data needed for testing which considers the legal requirements around data handling and sharing as well as outlining the protocols and agreements needed to enable data sharing between organisations.
6.6 Identifying and using evidence to test for fraud – **designing individual tests**	Identify that for tests for fraud and error to be successful it is necessary to design the tests in advance having identified appropriate test data or	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 that there is a clear rationale for each test carried out within a fraud loss measurement exercise, and that each test has been designed to find incidences of fraud or error, with the

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
	evidence to be used.		results likely to enable a conclusion to be drawn whether fraud or error has occurred.
6.7 Identifying and using evidence to test for fraud – **designing working papers to provide an evidence trail**	Identify the need for the approach and results of testing for fraud and error to be documented through well-designed working papers.	Explain how to design working papers to provide an evidence trail of the tests undertaken and results obtained in order to demonstrate the approach taken and consistency across the testing of each item sampled.	Demonstrate that appropriate working papers have been designed for each test to be undertaken which help provide a consistent approach to testing that can be documented.

Competency 7: Estimation and Measurement

9 elements:

1.1	Understanding the principles of fraud measurement	1.6	Validation and benchmarking
1.2	Being able to make a decision on whether irregularity has occurred	1.7	Understanding fraud risk drivers and their impact
1.3	Categorising test results	1.8	Calculating prevention savings
1.4	Applying results of fraud loss measurement	1.9	Measuring the effectiveness of the counter fraud strategy
1.5	Understanding the difference between detected, prevented and estimated fraud		

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
7.1 Estimation and Measurement – **understanding the principles of fraud loss measurement**.	Identify that levels of underlying fraud and error within a particular target population can be measured and estimated through undertaking a fraud loss measurement exercise.	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 Estimation and Measurement – **being able to make a decision on whether irregularity has occurred.**	Identify that the purpose of each test undertaken in a fraud loss measurement exercise is to enable a decision to be taken as to whether an incidence of fraud or error has occurred.	Explain how to decide for each item reviewed within a test sample as to whether; an irregularity (potentially fraud or error) has taken place; the item being reviewed is correct; or if additional testing is required to reach a decision.	Demonstrate how the results of testing have been reviewed in order to reach a conclusion as to whether fraud or error has occurred; or if additional testing is required to reach such a conclusion.
7.3 Estimation and Measurement – **categorising test results**	Identify that it is necessary to categorise test results in order to show by number and by value how many items within the sample found irregularity had occurred, and how many represented a correct item or transaction.	Explain how to categorise the results of testing to differentiate between irregularity (fraud or error); correct payments; or still unsolved	Demonstrate that the test results have been categorised to show, within the sample, how many items and their value: were correct (no fraud or error); fraud or error had occurred; or whether a firm conclusion could not be reached, and the possibility of irregularity remains unresolved.
7.4 Estimation and Measurement – **applying results of fraud loss measurement**	Identify that the purpose of fraud loss measurement testing is to be able to interpret and apply the results of actual	Explain how to apply the results obtained from testing for fraud and how these can be interpreted and extrapolated within the population	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

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
	measured irregularity from the test sample and use these to estimate levels of irregularity within the overall target population.	being reviewed.	the target population including the extent to which previously undetected losses exceed levels of irregularity currently reported.
7.5 Estimation and Measurement – **understanding the difference between detected, prevented and estimated fraud**	Identify different categories of measured fraud, including detected, prevented and estimated.	Explain the difference between detected fraud and error, prevented fraud and error, and estimated fraud and error.	Demonstrate the application of results arising from fraud measurement that distinguishes between and shows levels of detected, prevented and estimated fraud and error.
7.6 Estimation and Measurement - **validation and benchmarking**	Identify how benchmarking to other organisations can help to compare and validate levels of irregularity currently being detected, prevented or estimated.	Explain the benefits of comparison to other public sector organisations to validate findings and the levels of irregularity measured and estimated.	Demonstrate the use of benchmarking to other organisations in order to be able to gain insights through comparison as to the levels of irregularity currently being detected, prevented or estimated.
7.7 Estimation and Measurement – **understanding fraud risk drivers and their impact**	Identify that the likelihood of particular fraud risks can alter depending on the extent to which particular risk drivers are present, and that these changes can be measured and monitored.	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.	Demonstrate that drivers for fraud risks have been identified and understood, and that the extent to which these drivers are increasing, or decreasing, is being measured and monitored through use of fraud risk indicators.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
7.8 Estimation and Measurement – **calculating prevention savings**	Identify the importance of being able to quantify and measure the future impact of action taken to prevent fraud.	Explain the benefits of calculating ongoing savings through prevention and the need to use / develop a robust methodology for calculating these savings that is accepted across the public sector.	Demonstrate the calculation of ongoing savings arising from preventative action taken, using a methodology that is accepted across the public sector.
7.9 Estimation and Measurement – **measuring the effectiveness of the counter fraud strategy**	Identify that fraud measurement should also include measurement of the effectiveness of the organisational counter fraud strategy and related activities.	Explain how the effectiveness of counter fraud strategy needs to be measured; how bench marking can be used for comparison purposes; and overall performance targets can be set. Explain that the measures should cover all key activities across the counter fraud disciplines and not just those relating to measurement.	Demonstrate how the effectiveness of the organisational counter fraud strategy, and related activities, is measured and monitored, including: the use of performance and risk indicators; performance targets; and comparators such as bench marking.

Competency 8: Stakeholder engagement and reporting

12 elements:

1.1	Identifying and engaging key stakeholders	1.7	Reporting on previously unknown and undetected fraud losses.
1.2	Scope of fraud reporting	1.8	Getting stakeholder buy-in for fraud measurement and reporting
1.3	Rhythm for fraud reporting	1.9	Making links to organisational fraud risk appetite and tolerance
1.4	Developing supporting processes for fraud and error reporting	1.10	Aggregating results
1.5	Understanding the scope of fraud reporting	1.11	Understanding the limitations of fraud measurement and reporting
1.6	Setting reported fraud into the organisational context	1.12	Reporting on the performance of counter fraud activities

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
8.1 Stakeholder engagement and reporting – **identifying and engaging key stakeholders**	Identify that it is important for the results of fraud measurement and testing to be communicated to key stakeholders including associated governance structures at Board and Executive Committee levels.	Identify and explain who the key stakeholders are within the organisation for communicating results of fraud reporting and measurement.	Demonstrate that the results of fraud measurement and testing have been communicated to all key stakeholders, including where appropriate to the wider counter-fraud function.
8.2 Stakeholder engagement and reporting – **Scope of fraud reporting**	Identify the need for fraud measurement reporting to provide a comprehensive assessment of the overall level of fraud through comparing details of fraud detected or prevented with additional estimates of undetected fraud derived from measurement testing.	Explain that the scope of fraud measurement reporting requirements needs to cover both: ongoing discoveries of prevented / detected fraud and error through the operation of controls; and the measurement of fraud and error occurring either as a result of control failure or resulting from the limitations of any controls in place (residual risk).	Demonstrate how the scope of fraud measurement reporting covers both: ongoing discoveries of prevented / detected fraud and error through the operation of controls; and the measurement of fraud and error occurring either as a result of control failure or resulting from the limitations of existing controls in place (residual risk).
8.3 Stakeholder engagement and reporting – **Rhythm for fraud reporting**	Identify that a characteristic of effective reporting is the establishment of a regular reporting rhythm.	Explain how to develop a regular rhythm of fraud and error reporting.	Demonstrate that a regular rhythm of fraud and error reporting has been established and is being followed.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
8.4 Stakeholder engagement and reporting – **Developing supporting processes for fraud and error reporting**	Identify the need for all areas of an organisation to contribute to the regular reporting of fraud and error.	Explain how to ensure that the regular reporting of fraud and error prevented / detected through existing controls is supported by reporting processes that cover all key areas of spend / income / fraud risk within the organisation.	Demonstrate that the regular reporting of fraud and error prevented / detected through existing controls covers all key areas of spend / income / fraud risk within the organisation.
8.5 Stakeholder engagement and reporting – **Understanding the scope of fraud reporting**	Identify that the main categories of fraud reporting covers: detected fraud; prevented fraud; ongoing savings; recoveries of losses.	Explain the scope for the regular reporting of fraud and error that is prevented / detected through existing controls needs to cover: Detected after payment; Prevented before payment; Ongoing prevented savings; Recoveries of detected fraud.	Demonstrate that the scope for the regular reporting of fraud and error that is prevented / detected through existing controls covers: Detected after payment; Prevented before payment; Ongoing prevented savings; Recoveries of detected fraud.
8.6 Stakeholder engagement and reporting – **setting reported fraud into organisational context**	Identify the importance of using context when reporting fraud and error to give the reader an idea of the scale of the findings.	Explain the need to help stakeholders understand the organisation's vulnerabilities to fraud. This includes putting reported incidences (including results of testing) of fraud and error detection / prevention into context, such as a percentage of spend / income; activity levels (numbers of transactions) for all areas of key	Demonstrate the use contextualisation within fraud measurement reports, including: the percentage of fraud or error compared to spend / income; the incidence of fraud compared to activity levels (numbers of transactions) to enable stakeholders understand the organisation's vulnerabilities to fraud.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
		fraud risks.	
8.7 Stakeholder engagement and reporting – **reporting on previously unknown and undetected fraud losses.**	Identify the need for fraud loss measurement to provide an assessment between existing levels of detected fraud and an estimate of undetected fraud.	Explain the need to have a programme to test for, measure, and report levels of fraud and error beyond what is covered by regular reporting of detected fraud in order to provide estimates and assurance in relation to the level of undetected fraud and error.	Demonstrate the establishment and use of an ongoing programme of fraud loss measurement which is used to estimate levels of undetected fraud and error.
8.8 Stakeholder engagement and reporting – **getting stakeholder buy-in for fraud measurement and reporting.**	Identify the importance of getting stakeholder buy-in for a programme of fraud measurement and reporting.	Explain the need to obtain stakeholder buy-in for the measurement programme to provide the organisation with ongoing assurance about the levels of fraud and error the organisation has exposure to; and the extent to which undetected fraud or error has materialised.	Demonstrate that buy-in has been obtained from a range of stakeholders for an ongoing programme of fraud measurement that will provide the organisation with ongoing assurance about the levels of fraud and error the organisation has exposure to; and the extent to which undetected fraud or error has materialised.
8.9 Stakeholder engagement and reporting – **making links to organisational fraud risk appetite and tolerance.**	Identify the need when reporting results of fraud measurement to put these into context with stated fraud risk tolerances and risk appetite.	Explain how to link the results from the fraud measurement programme to an organisation's risk appetite and tolerance, including assessing the cost-effectiveness of new controls	Demonstrate when reporting the results of fraud measurement that reference is made to the organisation's risk appetite and accepted tolerances. This should enable evidence-based decision making about

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
		introduced since an area was last measured.	the response to the levels of fraud and error found and the extent to which additional actions or controls are cost effective.
8.10 Stakeholder engagement and reporting – **aggregating results**	Identify the need to aggregate the results of all the activities within each annual plan of the organisational fraud measurement programme to provide an overview of both detected cases and estimated levels of fraud.	Explain the need to aggregate on at least an annual basis all the results from the various activities relating to fraud reporting, measurement and estimating to provide the organisation with a view on levels of irregularity and how this compares with previous reporting periods.	Demonstrate the aggregation and reporting of the results from all fraud reporting, measurement and estimating activities on at least an annual basis, with comparisons made to previous reporting periods.
8.11 Stakeholder engagement and reporting **– understanding the limitations of fraud measurement and reporting**	Identify that the scope of fraud reporting or measurement processes will have limitations and that and that it is important to acknowledge what these are and what unmeasured areas represent.	Explain that there will be limitations with reported and estimated levels of fraud, including fraud risks that have not been measured or areas that are unmeasurable.	Demonstrate and acknowledge the limitations of fraud reporting, including recognition of unmeasured fraud risks and that there will be some elements of the organisation's "Iceberg" that may be unmeasurable.
8.12 Stakeholder engagement and reporting **– reporting on the performance of counter fraud activities**	Identify the need to measure and report regularly on the effectiveness of the counter fraud strategy and related activities.	Explain the need to report regularly, and at least annually, on the effectiveness of the counter fraud strategy and the performance of related activities.	Demonstrate that the effectiveness of the counter fraud strategy is measured and monitored and that the results are reported regularly, at least annually.

D. Guidance on Processes

D1. Introduction

This guidance covers the processes for the Fraud Measurement discipline.

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 measure 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 scope of the Fraud Measurement discipline requires those within the discipline to:

- understand organisational vulnerabilities to fraud by identifying key areas of risk for fraud;
- understand and be able to carry out fraud risk assessments accurately;
- establish reporting processes to collect data on instances of fraud and error found through business systems and controls;
- run fraud testing exercises to measure and estimate levels of undetected fraud and error;
- calculate prevented savings where new controls have been put in place; establish actual levels of fraud and error loss compared to sums recovered, and;
- report and communicate their findings and assessments to senior managers and key stakeholders.

The creation of fraud measurement processes and standard operating procedures should be considered to achieve the objectives for fraud measurement outlined above. 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.

Those working in Fraud Measurement should have a working knowledge of relevant legislation and policy and understand how it impacts upon their role, including:

- Fraud Act 2006
- Digital Economy Act 2017
- General Data Protection Regulation
- Annex 4.9 of Managing Public Money

D2. Process for capturing and reporting detected loss and prevented loss due to fraud

It is important that those within the Fraud Measurement discipline are able to communicate to others in their organisation on the levels of fraud and error experienced; and what losses have resulted and the extent to which these have been written-off as unrecoverable.

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. Additional testing to find undetected fraud; either through testing to see if existing risk exposures have been exploited by fraudsters, or by testing vulnerabilities in the operation of key counter-fraud controls, and measuring associated losses will help develop an understanding of the levels of fraud and error that are currently undetected.

It is important that a reporting process exists that connects all business units with those responsible for measuring and reporting fraud and that a regular rhythm (at least quarterly) of reporting is established.

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 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 Counter Fraud Centre of Expertise to collate reported fraud across central government (see Annex A). Accompanying this should be a brief narrative to describe each fraud and how it happened.

D3. Identifying areas vulnerable to fraud and selecting areas for measurement

This process requires participants to identify areas of spend / income that are likely to present significant fraud risks. They should use either their organisation's high-level or intermediate-level Fraud Risk Assessment (FRA) or their own analysis to identify areas where fraud is most likely to be found and where measurement exercises will add the most assurance value by looking for, and measuring, instances of undetected fraud.

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 high-level FRA. It is important to recognise any significant areas of spend / income which are not represented on the high-level FRA and to flag these as potential gaps in the FRA.

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

Measurement exercises may be undertaken either: (i) in an area where fraud is already being found, but assurance is required to determine if there is additional, undetected, fraud; or (ii) in areas where little or no fraud is currently being reported in order to measure and estimate actual levels of underlying fraud.

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.

In the absence of a high-level fraud risk assessment then a Spend Area Assessment can be undertaken to prioritise areas for measurement activity. To create a Spend Area Assessment requires participants to identify key areas of spend / income and then to apply a basic risk assessment against each area in order to identify areas likely to be vulnerable to the risk of fraud, where testing is most likely to find fraud and therefore where a fraud loss measurement exercise would add the most assurance value.

The participant should score each area against four risks. An example scoring template is shown below which uses four key risk factors:

- **Annual gross financial risk** – the materiality of each area
- **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.
- **Control/residual risk** – the extent to which there is assurance that the controls within a particular area are well-designed and operating as intended.

Example scoring template for assessing areas of spend in relation to fraud risks:

Risk factor	Score	Narrative justification for scores
Annual gross financial risk **(G)**	**1** = <£10m **2** = £10-100m **5** = >£100m	
Reputational risk **(H)**	**1** = Scheme is not high profile and has received limited media coverage **2** = Scheme has attracted significant recent media attention	
Inherent risk **(I)**	**1** = Spend area regularly reports levels of fraud and error via the Consolidated Data Request (CDR) above 0.5% of annual spend. **2** = Spend has occasional reports of fraud & error occurring which in value are less than 0.5% of annual spend. **3** = Spend has a detection and reporting process but no reports of fraud and error occurring. **4** = It is not known whether a detection and reporting process is in place for fraud and error.	
Control / residual risk **(C)**	**1** = Controls are well designed, operating and there is little or no residual risk **2** = Controls are generally well-designed and operating, but a small amount of residual risk remains **3** = Controls do not cover all the fraud and error risk, and significant residual risk remains post-operation **6** = It is not known how well-designed or operationally effective the controls are.	

Risk factor	Score	Narrative justification for scores
Total risk score:	Annual Gross = **G** Reputational Risk = **H** Inherent Risk = **I** Control/Residual Risk = **C** **(G+H) x (I+C) = Area Risk Rating** **=**_____	

An “area” selected for measurement activity can cover any process by which a department pays out expenditure or receives income. This could be payments directly to the public, or to third party contractors that provide services to the public. They also include payments to public sector employees to provide services. Examples of expenditure include grants schemes, contracted procurements, or means-tested services; whereas income includes fees, levies and charges.

The areas selected should be ones 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.

Consideration should be given to the financial size of the area, the inherent risk (i.e. 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.

Indicators of good quality	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). · Critically 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 high-level 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: · Statements that the spend area is high risk but without reasoning or justification for this, or; · reasoning that does not 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 organisational fraud risk assessments.

D4. Carrying out a detailed Fraud Risk Assessment

A detailed Fraud Risk Assessment (FRA) is key for understanding how fraud could happen within the target area for which fraud measurement and assurance is required. Understanding how fraud can occur – the fraud risks – helps identify particular fraud risk exposures that might have been exploited by a fraudster. Testing of those exposures will build understanding and measurement of levels of underlying and previously undetected fraud.

The process for producing the detailed FRA is the same as is outlined in the GCFP Standard for Fraud Risk Assessment, but for Measurement there are additional steps to consider how identified risks can be tested to see if fraud has occurred and the evidence available to enable this to happen.

There are six stages to follow in the process to produce a FRA which supports fraud testing and measurement:

Stage 1: Identify fraud risks

- View the target spend area through three different perspectives to help provide a comprehensive list of risks how fraud could arise in relation to:
  - The eligibility criteria for making a payment, receiving an income,
  - All the Individuals involved – both internally and externally,
  - Each step of the process from end to end.

- This identification process 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.

- The process should also be collaborative: work with 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.

Stage 2: Define fraud risks

- Risk definition is a crucial part of writing a good quality detailed FRA. A detailed FRA requires descriptions of identified risks to be very specific about how individual instances of fraud could occur, rather than a generalised statement about fraud happening.
- The more specific the risk is, the easier it is to identify associated controls, the residual risk, and how specifically testing could show if that risk had occurred.
- A good written risk definition will describe who might commit the fraud (the actor); how they commit the fraud (the action) and what the consequences might be (outcome). Outcome should consider all relevant factors, such as social impacts, reputational impacts etc and not just financial impacts.

Indicators of good quality	Indicators of poor quality
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.

Stage 3: Identify controls

- Here, control refers to any action that could mitigate against a specific fraud risk either through prevention or detection activities.
- Ensure that how each control works in relation to the fraud risk is thoroughly and

clearly explained.
- Be sure to identify how the control affects or could affect the fraud risk.

Indicators of good quality	Indicators of poor quality
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	

Stage 4: Identify residual risk

- Residual risk refers to 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.
- Describe the residual risk specifically and in detail. This will help identify evidence that could be used for testing to indicate whether the fraud is occurring.

Indicators of good quality	Indicators of poor quality
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	

Stage 5: Categorise the internal and external evidence or comparator data available for testing

Once the fraud and error risks have been analysed, 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 the availability, completeness and quality of it.

Evidence or comparator data can be categorised into three types:

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

It is also important to consider the quality of the evidence – its accuracy, age, reliability etc, and how it is compiled and stored – to understand the limitations this may have when undertaking testing. Once evidence has been identified a department must evaluate it for 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 also consider the quality of the evidence. 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.

Identification of evidence or comparator data available for testing:

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

Stage 6: Select risk to test

Ensure that all fraud risks in relation to the target area being reviewed have been identified and captured. Once all of the fraud risks have been identified and the associated controls, residual risk and potential evidence 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 achievable and workable based on the type of testing proposed and the resource available. The fraud measurement practitioner must document why a fraud risk has been selected for testing.

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.

Indicators of good quality	Indicators of poor quality
Use a comprehensive 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	Too many or too few risks have been chosen for testing and it is not clear how

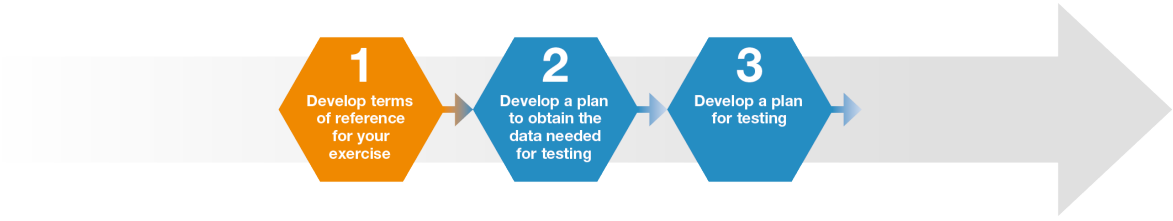
Indicators of good quality	Indicators of poor quality
is clear what evidence can be used for testing.	they will be tested for fraud
Evidence chosen for testing is likely to allow conclusions to be drawn about whether fraud or error has taken place	It is not clear how the evidence will be used to identify if fraud or error has taken place

D5. Planning and undertaking testing to find fraud and error

Before testing for fraud and error is undertaken within a fraud measurement exercise it is necessary to plan the tests carefully to ensure that they will be effective and find fraud if it is present. Following the identification of areas of high fraud risk a decision will need to be taken about whether the cost of conducting a bespoke fraud measurement exercise is justified.

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

Stage 1: Develop terms of reference for your exercise.



These should cover the scope of the exercise, the resource requirements, and have a clear objective to find and measure fraud.

- The resourcing and the amount of time it is likely to take to collect data and undertake testing. If undertaking a data sharing activity it can often take a number of weeks or even months to receive approval by both parties
- Secure an appropriate Senior Responsible Officer for the exercise who will secure the necessary resources, review progress, and sign off on decisions.

Stage 2: Develop a plan to obtain the data needed for testing.

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

- Internal data held within the scheme or process being tested
- Internal data held elsewhere within the organisation
- Data that can be self-generated through analysis or through an inspection or site visit.
- Open source data
- External data held by other public sector bodies. For this there will be a need to arrange a data share agreement with the third-party organisation. The GCFP Data Analytics Standard should be a point of reference for further details, but key steps to consider are:
  - Firstly, identify the source for data sharing.
  - Secondly, refer to the detailed fraud risk assessment to help identify the intended use of data.
  - Thirdly, contact the Departmental Data Protection Officer for help in completing a Data Protection Impact Assessment (DPIA).
  - Use steps 1 and 2 to implement a Data Sharing Agreement
  - Make use of the Digital Economy Act, which provides a legal basis for data sharing.

Stage 3: Develop a test plan:

The test plan should scope and document the following:

- Each fraud risk to be tested.
- Consideration of how the population of spend or income that is being tested 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 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 irregular (fraud or error).

Testing will be unique to each exercise, so this standard does not describe this element of the process in detail. However, it will almost always be a case of taking each sampling unit and assessing it against processing criteria, controls and evidence and determining whether:

(i) the payment or transaction item is correct and valid; or
(ii) whether irregularity (i.e. fraud or error) has occurred. It can be beneficial to start with the premise that every unit in the sample is irregular and seek to find sufficient proof that they can be validated as regular, and if not must continue to be considered as potentially irregular with additional testing required. If no further tests can be identified the sample item should be classified as 'unresolved'.

It is important to note that a fraud measurement exercise is not primarily a control checking exercise. An opinion on whether the controls in place are working as intended is not the desired result here, as these exercises are intended to produce an estimation of the financial loss to fraud and error due to the identified residual risks in the area being measured.

However, it can be beneficial to run in parallel a separate measurement exercise to test and measure fraud losses due to vulnerabilities and failures in the way that counter fraud controls are operated. Combining both types of measurement exercise enables the organisation to be informed of both losses due to gaps and weaknesses in the design of controls as well as those arising from the failure to operate those controls correctly.

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 include:

- Training of staff undertaking measurement activities;

- Providing written guidance;
- The use, and design of, working papers which outline the tests to be performed and provide contextual information about expectations for how they will be performed;
- Supervision and quality assurance reviews.

Indicators of good quality	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 irregularity.	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 majority of risks previously selected to be tested, with reasonable justification as to why other risks selected were not tested.	Testing covers less than half of the risks previously selected for testing, and it is unclear why the remaining risks were not tested.

D6. Choosing statistically valid samples for testing

When testing for instances of fraud the ideal would be to test the whole population. On occasions this is possible using data matching across the entire population. However, usually this is impractical or too resource intensive. The solution is to use statistical

sampling. The key principle with statistical sampling is to ensure that any results from testing a sample can be 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 should:

- Include some degree of randomisation
- Involve a 'Probability' sample where any unit within the population has a known, non-zero, chance of being chosen.
- Be supported by clear and evidenced justification

Non-probability sampling is not an acceptable sampling method. That type of sampling might be something like convenience sampling—e.g., choosing a sample based on units that are nearest or most accessible. A sample taken in this way is based on subjective judgment, whether based on what the tester thinks a typical sample would look like, or selecting sampling units which are the ones easiest to obtain or test.

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:

- If the sampling frame is large then random sampling may be impractical

- A complete list of the population may not be available
- Minority 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 sample

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

The choice and selection of strata is based on a belief/evidence that the characteristics of each sub-population could result in differing levels of fraud or error and use of this technique requires knowledge of the population composition. A fraud measurement practitioner could, for example, stratify payments by value, by geographical location or by 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. What this means is that while individual cases are still randomly sampled, more will be selected from high risk strata and fewer from low risk strata. However, care needs to ensure that test results are interpreted for each stratum first before aggregating to reflect the overall population.

Advantages:

- Strata can be proportionally represented in the final sample

- It is easy to compare subgroups
- Can be used to target subpopulations 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 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 / 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

- Monetary Unit Sampling 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 data is divided into clusters and random sampling is used to select a sample of whole clusters to test from all the clusters.

The sample will be obtained from a collection of entire cluster groups. It is usually used with naturally occurring groups of individuals.

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

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 ±2% will mean that the 'true' rate of fraud within the parent population is expected to be within the range of 3% - 7%.

Determining the desired confidence level and margin for error

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

To determine the sample size for a given confidence level it is necessary to know or estimate the level of irregularity 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 attribute of irregularity). In these instances, it is recommended that a sample size corresponding to a 5% estimated rate of irregularity 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) gives an idea of different sample sizes required.

90% Confidence Level

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

95% Confidence Level

Estimated Irregularity \ Precision ±	8%	6%	5%	4%	3%	2%	1%
8%	44	79	113	177	314	707	2827
6%	34	60	87	135	241	542	2167
5%	29	51	73	114	203	456	1825
4%	23	41	59	92	164	369	1475
3%	17	31	45	70	124	279	1118
2%	12	21	30	47	84	188	753
1%	6	11	15	24	42	95	380

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.

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

Indicators of good quality	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 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,	Unclear or no explanation of how the sample chosen reflects the overall

Indicators of good quality	Indicators of poor quality
including any exclusions and the reasons for exclusion.	population.
If the sample includes different categories (for example low/high risk, or low/medium/high value), then the process for deciding on these categories is explained, and the impact on how this affects 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), then the process for deciding on these categories is not clearly explained, and the impact on how this affects 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.

D7. Identifying and selecting evidence / test data

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

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

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

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.

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 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.

The next stage is to consider the availability of each possible data source; who owns it and what steps would be necessary to obtain the data. This includes the need to consider data sharing agreements and use of legislation such as the Digital Economy Act to obtain the data. Consideration should be given to the data products available that could be used to validate whether fraud or error has occurred, such as those available through Open Source Intelligence Tools. Also consider the National Fraud Initiative (NFI) run from Cabinet Office, which offers a web-based application called App Check that can provide data instantly from 1,300 organisations including Home Office Immigration data, Met Police ID fraud data, and a variety of public sector datasets.

Subsequently, it is necessary to evaluate the format and quality of the data to be used as evidence and how this could affect the quality and results of testing. This includes ascertaining the data fields available, the reliability of the collection method, how recent and up to date the data is, how accurate it is likely to be, and how complete. 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

Indicators of good quality	Indicators of poor quality
Available evidence is clearly explained, including how it could be used to test for fraud	Evidence is not clearly explained, or does not describe how it could be used to test for fraud
A wide range of external evidence has been considered and obtained for testing	Only internal evidence (already held as used as part in the decision or at

– evidence held within the organisation but not used in the decision or at payment, as well as evidence held by external organisations	payment) has been considered.

D8. Estimating and measuring levels of fraud and fraud losses

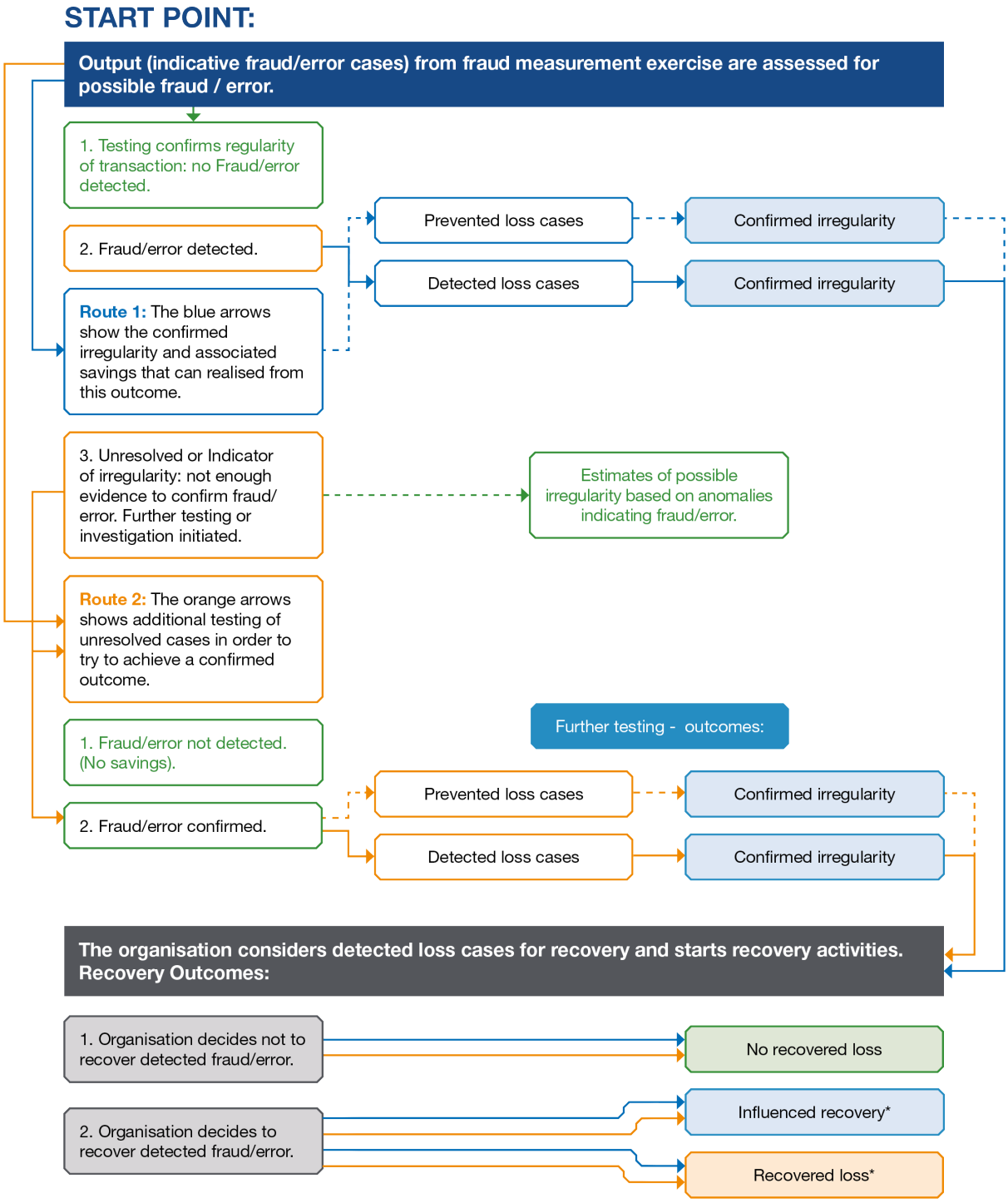
Once testing for fraud and error has been completed it is necessary to interpret the results.

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

- Fraud
- Error
- Irregularity
- Indicators of irregularity
- Unresolved cases
- Regular transactions

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 E3 of this Standard.

The following flow chart presents the methodology for making decisions on whether detected fraud / error has been established or whether additional testing or investigation is required in order to reach a decision:



Measure Type

Evaluated saving | Potential saving

* Depending on the size of the measurement exercise and time frame for reporting, it might not be possible to a) track cases sent for recovery and derive recovered amounts or b) for the organisation (where they cannot provide evaluated evidence) to provide assumptions on the amount they expect to recover, so Influenced Recovery and Recovery Loss Savings are not always possible to measure.

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 ±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.

The **third step** is to calculate what this means in terms of the value of the population as a whole, and also the number of transactions or items within that population. For example, if the monetary value of the population was £1m, and it involved 10,000 transactions then it can be estimated that the rate of monetary 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.

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 such as Stratified sampling to ensure that the estimated results accurately reflect the population. In this case 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.

D9. Methodology to follow for calculating prevented savings

Types of savings generated from findings of detected fraud / error from fraud measurement exercises

There are three types of savings generated from fraud / error cases detected as a result of fraud 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.

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: Where it is not possible to derive the amount recovered it is possible to use the value of the fraud / error detected as lost as a proxy value of the potential amount that could be recovered.

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. The following three measures have decreasing levels of certainty attached to them:

1 Evaluated Measure: Evaluated 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 Calculated measure: Calculated savings are 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.

3 Potential measure: Potential savings show the value of the fraud/error for the Detected loss cases. The value of the fraud/error is not an evaluated saving as, although the value has been detected and evidenced, recovery has not yet happened. Recovery can be a lengthy, expensive process. Organisations may consider the net benefit of doing so, and therefore may not always choose to pursue recovery. Alternatively, it may not always be possible to recover the full amount in each case where recovery is attempted.

Identifying and calculating Preventative savings

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

1 Point of interdiction: this saving is from loss prevented at the point where fraud/ error has been detected. As a result, the payment scheduled to be processed has now been stopped from being processed. The value of the prevented payment can be evidenced with certainty and attributed to the measurement exercise as an **evaluated measure**.

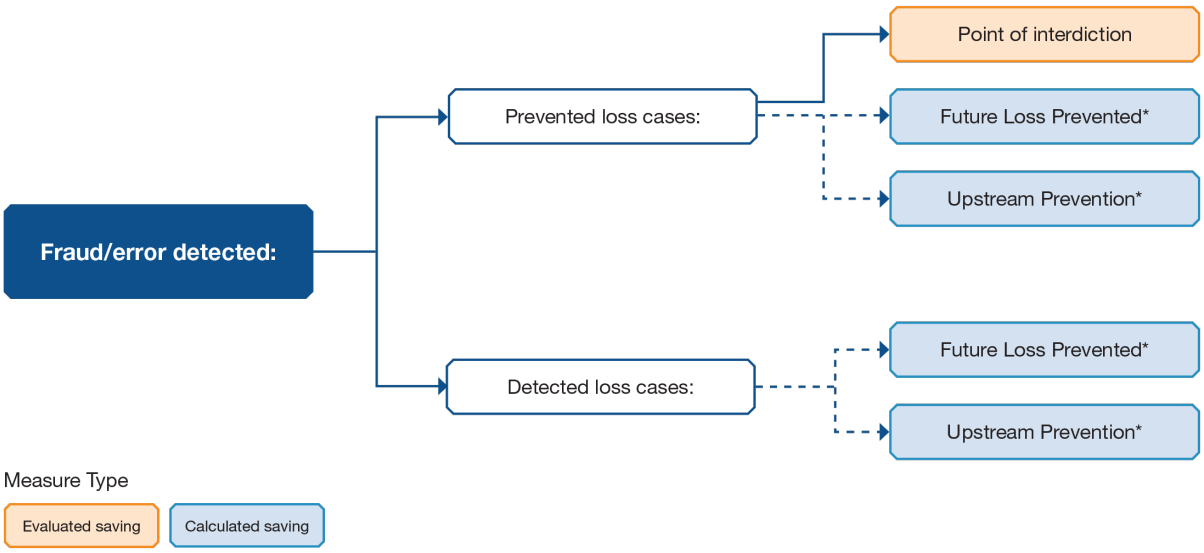
2 Future Loss Prevented: 'Future Loss Prevented' can be generated from both Prevented loss cases and Detected loss cases. These savings occur where it can be evidenced that, had the fraud/error not been detected by the measurement activity or exercise then it would have been more probable than not that the fraud/error would have continued for a period of time 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 **calculated 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 **calculated measure**.

Preventative savings: measures by case type and savings type

This diagram summarises the different Preventative savings measures that can be generated from prevented loss cases and detected loss cases:

Preventative savings: measures by case type and measure type



* Savings measure not always applicable or possible to measure, denoted by the dashed lines.

Agreeing a methodology for calculating prevented savings

It is important that the methodology used to calculate prevented savings is sufficiently robust to stand up to scrutiny and is consistent with similar methodologies employed across government. The Counter Fraud Centre of Expertise 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. The methodology provided at section E4 has been approved by the Prevention Panel.

D10. Reporting on fraud testing and estimation.

The results from fraud 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.

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.

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

Indicators of good quality	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 for 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 / 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

E: Guidance on Products

E1. Introduction

All central government departments should report identified loss from fraud, bribery, corruption and error, alongside associated recoveries and prevented losses, to the counter fraud centre of expertise in line with the agreed government definitions. In addition, they should also undertake activity to try and detect fraud in high-risk areas where little or nothing is known of fraud, bribery and corruption levels. This activity should include using loss measurement activity to find and estimate previously undetected fraud or error.[2]

This document sets out the expected minimum standards for concepts to be applied and tools and techniques to be utilised as part of a programme of testing, measuring and reporting instances of, and losses arising from, fraud and error.

For simplicity, we have referred to these tools and techniques as **products**. This section covers the requirements of organisational reporting of prevented and detected fraud, and the tools and techniques needed to undertake fraud loss measurement exercises in order to estimate undetected losses.

E2. Fraud reporting - details of requirements to include in the reporting of fraud and error found through the operation of existing controls

Testing within a fraud measurement exercise may easily establish that an individual transaction or payment should not have been made and therefore is irregular. However, for an action to be defined as fraudulent there needs to be evidence of a degree of dishonesty such that the false representation, omission of facts or abuse of position is made knowingly and with the intention of gaining at the expense of the organisation.

However, to prove fraud to a criminal standard there has to be a high degree of proof, such that an act or omission is proved 'beyond a reasonable doubt'.

It is recognised that few instances of fraud will be proved to a criminal standard, unless a criminal sanction is to be applied. Therefore, it is advised that for the recording of fraud a pragmatic approach, using the civil burden of proof, is followed by organisations. Cases should therefore be recorded as fraud where the organisation judges that the misrepresentation, omission or abuse of position has been made fraudulently on the

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/894811/Counter_Fraud_Functional_Standard.pdf

balance of probabilities. This means that instances of irregularity should be recorded and reported as fraud as soon as there is prima facie evidence that there is dishonesty involved and organisations will need to make a judgment that the action or inaction was more likely than not to have been made to defraud. Consequently, the reporting of cases of irregularity as fraud should not be reliant upon a prosecution being taken, which might not happen in minor cases of dishonesty or else take months or years to progress.

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, as defined in this document

The point at which fraud should be referenced is the point at which the fraud/error 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.

For the purpose of reporting, cases of irregularity are broken down into the following categories:

- Detected Fraud
- Prevented Fraud
- Error
- Recovery of losses

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 following:

- 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 even where some investigation actions may be outstanding, provided the organisation has reached a decision in the reporting period that there is a prima facie case of 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.

Costs associated with investigating a case must not be included within a detected fraud loss figure.

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 or 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.

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.

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.

Recoveries

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.

E3. Detailed fraud risk assessments of targeted areas

A detailed fraud risk assessment of each specific area that is being targeted for fraud testing and measurement should use a template that contains the following elements in line with the process guidance provided in section D4:

Description and Assessment of Fraud Risk
For each specific fraud risk identified, this should identify the 'Actor' – who will commit the fraud (may be a single individual or one or more individuals) Describe the 'Action' – what the fraud is and how committed Describe the 'Outcome' – what are the resulting consequences, including social, physical or reputational harm, as well as financial impact.
Description and Assessment of Controls
For each specific fraud risk identified, this section should identify and describe each control that is considered to mitigate the fraud risk. The nature of each control identified and the type of action it provides – directive, preventative, detective, etc.

A description of what each control actually does to mitigate the fraud risk A description of the limitations of each control – what they don't do to mitigate the fraud risk
Description and Assessment of Residual Risk
Residual risk should be a description of how fraud could still happen despite the controls in place. It uses the limitations of the controls that have been identified and uses these to explore how they could allow a fraud to happen or be exploited by a fraudster to commit fraud in a way that gets around the controls.
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.

E4. 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 it is expected that the report of a single fraud measurement exercise should contain the following sections:

- An introduction to explain the spend area tested.
- The sample methodology employed and sample size.
- The approach taken to testing.
- The results from testing, and the amount of fraud / error found within the sample.

- Actions and recommendations around controls and future measurement in that specific area.
- Conclusions about estimated levels of fraud / error within the wider population.

Where an organisation judges that it has a fraud risk but that a fraud measurement exercise is not justified it could (in certain circumstances) be acceptable to extrapolate and report from an exercise performed on a similar profile of expenditure 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:

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

Definitions of reporting categories

Fraud

The key element for identifying fraud is intent. Where there is, on balance of probability, 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 a balance of probabilities that there was no intent to defraud, then this should be classified as ‘error’.

Indication of irregularity

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 then this should be recorded as an ‘indicator of irregularity’.

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.

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 measurement exercises may tend to report more error, as often a full fraud investigation (see the GCFP Investigation Standard) would be required to prove the necessary intent to term the loss a fraud, which will not be with the scope of a sampling exercise aimed at measuring losses.

Reporting findings from fraud measurement exercises

The following is an example template to be used for reporting these categories of findings:

Fraud risk tested	Sample size		Transaction verified as correct		Fraud		Error		Indicator of irregularity		Unresolved	
	No. of Cases	Value £	No. of Cases	Value £	No. of Cases	Value £	No. of Cases	Value £	No. of Cases	Value £	No. of Cases	Value £
FR 1												
FR 2												
FR 3												
FR 4												
FR 5												
TOTALS :												

Estimating and interpreting results in relation to the overall population from which the sample was drawn

The actual findings found 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, and using this 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.

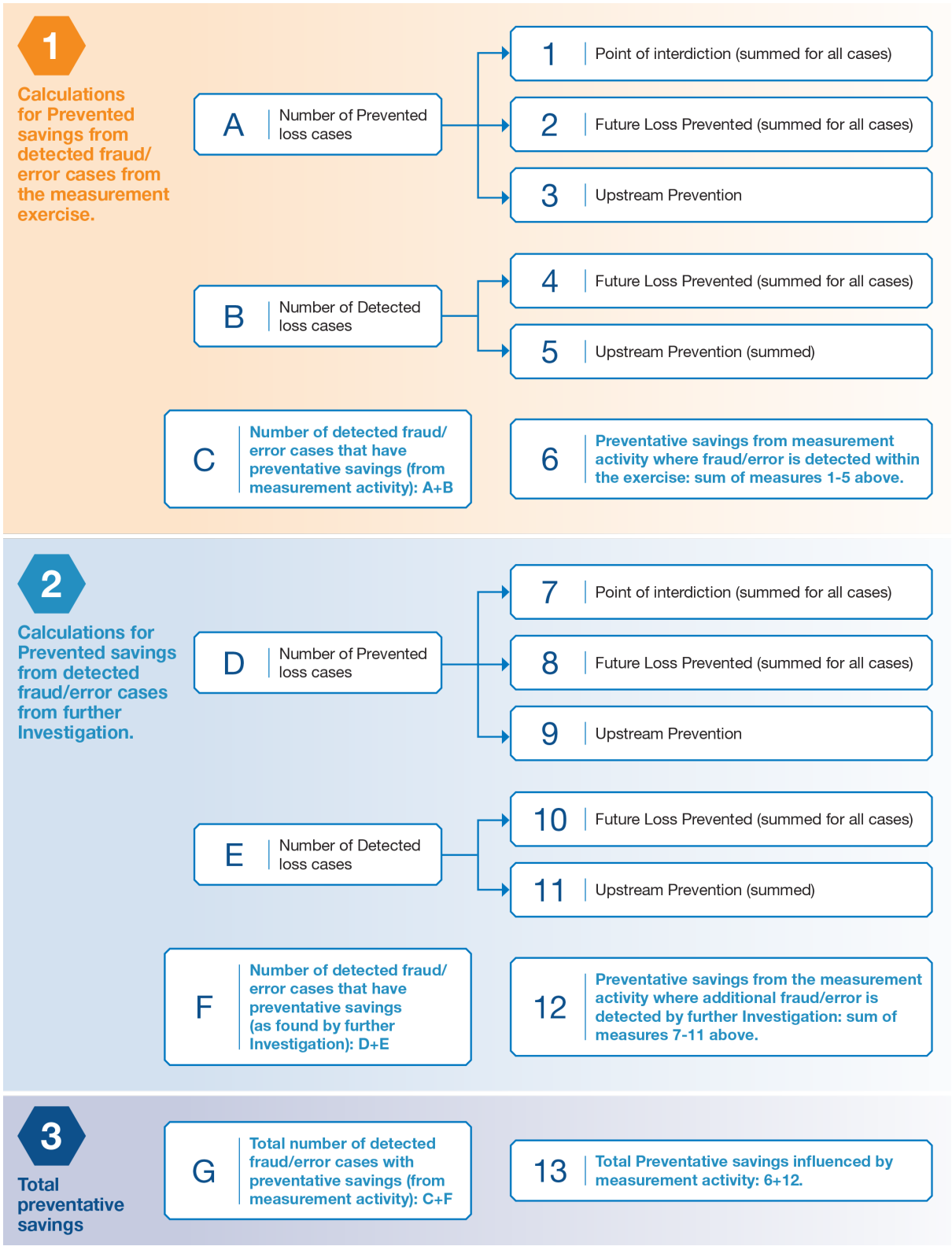
The following is an example template to be used for reporting the estimates of these ranges:

Fraud risk tested	Sample: Calculated precision rate and confidence levels		Transaction verified as correct		Irregularity: Fraud and Error		Indicator of irregularity		Unresolved	
	Precision	Confidence Level	Range of cases	Range of values £	Range of cases	Range of values £	Range of cases	Range of values £	Range of cases	Range of values £
FR 1										
FR 2										
FR 3										
FR 4										
FR 5										
TOTALS:										

E5. Calculation of savings generated through a fraud measurement exercise including future (prevented) savings resulting from improved controls or the introduction of new controls and processes

Template for calculating Preventative savings influenced by the measurement activity.

Reference should be made to the process guidance for calculating savings provided at D9.



F. Guidance on Organisation

F1. Introduction

Fraud is the most common crime in the UK today, and the activities of every government organisation will leave it exposed to a variety of fraud risks. Executive Boards in every organisation should plan to measure or estimate the extent to which fraud is impacting the organisation. 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.

Fraud is one of the risks that all organisations dealing with money face. Fraud can be the result of internal and external threats, or a combination of the two. Fraud can be perpetrated by individuals or groups of individuals. Additionally, it can be the result of bribery or corruption and can be defined as serious and organised crime in some circumstances. Fraud can also be related to, or be an enabler of, broader crimes.

In the same way that organisations should demonstrate that they are managing risks within their programmes, projects and operations, an organisation should consider how it measures the success of its counter fraud strategy and 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.

The accountable individual at board level **must** be able to determine not only the amount of fraud and error prevented, detected and recovered, but also estimate the possible losses arising from the organisation's residual fraud risk exposures.

Fraud measurement therefore lies at the heart of an effective counter fraud response. HM Treasury in their publication 'Managing Public Money'[3] advises that effective management of the risk of fraud includes 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.

---

3 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835558/Managing_Public_Money__MPM__with_annexes_2019.pdf

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.

These standards outline what a public sector organisation is expected to have in place to enable an effective programme of testing, measurement and reporting of fraud and error, which will inform and enable the organisation to manage fraud risk.

F2. Mapping and understanding assurance requirements in relation to fraud risks to quantify associated fraud risk exposures and resulting losses

It is essential that an organisation is able to map and understand the fraud and error risks it faces through producing high and intermediate fraud risk assessments as prescribed within the GCFP Standard for Fraud Risk Assessment.

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

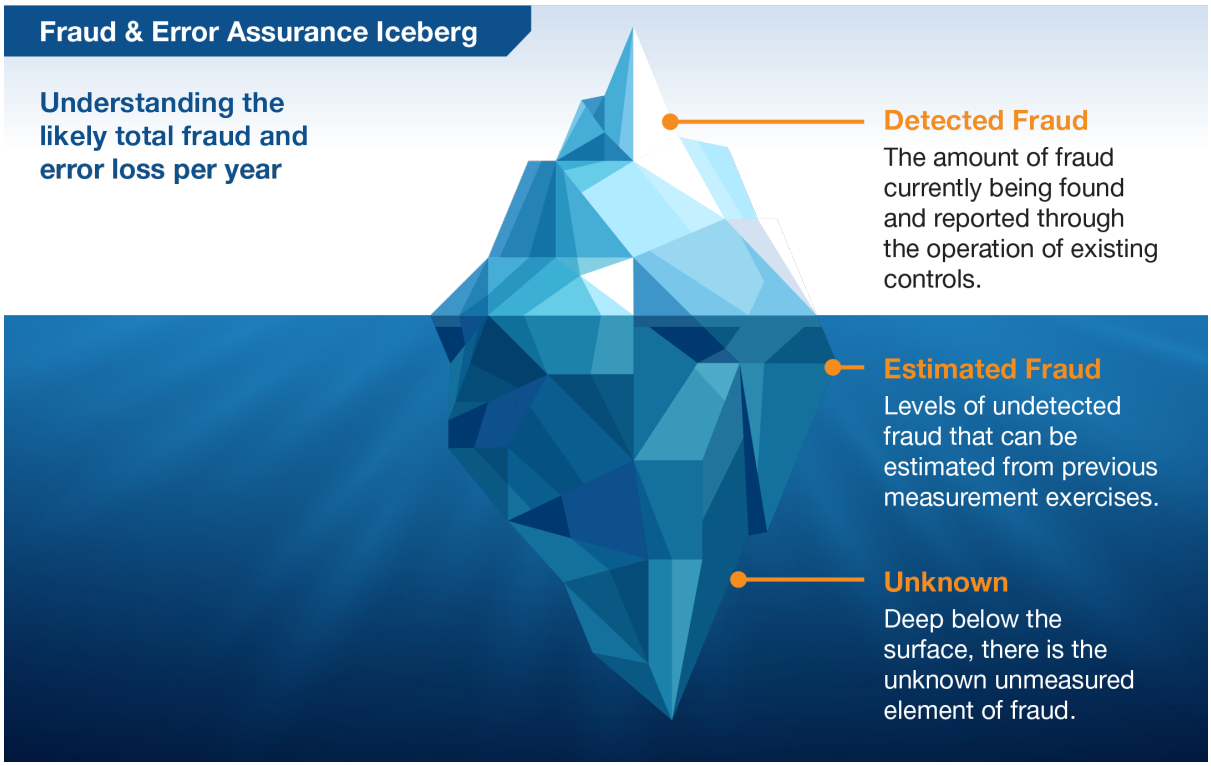
The first element of the assurance map is to ensure that there is an effective reporting process which captures instances of fraud and error within each of the areas of the business where fraud risks exist and reports these to the central counter fraud function. This allows an organisation to measure the amount of fraud and error that is being discovered through the operation of controls in particular areas of the business.

There is a need to gain ongoing assurance that such reporting is comprehensive to ensure that all instances of fraud or error identified through the operation of the organisation's control framework have been captured and reported. This allows an organisation to measure the amount of fraud and error that is being found through the operation of existing controls in particular areas of the business. Assurance requirements should also include identifying and comparing levels of fraud and error across different parts of the organisation and providing challenge where little or no cases of fraud and error are being found.

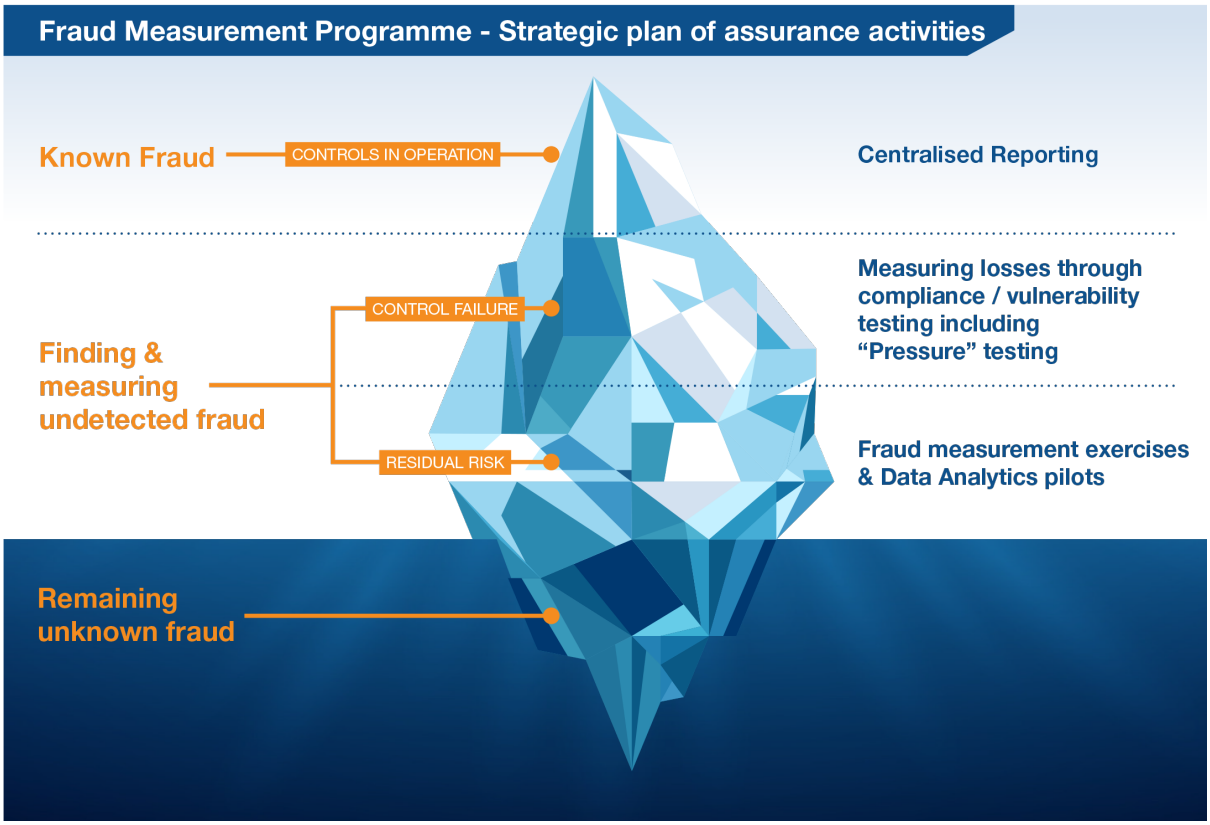
The second element of the assurance map is to obtain assurance on the operation of key controls that are designed to prevent or detect instances of fraud or error. This testing looks at the vulnerabilities of these controls and assesses the extent to which they have operated correctly. The assurance 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.

The third element of the assurance map is to 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.

Fraud and error – a model of the scope and purpose of organisational assurance requirements:



The purpose of delivering assurance activities in relation to fraud and error is in order 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 'iceberg' through those activities as illustrated in the diagram below:



Fraud and error – organisational assurance requirements:

Area	Assurance requirement
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

Assurance should also include the provision of benchmarking between different parts of the business 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.

F3. Building a fraud measurement programme within the organisation

Organisations should develop a multi-annual 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 and on-going reporting of 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.

F4. Developing and implementing an annual plan as part of the ongoing fraud measurement programme

The fraud measurement programme should be implemented through annual plans which carry out fraud measurement activities within the scope of the fraud measurement programme. The annual plan should also ensure that activities are carried out to provide the assurance requirements detailed in the assurance map for fraud and error risks.

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

F5. 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 & Risk Committee, should have oversight of the fraud measurement programme and the development of the annual 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 & 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.

F6. Measuring the effectiveness of the counter-fraud strategy

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

- Key Performance Indicators and metrics – to measure the effectiveness of activities within the strategy to find or prevent fraud and error; and to demonstrate the achievement and success of key activities within the counter fraud strategy;
- 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. This might include: increased numbers of transactions; new areas of spend; turnover of staff; identified new threats; increased instances of particular frauds across the public sector, etc.

F7. Continuing Professional Development (CPD)

The organisation should ensure that all individuals who are performing fraud measurement activities undertake regular learning and development to keep their skills and knowledge up to date. On a generic level the skills and knowledge development they need will be counter fraud knowledge, and knowledge of understanding and meeting organisational assurance requirements. In addition, there is a specific requirement to keep up to date with developments in the areas and techniques mentioned and covered in this Fraud Measurement Standard.

G. Further information and Glossary

G1. Glossary

Assurance: part of corporate governance in which an organisation plans and undertakes activities to provide management, and organisational stakeholders, with accurate and current information about the efficiency and effectiveness of its policies and operations, and the status of its compliance with statutory, and other, obligations.

Bribery and Corruption: the promise, offer or gift of an advantage, financial or other, to another person with the intention of inducing that person to perform a relevant function or activity improperly; and conversely the agreed acceptance of such an inducement.

Business Insight: is defined as being able to understand the 'bigger picture' and identify what may be happening below the surface or what may occur in the future.

Confidence Levels: the extent to which a sample drawn from a population is considered to be representative of that population. Expressed in percentage terms it gives an indication of the likelihood of any sample selected is representative.

Controls: the design, application and review of policies, procedures, standards, systems, training and culture to address risk.

Counter Fraud: activities designed to understand, manage and mitigate organisational fraud risks.

Counter Fraud Function: team or individual responsible for the management of counter fraud activities within a government organisation.

Disciplines: distinct specific areas of expertise, knowledge and skills that provide recognised capabilities within the counter fraud profession.

Evidence: the collection and analysis of data from which a conclusion can be drawn e.g. whether or not a transaction is regular or irregular.

Error: an item or transaction that is irregular but where there is sufficient evidence on a balance of probabilities that there was no intent to defraud.

Estimation: using statistical methods to provide an assessment of levels of fraud that are likely to exist although not currently detected.

Fraud: is defined as set out 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. In HMG we use this definition but for recording and reporting instances of fraud we apply the civil law 'balance of probabilities' test.

Fraud Measurement: building a picture of the extent to which an organisation is impacted by fraud. This includes identifying and recording known instances of fraud and adding to this an assessment of levels of undetected fraud, as well as measuring preventative savings through actions taken.

Fraud Risk Assessment: is 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.

Fraud Landscape: understanding of current and future organisational, national and international fraud trends (horizon scanning) as well as the organisation's fraud profile; namely the estimated, detected, recovered, prevented and unknown fraud.

Governance and Oversight: the means by which an organisation is directed and controlled.

Inherent risk: also defined as gross risk, is the risk to the organisation assuming there are no controls in place.

Irregularity: an item or transaction that is incorrect, has no legal basis or has arisen through bribery or corruption. It combines both fraud and error.

Management Information Systems (MIS): a process, or a suite of linked or independent processes, which provide an organisation or part of that organisation with the information needed to manage effectively their day-to-day operations and provide advance notice of beneficial opportunities or adverse events.

Margin of Error (Precision): the extent to which any level of finding / rate of error ascertained from testing a sample reflects the 'true' rate of error within the population from which the sample was drawn. The margin of error is expressed as a range with likely minimum and maximum values.

Qualitative and Quantitative Techniques: quantitative research is the collection and use of numerical data that is used and analysed using mathematically based methods (in particular statistics); qualitative research is any which does not involve numbers or numerical data. Qualitative research seeks to answer questions about why and how things have happened and why people behaved in a certain way. It thus provides in-depth information about human behaviour, including those behaviours analogous to fraud. It often involves words or language, but may use pictures or photographs and observations.

Residual risk: also defined as net risk, is the risk remaining once the risk response has been applied successfully.

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.

Risk Appetite: the amount of risk an organisation is willing to accept at the enterprise level.

Risk Tolerance: the threshold levels of risk exposure that with appropriate approvals can be exceeded, but which when exceeded will trigger some form of response e.g. reporting the situation to senior management.

Statistical Sampling: taking a relatively small items that are representative of a much larger population on which to conduct research and testing in order to draw conclusions about the population from which the sample was drawn.

Strategy: a plan of action designed to achieve a mid-to-long-term aim. In the context of counter fraud standards, it means developing a mid-to-long term plan of action considering current and future strengths, weaknesses, opportunities and threats, and look to build toward a defined future state.

Testing: the application of comparing a situation or data with other data and information for comparative purposes with a view to ascertaining the correctness, or otherwise, of that situation or data.

Annex A

Typology used to report fraud and error in Central Government			
External - Expenditure	Procurement - Collusion between contractors		Computer hacking and unauthorised misuse
	Procurement - mis selling		Other
	Procurement - other		**Total (Number of cases and value)**
	Means-tested payments	**External - Third Party**	Charge Evasion
	Means-tested payments - Childcare		Fine and court costs evasion
	Means-tested payments - Income		Tax fraud - national
	Means-tested payments - Disability		Tax fraud - local
	Means-tested payments - Carer's		Other
	Means-tested payments - Education		**Total (Number of cases and value)**
	Means-tested payments - Working hours	**Internal - Staff**	Payment fraud
	Means-tested payments - Other		Receipt fraud
	Grants - Fraudulent grant application		Exploiting assets and information
	Grants - Fraudulent application from charities		Identity theft
	Grants - Misuse of grant funding		Personnel management
	Grants - Other		Travel and expenses, pay and other allowances
	EU payments		Procurement fraud - Staff collusion
	Loans		Procurement fraud - GPC
	Assets - Theft and misuse		Procurement fraud - other

	Assets - Written off		Theft of assets
	Other		Management reporting fraud
	Total (Number of cases and value)		Computer hacking and unauthorised misuse
External - Supplier	Exploiting assets and information		Other
	Identity theft		**Total (Number of cases and value)**
	Post contract fraud	**Overall Total (Number of cases and value)**	