



Government  
Counter Fraud  
Profession

Operated by the Public Sector Fraud Authority

# Government Counter Fraud Profession

## Practitioners Standard for Fraud Detection

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

Public Sector Fraud Authority

Publication date: May 2025

© Crown copyright May 2025

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

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

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

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

# Document Control

Information	This document is part of the Government Counter Fraud Profession (GCFP) Standards and Guidance
Date Published	May 2025
Review Date	May 2028

# Version Control

Version	1.0
---------	-----

# Contents

<b>A. Professional Standard and Competencies for Fraud Detection Practitioners</b>	<b>6</b>
A1. Purpose	6
A2. Introduction	6
A3. How This Document is Structured	7
A4. Government Functions (UK)	8
A5. Public Sector Fraud Authority	9
A6. Government Counter Fraud Profession	10
A7. Government Counter Fraud Framework	10
A8. Roles and Responsibilities	13
A9. Key Components Explained	14
A10. Competency Levels	14
<b>B. Fraud Detection Competency Framework</b>	<b>15</b>
<b>C. Guidance on Processes for Fraud Detection</b>	<b>20</b>
C1. Introduction	20
C2. Fraud Detection Model	20
C3. Continuous Improvement Detection Framework	22
<b>D. Guidance on Products for Fraud Detection Practitioners</b>	<b>23</b>
D1. Introduction	23
D2. Fraud Detection Strategy	23
D3. Fraud Detection Action Plan	24
D4. Fraud Detection Exercise Plan	25
D5. Fraud Detection Report	26
D6. Reporting Routes	27
<b>Tools</b>	<b>28</b>
D7. Fraud Detection Dashboard	28
D8. Fraud Detection Checklist	29
<b>E. Guidance for Organisations</b>	<b>31</b>
E1. Fraud Detection Strategy	31
E2. Proactive and Reactive Detection	31
E3. Aligning Fraud Detection and Prevention	31
E4. Intelligence	32

E5. Audit, Compliance and Inspection Activity	32
E6. Fraud Risk Assessment	33
E7. Fraud Measurement	34
E8. Data Analytics	34
E9. Culture	37
E10. Counter Fraud, Bribery and Corruption Training	37
E11. Communication and Engagement	37
E12. Horizon Scanning	38
E13. Media	38
E14. Legal Obligations	38
<b>Supplementary Information</b>	<b>40</b>
E15. Fraud Indicators	40
E16. After a Detection Exercise	42
E17. Categories of Fraud Detection	43
E18. Fraud Detection Methods	43
E19. Fraud Control Testing	44
E20. Fraud Detection Software	45
E21. System Monitoring	46
E22. Data Matching	46
E23. Exception Reporting	46
E24. Random Sampling	47
E25. Evolving Technology	48
<b>F. Further Guidance</b>	<b>49</b>
F1. Further Information	49
F2. Products From Other Standards	50
F3. Functional Standards	51
F4. Further Reading	53
<b>Glossary</b>	<b>55</b>
<b>Appendix 1 - Full Competency Framework</b>	<b>59</b>



# A. Professional Standard and Competencies for Fraud Detection Practitioners

## A1. Purpose

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

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

Their aim is

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

The professional standards and competencies are not intended to cover every eventuality or every specific issue that may arise and should be adapted to the organisation's resources

and fraud risk profile. This standard should be read in conjunction with all other GCFP Standards. The standard does not supersede an organisation's operating procedures. The GCFP standards are designed and intended for individuals and should be read in conjunction with organisational operating standards where these exist.

## A2. Introduction

In order for public bodies to understand and tackle public sector fraud, they must be able to find it.<sup>1</sup>

People need to have the right skills, knowledge and experience to support organisations to prevent, detect and respond to fraud. Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk.<sup>2</sup>

**Fraud detection (in this context) is the process of recognising and identifying potential fraud and differentiating this from legitimate activity using appropriate tools, techniques and knowledge.<sup>3</sup>**

**This core discipline is focused on the skills, knowledge and experience required to implement detection techniques and practices, aiming to identify fraud through systems, strategies, data techniques and data analysis.**

---

<sup>1</sup> <https://www.gov.uk/government/publications/cross-government-fraud-landscape-report-2021-2022/cross-government-fraud-landscape-report-2021-2022-html>

<sup>2</sup> <https://www.nao.org.uk/wp-content/uploads/2024/11/fraud-overview-2023-24.pdf>

<sup>3</sup> "Fraud detection" is an activity not to be conflated with the "detected fraud" category used in cross-government reporting, which is submitted to the PSFA via the Consolidated Data Request (CDR).

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

[The Government Counter Fraud Functional Standard GovS 013](#) states that organisations should undertake proactive fraud detection activity.

*“Proactive detection activity can include fraud, bribery and corruption measurement and assurance activity, or the use of data sharing and/or data analytics to attempt to find fraud in a specific business area, based on a good understanding of the risks in that area. Organisations should undertake activity to try and detect fraud, bribery and corruption in high-risk areas where little or nothing is known of fraud, bribery and corruption levels. This activity should include using loss measurement activity (fraud measurement and assurance) where suitable.”<sup>4</sup>*

Fraud detection through reporting routes, systems, strategies, data techniques and data analysis may suggest that fraud has occurred, however it does not automatically confirm it is fraud. Detection practitioners must use their own skills and experience, as detection results may indicate fraud, error, false positives or legitimate activity. It is important to differentiate between these outcomes and verify results. The human element of detection is essential. Everyone associated with an organisation has a responsibility to detect fraud, supported by specialists with specific roles in this area.

Effective fraud detection cannot be undertaken in isolation from other counter fraud disciplines. For fraud detection to be effective it needs to consider the interdependencies of an organisation’s prevention measures, fraud risk and threat profile, the results of recent fraud measurement activity, the controls in place to prevent and detect fraud, and the results of audit and compliance reports.

As part of the continuous improvement process, consideration may be given to understand how and why any detected fraud or error occurred in the first place, in order to take or recommend corrective measures to safeguard public funds in the future.

### A3. How This Document is Structured

This document contains the following

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

These standards have been created, reviewed and agreed by the GCFP Board, the body with oversight of the profession, and the 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<sup>5</sup> (CSAG).

4 [https://assets.publishing.service.gov.uk/media/612e5a8ce90e0705355a552b/6.7628\\_CO\\_Govt-Functional-Std\\_GovS013-Counter-Fraud\\_v4.pdf](https://assets.publishing.service.gov.uk/media/612e5a8ce90e0705355a552b/6.7628_CO_Govt-Functional-Std_GovS013-Counter-Fraud_v4.pdf)

5 The Cross Sector Advisory Group (CSAG) is a cross-industry group of experts in a range of disciplines who provide advice to evolve and shape the Profession. This group provides advice to the GCFP Board.

## A4. Government Functions (UK)

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

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

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

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

### The Government Functions

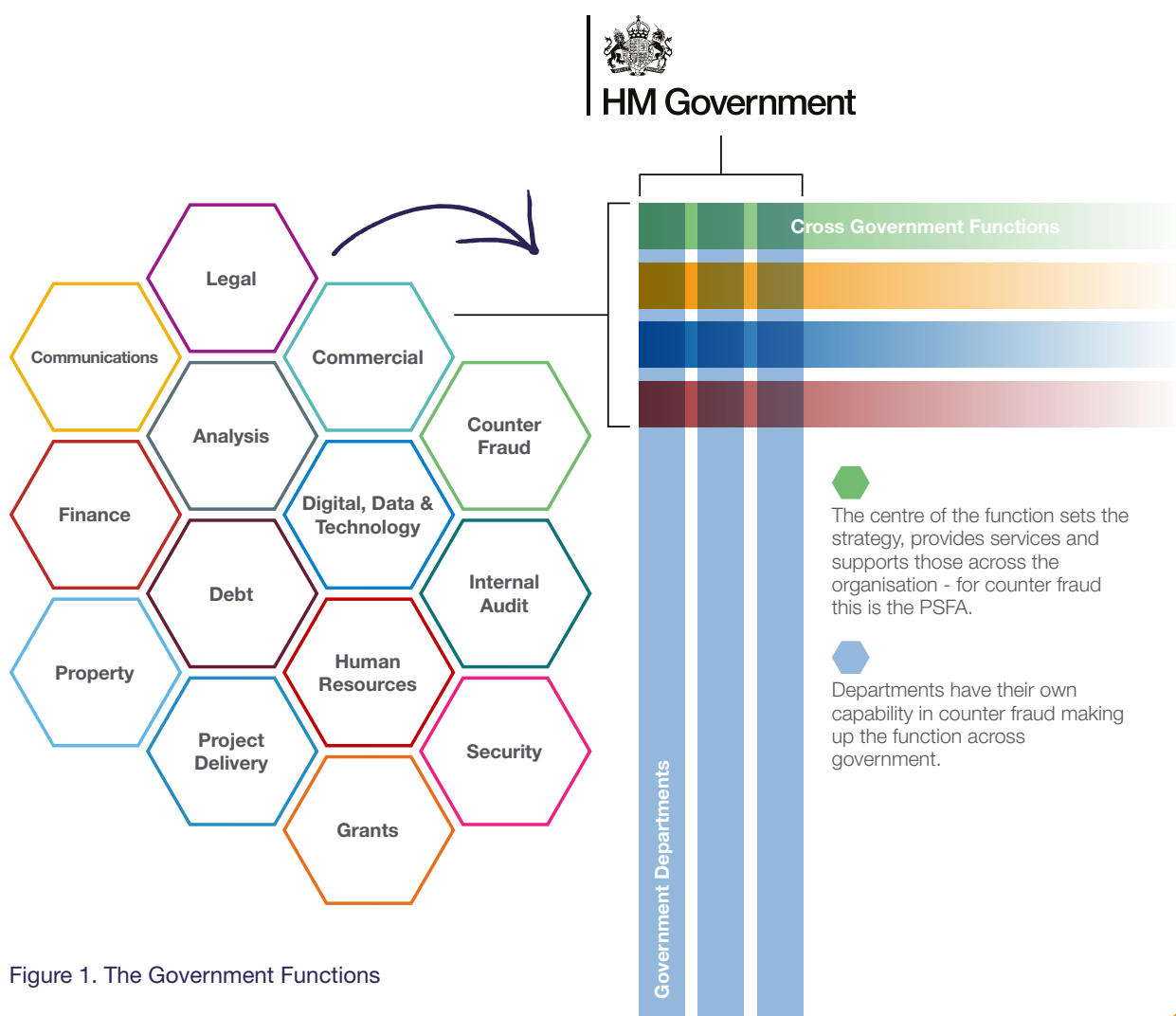


Figure 1. The Government Functions



## A5. Public Sector Fraud Authority

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

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

### It brings:

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

**The PSFA is changing the way that government manages fraud.**

### Its mission is to<sup>6</sup>:

- ✓ Modernise the fraud and error response by widening access and use of leading practices, tools and technology, better protecting taxpayers' money
- ✓ Build expert-led services developed in collaboration with experts in departments and public bodies to better fight fraud and error through risk, prevention, data and enforcement techniques
- ✓ Develop capability in the public sector to find, prevent and respond to fraud both organisationally and individually
- ✓ Put performance at the heart of the public sector fraud conversation focusing on investments and outcomes
- ✓ Aim to be seen as a beacon of fraud and error expertise and a destination for those wanting to make a difference in fighting public sector fraud.

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

## A6. Government Counter Fraud Profession

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

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



The GCFP Cross  
Government Board leads  
oversight of the Profession

## A7. Government Counter Fraud Framework

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

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

## The Government Counter Fraud Framework

### Organisational Level

#### Functional Standards

The Functional Standards detail the basics that an organisation should have in place to have an effective counter fraud response. This includes a level of fraud awareness across the organisation.

### Core Disciplines

#### Leadership, Management and Strategy

An awareness across all specialist areas and the capability to define an effective counter fraud response and how to deploy the specialisms in the business.



### Subdisciplines



Figure 2. The Government Counter Fraud Framework

## Membership Categories

There are five membership categories mapped to the GCFP framework, namely



Figure 3. The Government Counter Fraud Framework Membership Categories

### The Fraud Control Cluster

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



Figure 4. The Fraud Control Cluster

The Fraud Detection Standard is part of the GCFP framework of standards. It will support the GCFP Fraud Control membership pathway. To be acknowledged as a counter fraud practitioner these standards will have to be met. A combination of the disciplines from the **Fraud Control** cluster allows individuals working in the area of fraud risk and prevention to advance within the Government Counter Fraud Profession.


For information regarding how you can be recognised as a member of the Government Counter Fraud Profession (GCFP) please contact:

[GCFP@cabinetoffice.gov.uk](mailto:GCFP@cabinetoffice.gov.uk)

## A8. Roles and Responsibilities

All employees and those associated with an organisation have a part to play in promoting an effective counter fraud environment, where fraud detection is encouraged and supported. For the purposes of this standard, a practitioner will be operating within the counter fraud environment and will have the ability and opportunity to undertake, measure and influence fraud detection activities through the work they carry out.

Leadership across an organisation should encourage detection activity, seeking to find fraud in order to support effective governance, promote compliance with processes and controls, and ultimately prevent the same fraud from reoccurring through a continual process of refinement and improvement of the overall organisational counter fraud response.



All employees and those associated with an organisation have a part to play in promoting an effective counter fraud environment



## A9. Key Components Explained

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

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

1

### Counter Fraud, Bribery and Corruption Knowledge

Knowledge of fraud offences and typologies. Understanding the fraud landscape, why fraud is committed and its impact, in order to detect fraud.

2

### Organisational Knowledge

Knowledge of organisational structures and fraud response.

3

### Detection Methods

Knowledge and understanding of methods of detection and controls and how to apply them effectively.

4

### Evaluation

Understanding how to evaluate detection outputs to identify appropriate next steps and improve controls, methods and responses.

5

### Engagement and Communication

Building and maintaining relationships with a range of stakeholders and understanding the internal and external communication landscape to inform and improve detection.

## A10. Competency Levels

General rules about the competency levels are set out below

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



## B. Fraud Detection Competency Framework

### Practitioner Competency

The below competencies are required to attain Practitioner level. The full Detection Competency framework can be found at **Appendix 1**. Guidance on terminology can be found in the Glossary.

#### 1. Counter Fraud Bribery and Corruption Knowledge

**Knowledge of fraud offences and typologies. Understanding the fraud landscape, why fraud is committed and its impact, in order to detect fraud**

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

## 2. Organisational Knowledge

### Knowledge of organisational structures and fraud response

- 2.1 Demonstrate knowledge of how an organisation is structured, including roles and responsibilities relating to counter fraud

---

- 2.2 Demonstrate knowledge of the range of internal stakeholders within an organisation who can support fraud detection

---

- 2.3 Apply knowledge of the organisational fraud risks and controls and how these impact on detection and detection methods

---

- 2.4 Demonstrate an understanding of the contribution that fraud detection makes to effective fraud deterrence

---

### 3. Detection Methods

#### Knowledge and understanding of methods of detection and controls and how to apply them effectively

- 3.1 Demonstrate an understanding of the difference and connection between Fraud Detection, Investigation, Intelligence and Fraud Prevention
- 3.2 Apply the different stages of the Fraud Detection Model<sup>7</sup> and explain how these feed into and inform detection
- 3.3 Demonstrate an understanding of the difference between proactive and reactive detection
- 3.4 Demonstrate the application of detection techniques, methods and tools within the organisation, whilst actively seeking innovative ways to improve detection
- 3.5 Demonstrate an understanding of the different types of data held by an organisation which can be used to detect fraud
- 3.6 Demonstrate an understanding of the factors which affect the quality of both the data and its analysis
- 3.7 Demonstrate an understanding of the role of data analytics in fraud detection and evaluation and how it may be applied
- 3.8 Demonstrate an understanding of the different types of audit, compliance and inspection activity and how these can assist fraud detection
- 3.9 Demonstrate the ability to create a fraud detection plan
- 3.10 Demonstrate the ability to use external data to support fraud detection

<sup>7</sup> Fraud Detection Model - as described in section C2 of this document

## 4. Evaluation

### Understanding how to evaluate detection outputs to identify appropriate next steps, and improve controls, methods and responses

- 4.1 Demonstrate how to apply the continuous Improvement Detection Framework and identify opportunities for improving fraud control methods and responses as new risks emerge

---

- 4.2 Demonstrate how to assess and interpret the outcomes of detection by recognising and differentiating between potential fraud, error, and legitimate activities

---

- 4.3 Demonstrate the use of appropriate options and next steps for detection outcomes

---

- 4.4 Demonstrate the ability to create a report of detection activity undertaken to record and communicate detection findings and recommendations

---

- 4.5 Demonstrate the ability to identify, continually develop and refresh sources of information which inform the detection of fraud

---



## 5. Engagement and Communication

**Building and maintaining relationships with a range of stakeholders and understanding the internal and external communication landscape to inform and improve detection**

**5.1** Demonstrate how to use a range of communication channels and techniques to promote fraud detection across the organisation

---

**5.2** Demonstrate awareness of the external environment around emerging risks that could impact detection within the organisation

---

**5.3** Demonstrate how to identify, build and maintain stakeholder relationships through a range of communication mechanisms to identify and detect fraud

---

**5.4** Demonstrate the ability to work collaboratively with relevant internal and external stakeholders and be able to identify when to bring in specialists from inside or outside the organisation

---

**5.5** Demonstrate how to effectively communicate the findings and outcomes of detection activities

---

## C. Guidance on Processes for Fraud Detection

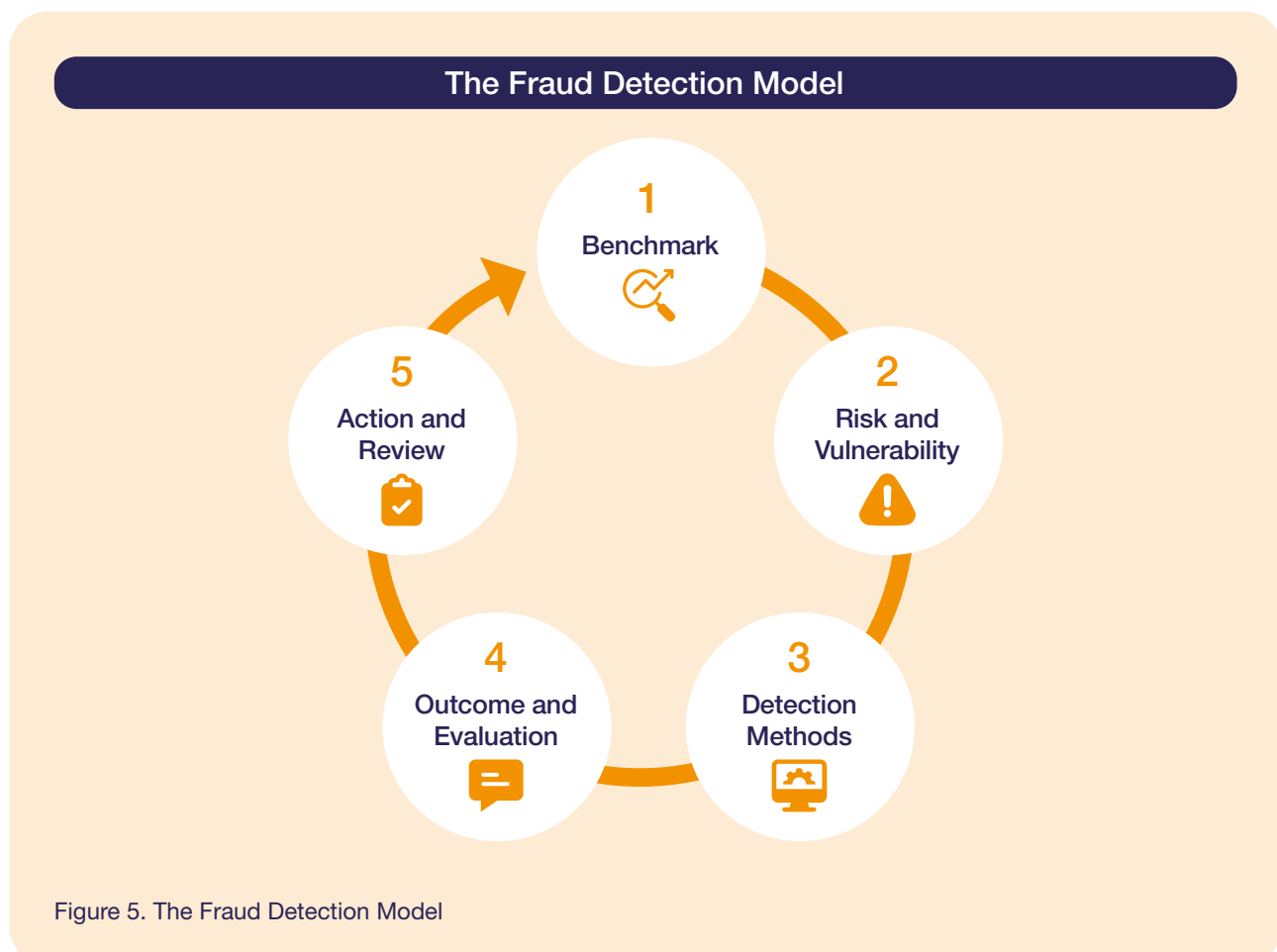
### C1. Introduction

This guidance supports the standard for a fraud detection practitioner. All processes and procedures should be regularly revised and evaluated to ensure they remain best practice. Set out below are the processes for undertaking, measuring and improving fraud detection work.

### C2. Fraud Detection Model

The Fraud Detection Model is a process which helps to identify and focus the steps taken in a detection exercise. The model considers the benchmark or starting point, the gathering of relevant information to inform risks and vulnerabilities, the use of appropriate detection methods and the evaluation of outcomes leading to appropriate next steps being taken.

An effective detection exercise should go through the below steps, while an individual practitioner may oversee some or all of the steps in a given detection exercise depending on the organisation and their role within it.



## The Fraud Detection Model can be described in the following steps

### 1 Benchmark



**Step 1** in the Fraud Detection Model is understanding what is normal or typical activity or behaviour. This will enable you to ascertain what a discrepancy might look like in order to then be able to differentiate between possible fraud, possible error, false positives and legitimate activity after detection methods have been utilised. This understanding of what normal is will either come from direct knowledge and experience or from access to trusted and reliable sources or data.

### 2 Risk and Vulnerability



**Step 2** in the Fraud Detection Model is understanding what the fraud risk and vulnerabilities are within the specific area under examination. This information may be obtained from a variety of sources including fraud risk assessments, initial fraud impact assessment, audits, fraud loss measurement, horizon scanning, knowledge and experience, comparative issues or media reports. Understanding the relevant fraud risks and vulnerabilities enables a practitioner to effectively target specific areas for detection.

### 3 Detection Methods



**Step 3** in the Fraud Detection Model is the activity of detecting possible fraud, using the appropriate tools and techniques to look for anomalies and suspicious activity. The methods used will vary depending on the organisation and context of the exercise and may be derived from people, technology or a combination of both.

### 4 Outcome and Evaluation



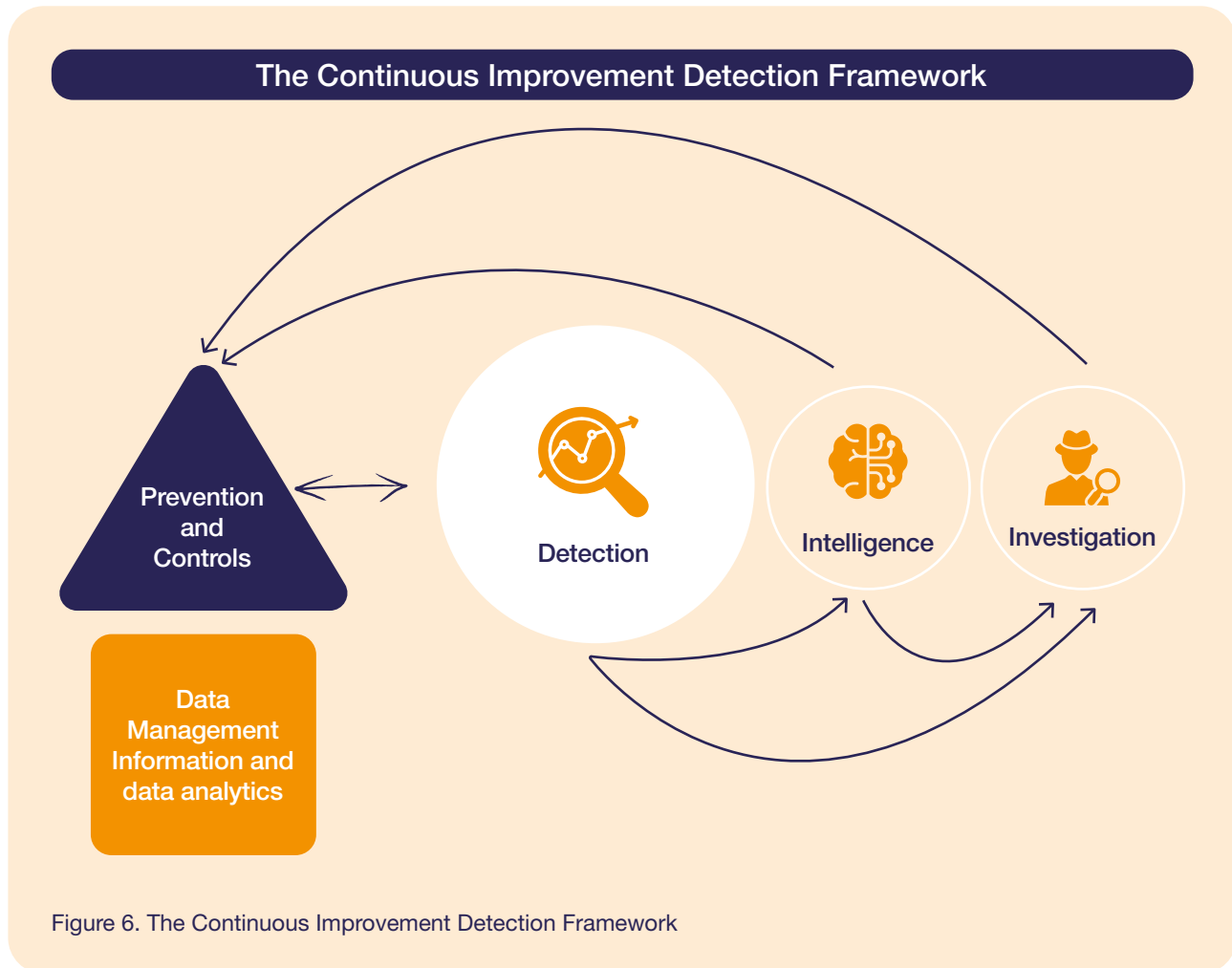
**Step 4** in the Fraud Detection Model is assessing and evaluating the outcomes of the detection activity, to determine whether there are sufficient grounds to suspect fraud by differentiating between what is legitimate activity, false positives, error and fraud. The evaluation of detection outcomes should also allow for an assessment of the most practical, reasonable and proportionate way to pursue these.

### 5 Action and Review



**Step 5** in the Fraud Detection Model is identifying and implementing possible next steps once potential fraud has been detected. How this is done will depend on the organisation's risk appetite and resources. Consideration should be given to potential further development through intelligence, investigation, prevention and controls, as part of the wider Continuous Improvement Detection Framework.

### C3. Continuous Improvement Detection Framework



The Continuous Improvement Detection Framework underpins the Fraud Detection Model and emphasises the importance of continuous feedback and refinement. By consistently feeding lessons learnt and performance effectiveness from detection, intelligence development and investigation back into prevention and controls, the organisation can continuously improve and evolve its strategies, tools and processes to detect and prevent fraud.

The process looks at **improvements** to reduce or mitigate fraud, error and loss. This should include ascertaining how widespread the issue is and may involve improving policies, enhancing employee training, updating algorithms, refining techniques,

improving controls, incorporating regular audits, implementing lessons learnt, communicating issues of interest to all relevant stakeholders or redesigning processes to minimise the likelihood of the fraud or error reoccurring.

This feedback loop ensures constant improvement, as insights from detection, intelligence development and investigations can all inform and enhance prevention strategies and lead to a more robust and effective approach to fraud detection.

## D. Guidance on Products for Fraud Detection Practitioners

### D1. Introduction


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

The detection strategy may be innovation focused and might involve the use of technology and data analytics to identify patterns, training staff to recognise signs of fraud, and establishing a framework for reporting and investigating suspected fraudulent activities. The ultimate goal of a fraud detection strategy is to detect actual losses, minimise potential losses and protect the organisation's resources and reputation.

### D2. Fraud Detection Strategy

The detection strategy may be a separate strategy or integrated into the counter fraud strategy, and may depend on the structure of the organisation. In order to implement the detection strategy, an annual detection action plan may be prepared, either separately or incorporated into the wider annual counter fraud action plan.

The detection strategy is a mid to long-term plan considering current fraud detection activity and future strengths, weaknesses, opportunities and threats, and looks to build toward a defined future state surrounding fraud detection. Organisations should have policies that support the delivery of fraud detection, its assurance requirements and supporting fraud detection procedures. These policies should be aligned to the counter fraud policy.



Organisations should have policies that support the delivery of fraud detection



### Detection Strategy Development<sup>8</sup>

- **Define Scope and Timeframe** – Establish the boundaries of the strategy, including which areas of the organisation and its operations are covered, and set a clear timeframe for implementation
- **Consult Stakeholders** – Engage with both internal and external stakeholders to gather insights, ensure alignment, and secure buy-in for the strategy
- **Optimum Future State Discussed, Agreed and Presented Simply** – Collaboratively defines the desired future state of the organisation's counter fraud capabilities, ensuring it aligns with overall business goals. Present this vision clearly and concisely
- **Define Key Activities That Will Be Undertaken** – Identify and agree upon the main actions required to implement the strategy effectively, ensuring that they address both current and future fraud challenges
- **Investment and Resources Analysed and Agreed** – Evaluate the necessary resources, and ensure the required investments are agreed upon and allocated



### D3. Fraud Detection Action Plan

A fraud detection action plan may support the broader fraud detection strategy, this is separate to the counter fraud action plan, which outlines the specific steps and measures to identify, prevent, and respond to fraudulent activities.<sup>9</sup> While the strategy provides the overarching vision and objectives, the action plan translates this into practical actions, detailing the necessary resources, timelines, responsibilities, and expertise for implementation. The need for a fraud detection action plan arises from the growing sophistication and frequency of fraudulent activity, necessitating a structured approach to detection. By having a well defined action plan, organisations can proactively address vulnerabilities, streamline detection processes, and ensure swift responses to potential threats. It would be good practice in the fraud detection action plan for each action to be SMART (Specific, Measurable, Attainable, Relevant and Timely) and have clear metrics and outcomes. The success of a fraud detection action plan could be measured by a number of indicators such as a reduction in fraud incidents, an increase in detection rates and the frequency of false positives.

The detection action plan should outline those policies and procedures that are to be used to implement a fraud detection programme. This plan should identify the resources needed, the requirement for any specialist skills, experience and the measures against which the detection programme will be evaluated. Organisations should ensure fraud detection is included in their counter fraud policy. This policy should articulate the organisation's approach to detecting fraud.

<sup>8</sup> <https://www.gov.uk/government/publications/building-a-counter-fraud-strategy-practice-note/building-a-counter-fraud-strategy-practice-note>

<sup>9</sup> The Counter Fraud Action Plan can be found in the GCFP LMS Standard available upon request

A fraud detection action plan may include:

1. **Introduction** which sets out the rationale behind the plan, linking it to the fraud detection strategy and counter fraud annual action plan sets the scene
2. A **section** which may take the form of a matrix or table that sets out the key actions/objectives to be completed in the forthcoming year. These actions could aim towards a variety of goals
  - increasing fraud detection capability
  - including fraud risk assessment
  - the introduction of key new controls to reduce risk or loss and any proactive detection activity
  - including fraud loss measurement, which will be undertaken to estimate the level of fraud
  - any new powers or legislation that will be pursued
  - the testing or implementation of any new data sharing or analytics tools.
3. The **matrix**
  - should have actions that are SMART (Specific, Measurable, Achievable, Realistic and Timely)
  - may be divided by framework specialism, payment stream, or area of the business
  - should have each action assigned to an individual and/or teams
  - should flag if there is/may be the requirement for specialist resources and any budget impact
  - should have agreed and realistic deadlines and set out high-level success/performance criteria for each action

## D4. Fraud Detection Exercise Plan

Before undertaking any detection activity, consideration may be given to producing an appropriate fraud detection exercise plan to define the parameters of the exercise. Having a defined plan is the starting point of a clear audit trail of decisions and activity. A fraud detection exercise plan may incorporate appropriate mechanisms to enable measurement of the activity. A fraud detection exercise plan might include

- **Background** – A description of why the particular area is being looked into and why the exercise is being undertaken, for example, following a specific incident, risk, investigation, intelligence report, fraud report or as part of a wider risk review
- **Scope** – What are you examining, what are you trying to find and how will you know if you find it, what is included in and excluded from the exercise?
- **Methodology** – Details of planned activity including sample type and size (where relevant), and justification for this. What tools will be used (including technology), timelines, resources required and data sources. How the fraud detection exercise will be measured
- **Considerations** – Relevant considerations regarding data governance, public sector equality duty and equality impact assessments, policies and procedures
- **Stakeholder identification** – Who needs to know about the exercise and whose help do you need in order to carry it out effectively, what expertise is required (for example analytical and/or audit)

Following a fraud detection exercise a report of findings (fraud detection report) may be compiled with recommendations.


## D5. Fraud Detection Report

Once a detection exercise has been completed, a fraud detection report may be compiled to collate findings and make recommendations to inform further detection work or highlight any wider issues that may have been uncovered. Depending on the nature of the exercise and issues identified, the report may come at the end of the exercise itself or upon the conclusion of any subsequent investigations or actions that the exercise produced, in order to give a holistic assessment. If there are concerns that need immediate or urgent attention it may be appropriate to issue an interim report.

The report may include

- An executive summary
- Background and methodology (a summary from the initial detection plan)
- Findings
  - Nature of the fraud identified (if any) describing the type of fraud detected
  - Scale of potential fraud identified, detailing the frequency and estimated or actual value of the loss
  - Control weaknesses identified, including additional issues like the prevalence of errors or poor data quality
- Recommendations for improving controls, prevention methods and data cleansing
- Recommendations for remedial or further action, for example, further intelligence gathering or investigation
- Recommendations for further detection in other areas based on the methods or findings in the current exercise. If the findings, methods or recommendations have any possible implications or applications for other areas of counter fraud work


Reporting on detection activity forms part of the continual improvement process. By reporting on the outcomes of detection exercises and appropriately communicating the findings, practitioners can feed into the organisation's wider counter fraud response and enhance fraud controls. The report may be sanitised and circulated within a team, organisation or amongst external partners as appropriate.



Once a detection exercise has been completed, a fraud detection report may be compiled to collate findings and make recommendations

## D6. Reporting Routes

Organisations should have well established and documented reporting routes for staff, contractors and members of the public to report suspicions of fraud, bribery and corruption and a mechanism for recording these referrals and allegations.<sup>10</sup> Having established reporting routes is essential for fraud detection.<sup>11</sup> Providing a safe avenue for employees to report fraud and other criminality or misconduct within an organisation should allow employees (including suppliers and contractors) to come forward without having to refer to or involve management. Having appropriate methods of recording suspicions or concerns by area or type may also highlight potential patterns or problem areas over and above a specific allegation.



Having established reporting routes is essential for fraud detection

A fraud reporting policy and process may contain a number of factors<sup>12</sup>

- Be clear, simple and easily understood
- State the relevant legislation and what this means for whistleblowers and the process
- Define what constitutes a qualifying disclosure
- State who is, and who is not, covered by whistleblowing arrangements
- Publicise how to raise a concern and that concerns can be raised 24/7
- Stipulate who and where concerns should be reported to
- Refer to requests for anonymity
- Refer to requests for confidentiality
- State what whistleblowers can expect when reporting concerns
- Highlight the type of issues that can be raised
- Positively encourage anyone who has serious concerns about any aspect of their work to come forward and voice them
- Promote a policy whereby all persons can raise concerns without fear of retaliation and are protected from any such actions

10 [https://assets.publishing.service.gov.uk/media/612e5a8ce90e0705355a552b/6.7628\\_CO\\_Govt-Functional-Std\\_GovS013-Counter-Fraud\\_v4.pdf](https://assets.publishing.service.gov.uk/media/612e5a8ce90e0705355a552b/6.7628_CO_Govt-Functional-Std_GovS013-Counter-Fraud_v4.pdf)

11 <https://legacy.acfe.com/report-to-the-nations/2024/>

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

# Tools


Please see below for useful tools to assist in detection.

## D7. Fraud Detection Dashboard

A fraud detection dashboard may be designed to provide key insights into fraud trends, enabling quick decision making and a comprehensive understanding of the organisation's fraud landscape. A fraud detection dashboard may include

- **Fraud detection rate** – the percentage of transactions flagged as potentially fraud or error or false positive versus the total number of transactions
- **False positive rate** – the percentage of false positives or cases incorrectly flagged as potential fraud
- **Positive rate** – the percentage of positive or correctly flagged fraud
- **Seasonal or cyclical patterns** – analysis of whether fraud attempts rise at certain times of the year
- **By location or region** – geographical distribution of fraud incidents, useful for identifying fraud hotspots
- **By channel** – fraud cases classified by channels (online, in-person, mobile app), to see where vulnerabilities may lie
- **By business unit or department** – if applicable, show which departments or segments of the business are most affected by fraud
- **Detection time** – average time taken to detect fraud after it occurs, helping assess the effectiveness of the detection mechanisms
- **Unresolved rate** – the percentage of detected activity that remains unresolved at the time of reporting

- **Results of detection exercises** – summarising number of referrals to investigations and intelligence
- **Continuous improvement referrals** – number of referrals to prevention/controls/policy in order to improve fraud prevention and reduce risk
- **Emerging fraud patterns** – indicators of new or increasing types of fraud attempts, such as phishing, identity theft, or payment fraud
- **Fraud trends over time** – a line or bar chart showing the number of fraud cases, their financial value, or types of fraud over time (weekly, monthly, quarterly), to identify spikes or declines in fraudulent activity



A fraud detection dashboard may be designed to provide key insights into fraud trends



## D8. Fraud Detection Checklist

The following checklist is a tool which may assist practitioners in assessing fraud detection within your organisation.

Question	Benefits for detection
<b>1</b> Does your organisation have a fraud detection <b>strategy</b> and associated <b>fraud detection action plan</b> of activity?	A fraud detection strategy which aligns with the organisational counter fraud strategy is a mid to long term plan that looks to build toward a defined future state. The detection action plan will detail the detection activities the organisation will undertake. Regular review of the fraud detection strategy and detection action plan is essential as it ensures the effectiveness, reliability and improvement of systems by ensuring the effectiveness of controls, identifying weaknesses and gaps and promoting continuous improvement.
<b>2</b> Does your organisation undertake <b>pressure testing</b> to identify hidden or new fraud risks, understand how these have arisen and determine their potential impact?	Pressure testing is a proven way to proactively identify and eliminate the unknown risks an organisation faces. If organisations know where their processes and systems are vulnerable and challenge assumptions about how fraud is identified, assessed and managed, they are better equipped and informed to reduce the opportunity for fraud.
<b>3</b> Does your organisation undertake <b>fraud loss measurement</b> exercises to understand your level of fraud?	By undertaking fraud loss measurement exercises, an organisation is able to understand the level of fraud the organisation is exposed to and identify, quantify and report on fraud and error rates, new and current threats and vulnerabilities, areas of high risk and those characteristics which are giving rise to fraud.
<b>4</b> Is <b>technology</b> , for example, artificial intelligence (AI), data mining, predictive analytics, and machine learning used to detect complex or hidden fraud?	Technology can be used to detect fraud by identifying suspicious patterns, anomalies and trends or flagging known high risk actors in a system where manual processing may be impractical.
<b>5</b> Does the organisation have regular <b>audit, compliance and inspection</b> activity?	Audit, compliance and inspection activity provide a systematic review of financial records and processes helping to identify discrepancies, weaknesses and potential fraud indicators.
<b>6</b> Does the organisation have <b>fraud risk assessments</b> in place?	Fraud risk assessments i.e. Enterprise Fraud Risk Assessment, Thematic Fraud Risk Assessment, Full Fraud Risk Assessment and Initial Fraud Impact Assessment allow the organisation to understand where it has the potential to be vulnerable to fraud and error, by describing the fraud risks that the organisation faces and assessing their likelihood and impact. This in turn allows detection methods to be focused on areas of higher risk.

Question	Benefits for detection
<b>7</b> Are <b>lessons learnt</b> from past fraud incidents used to amend the fraud risk assessment and where necessary, enhance controls and detection processes and incorporated into the fraud detection strategy to refine and improve it?	By consistently feeding the lessons learnt from each detection exercise, intelligence development and investigations, back into the fraud risk assessment and internal control framework, the organisation can continuously improve and evolve its ability to detect and prevent fraud. This feedback loop ensures constant improvement, as insights from detection, intelligence development, and investigations can all inform and enhance prevention strategies and lead to a more robust and effective approach to fraud detection.
<b>8</b> Do you have access to <b>resources</b> to detect fraud? For example, data scientists, fraud practitioner, auditors and/ or analysts.	In order to have a robust and effective detection process, you need to have access to the necessary expertise and resources to support the detection strategy and activity.
<b>9</b> Does your organisation have a confidential and accessible fraud <b>reporting route</b> ?	Organisations should have an accessible fraud reporting mechanism in place that captures and allows reports of instances of suspected fraud, bribery and corruption. They should also have a policy and process communicated to all internal and external stakeholders.
<b>10</b> Is regular <b>fraud awareness training</b> provided to all staff?	Regular fraud awareness training is integral to fraud detection and should include everyone within the organisation including temporary staff and external contractors. Training increases awareness of what fraud looks like for the organisation and reaffirms an organisational commitment to tackling fraud.
<b>11</b> Do you undertake regular <b>fraud awareness campaigns</b> ?	Educating staff regularly across an organisation raises awareness of the fraud risks faced by the organisation, helping everyone to understand and recognise what fraud might look like, what to look out for and how to report any concerns and maintain the fraud culture of the organisation.
<b>12</b> Do you <b>horizon scan</b> for unknown fraudulent activity around your organisation?	Horizon scanning is a proactive approach that involves identifying emerging threats, trends, early signs of potentially important developments or significant incidents that may require further investigation within an organisational context. By systematically examining potential threats and opportunities, horizon scanning helps organisations detect early signs of fraud developments within an organisation or within comparable organisations. This may be a result of tip offs they received or from focussed investigative journalism. The media and investigative journalists play a particularly prominent role in bringing corruption issues to light.

## E. Guidance for Organisations

### E1. Fraud Detection Strategy

As detailed in the products section, organisations may wish to have a detection strategy that is detailed within its counter fraud strategy and should be approved by the organisation's board and audit and risk committee. In order to implement the detection strategy, an annual detection action plan may be prepared. This plan may outline the policies and procedures that are to be used to implement a fraud detection programme.

### E2. Proactive and Reactive Detection

Finding fraud is an essential part of government efficiency<sup>13</sup> and therefore all organisations should look for fraud proactively, to reduce loss and improve the organisation's overall counter fraud response to better safeguard public funds. This is not to say there is no requirement for reactive detection, there will always be occasions when reactive detection is the most appropriate approach.

Proactive detection involves searching for potential fraud before it is reported or is discovered. It aims to minimise the impact of fraud earlier by taking a risk based approach to selecting areas of focus, prioritising higher risk over lower risk areas, while also looking for hidden fraud in areas where little or no fraud has been found previously.

Proactive detection may be integrated into the organisation's wider counter fraud response, by working closely with the organisation's risk, prevention, intelligence, and investigation functions to collect and manage information on potential fraud and fraud risks.

Reactive detection occurs as a response to a specific issue being brought to the attention of the organisation, for example a tip-off. This reactive approach may be a standalone act of detection, but can also feedback into improving a particular control that may have been compromised (or non-existent). In cases of reactive detection work, the direction of focus will initially be dictated by the nature of the 'tip-off'.

### E3. Aligning Fraud Detection and Prevention

Effective fraud detection cannot be undertaken in isolation. Fraud prevention and fraud detection are both essential components of a comprehensive fraud management strategy within an organisation and work together to minimise the impact of fraudulent activities.<sup>14</sup>

Fraud prevention measures and controls contribute to detection activities by reducing the opportunities for fraud to occur, thereby making it easier for fraud detection systems to identify suspicious patterns and anomalies when they do arise.

Fraud detection can help to prevent loss from the system by identifying fraudulent acts before a payment is made or a service is provided. In this way, detection can serve as a control by identifying fraud at the earliest opportunity to reduce any potential harm or loss.

13 <https://www.gov.uk/government/publications/cross-government-fraud-landscape-report-2021-2022/cross-government-fraud-landscape-report-2021-2022-html>

14 [https://assets.publishing.service.gov.uk/media/64b1327448826b000d3a9e42/3270\\_GCFP\\_Prevention\\_Standard\\_V5.pdf](https://assets.publishing.service.gov.uk/media/64b1327448826b000d3a9e42/3270_GCFP_Prevention_Standard_V5.pdf)

Outputs from fraud detection can inform an organisation's fraud prevention strategy by identifying where and how fraud has occurred, enabling steps to be taken to mitigate a specific risk or remove it entirely. Information collected from fraud detection efforts provides insights into emerging threats, allowing organisations to adjust their controls including preventative accordingly. This contributes to the ongoing improvement of counter fraud strategies.

## E4. Intelligence<sup>15</sup>

Understanding intelligence is necessary for fraud detection because it provides insights into emerging threats, patterns, and behaviours that may indicate fraudulent activity. Intelligence helps organisations stay ahead of evolving fraud tactics by identifying vulnerabilities, predicting potential risks, and enabling more targeted and proactive responses. Feeding detection findings back into the fraud intelligence cycle enhances this process by creating a continuous loop of learning and improvement. Each instance of detected fraud contributes valuable information that can refine the intelligence picture, adapt countermeasures, and improve future detection efficacy.

Both strategic and tactical intelligence are essential for effective fraud detection. Strategic intelligence provides a broad view of longterm trends, emerging threats, and high level patterns, allowing organisations to anticipate future risks and align their resources accordingly. Tactical intelligence, on the other hand, offers more immediate, actionable insights into specific fraud activities, helping to detect and respond to threats in real time. Strategic intelligence informs the overall fraud prevention strategy, while tactical intelligence allows for swift detection and intervention.

Feeding the findings from tactical fraud detection back into the strategic intelligence ensures that organisations continually refine their understanding of fraud tactics, making detection efforts more targeted and efficient over time.<sup>16</sup>

## E5. Audit, Compliance and Inspection Activity

Audits, compliance checks and inspections can all help identify potential instances of fraud, control weaknesses, or other issues that warrant further examination.

### Internal Audit

Internal audit services provide independent assurance to organisations, by evaluating and improving the effectiveness of governance, risk management, and controls. It ensures that policies, programmes, projects, systems, and procedures are working as intended. Internal audit feeds into detection (and counter fraud more broadly) by highlighting high risk areas and identifying specific concerns, control weaknesses or vulnerabilities in a particular department or programme which may warrant further examination from a counter fraud perspective.<sup>17</sup>

Internal audit is performed within an organisation according to its needs. Large organisations may have an internal audit department which works continuously throughout the year examining areas of importance to management, areas deemed to be high risk or those that make a contribution to effective governance or the achievement of corporate objectives. Smaller organisations might undertake a number of internal audits per year when resourcing and other business priorities allow. Internal audits may be conducted in-house or contracted out.

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

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

17 <https://www.gov.uk/government/publications/government-functional-standard-govs-009-internal-audit>

## External Audit

External audits are primarily responsible for ensuring that an organisation's financial accounts represent a true and fair view of their financial performance for the year under review and their financial position at the year end. However, where the external auditor detects fraud they will take this into account when framing their audit opinion and will report the matter to management. Similarly, regulatory bodies conduct reviews to ensure compliance with laws and industry standards, and in doing so, may uncover non-compliance issues, such as violations of anti-money laundering regulations, which could point to fraudulent activities. The National Audit Office (NAO) for example, is the UK's independent public spending watchdog. The NAO supports Parliament in holding the government to account and help improve public services through audits.<sup>18</sup>

## Compliance Checks

Compliance checks are a proactive detection method aimed at ensuring the accuracy of information held by an organisation according to defined criteria. They may be risk based or include random sampling to detect both direct and indirect fraud or errors. These checks vary based on the organisation's focus and can involve reviewing service user information, conducting unannounced site visits, and ensuring that systems and procedures function as expected. The scope can also vary by service area and may involve reconciling expenses, receipts, timesheets, verifying identity documents or performing larger-scale reviews of equipment usage, stock, or other financial elements.

## Inspections

Inspections, whether related to quality control, health and safety, or operations, can also reveal control weaknesses that may facilitate fraud. For instance, a health and safety inspection might find that safety equipment is purchased but never delivered, indicating possible procurement fraud.

## E6. Fraud Risk Assessment<sup>19</sup>

Fraud risk assessments involve the identification of fraud risks and addressing an organisation's vulnerabilities to both internal and external fraud. Detection practitioners should understand the role of fraud risk assessments and have appropriate access to fraud risk assessments. Practitioners should understand that fraud risks with no corresponding detective controls will increase the likelihood of the fraud occurring.

A fraud risk assessment should effectively identify, describe and assess individual fraud risks and these should feed into a comprehensive fraud risk assessment for the entire organisation (Enterprise Fraud Risk Assessment).

A fraud risk assessment must consider an organisation's vulnerabilities to both internal and external fraud. It is an essential element of an effective counter fraud response and should be integrated into the organisation's overall risk management approach.

All organisations should undertake

1. Enterprise Fraud Risk Assessment (EFRA)<sup>20</sup>
2. Grouped (Thematic) Fraud Risk Assessment
3. Initial Fraud Impact Assessment (IFIA)<sup>21</sup> for new policies, programmes, projects and systems

<sup>18</sup> <https://www.nao.org.uk/>

<sup>19</sup> <https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

<sup>20</sup> <https://www.gov.uk/government/publications/enterprise-fraud-risk-assessment-practice-note/enterprise-fraud-risk-assessment-practice-note.html#:~:text=An%20Enterprise%20Fraud%20Risk%20Assessment%20is%20the%20most%20general%20level,be%20different%20for%20each%20organisation>

<sup>21</sup> <https://www.gov.uk/government/publications/initial-fraud-impact-assessment-practice-note>



#### 4. Full Fraud Risk Assessment (FRAs) for the areas of highest impact

Government Functional Standard GovS 013: Counter Fraud outlines the requirements of all public body organisations and regular reviews by the Counter Fraud Function's Centre of Expertise are completed to monitor and report progress against the standard.

savings from the implementation of additional controls or ways of working

- 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
- To measure the effectiveness of the organisation's counter fraud strategy

## E7. Fraud Measurement<sup>22</sup>

Fraud Measurement is about understanding the levels of fraud and associated error that are impacting an organisation. It helps understand organisational vulnerabilities through providing insight on where fraud and error is occurring, and how much is costing the business.

The results of fraud measurement can aid detection by quantifying suspicious activities and establishing benchmarks for normal behaviour, helping to pinpoint an organisation's vulnerabilities to fraud. By systematically measuring and analysing fraud related data, organisations can fine-tune their fraud detection strategies, enhance their ability to catch fraudulent activities early, prevent losses and mitigate potential risks.

The Government Counter Fraud Profession's Fraud Measurement Standard sets out the objectives for fraud measurement activity

- To establish the vulnerabilities of the organisation to fraud
- 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
- 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
- To be able to calculate the value of fraud and error prevented, including future

## E8. Data Analytics

Organisations gather, store and use vast amounts of information, and data plays an increasingly important role in detecting and preventing fraud. Analytics and artificial intelligence (AI) can be used to process this data more effectively and efficiently. As fraudsters adapt and invent new methods to defraud, organisations should also adopt innovative ways to tackle current and emerging fraud threats. Innovations in technology present opportunities to develop insights on known areas susceptible to fraud as well as identifying new areas of possible fraud.

Data analytics is a specialist discipline involving the collection, transformation and sorting and analysing of data in order to draw conclusions, make predictions and drive informed decisions. For the purposes of the detection standard, a detection practitioner should be aware of the role and potential of data analytics in tackling fraud, with sufficient familiarity to understand basic principles and have a practical understanding of how and when they may be applied, without necessarily being an expert in their technical development or implementation.

Data analytics can be used to detect fraud by identifying suspicious patterns, anomalies and trends or flagging known high risk transactions and actors in a system. This may be particularly beneficial when dealing with high volume fraud or larger data sets where manual processing may be impractical.<sup>23</sup>

<sup>22</sup> Fraud Loss Measurement Standard available on request from GCFP

<sup>23</sup> <https://www.counterfraud.gov.au/sites/default/files/2022-06/fraud-data-analytics-leading-practice-guide.PDF>



Over time, measured data can be used to develop predictive models that can estimate the likelihood of fraud before it occurs, enabling a more proactive approach to fraud detection.

The efficiency of data analytics is dependent on the type of data available, the quality of that data and the resources available to implement the analysis of that data.

When assessing the potential use of data analytics, consideration may be given to the following:

1. What data do you have available?
2. What are you trying to find or what might you find?
3. What do you need in order to find it?
4. What are you going to do with the findings arising from the data analytics?

It is crucial that data analytics is conducted by individuals with the appropriate skills and training. All such activities should be carried out with the permission of the Data Controller and in compliance with the organisation's responsibilities under the Data Protection Act 2018 and General Data Protection Regulation (GDPR). Additionally, these activities must align with the organisation's registration with the Information Commissioner's Office. Data analytics can be applied by using or comparing both internally and externally available data sets or information.

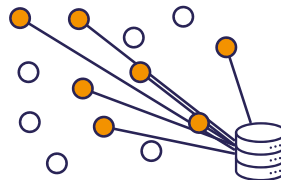
The vast array of tools that data analytics, and technology more broadly, can bring to counter fraud fall outside the scope of this standard, and its applications will vary greatly across organisations.<sup>24</sup> They can range from physical intervention tools, for example document scanning and identity verification devices, to bespoke or proprietary data analytic programmes and generative AI.<sup>25</sup>

<sup>24</sup> <https://www.counterfraud.gov.au/sites/default/files/2022-06/fraud-data-analytics-catalogue-of-techniques.PDF>

<sup>25</sup> <https://www.gov.uk/government/publications/introduction-to-ai-with-a-focus-on-counter-fraud>

## Data Analytics

New **information** and **indicators** can highlight cases of potential fraud  
**Domain knowledge** is used to **prioritise cases** for detailed examination



Improve data-driven insights, filling an organisation's gaps in knowledge

Identify process gaps that can allow fraud to occur



## Intelligence Gathering

Additional insights are used to **triage cases** and **feed into investigations**

Gather non data evidence

Target high risk cases



Direct the improvement of analysis by feeding back key insights



## Investigations

Investigations are only carried out on **highest risk cases**,  
 using all the information gathered to this point

Prepare cases against fraudsters

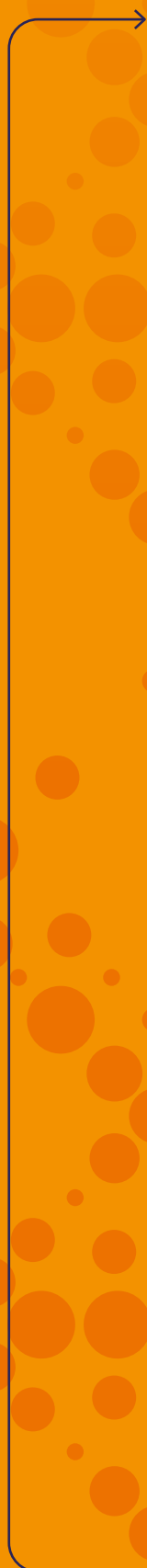
Enforces  
compliance

Takes action

Investigates



Identify the **critical information** for proving fraud



## E9. Culture<sup>26</sup>

Organisations should establish a workplace culture that encourages fraud reporting, while discouraging fraudulent, corrupt or other criminal activities. A workplace where fraud reporting is encouraged supports fraud detection as it highlights vulnerabilities and presents opportunities to detect further fraud.

Where a positive workplace culture exists, staff will be less likely to rationalise fraudulent or criminal conduct and be more responsive to identifying and reporting fraud. A positive counter fraud culture encourages staff at all levels to engage with counter fraud, bring different perspectives and propose new ideas, and be empowered to act with confidence and integrity in the way that they make decisions and work with others.

A culture built on honesty, transparency and integrity is a key organisational strength that can serve to reduce the risk of fraud from both internal and external threats. The identification of fraud should be viewed as a positive and proactive achievement. Finding fraud is a good thing, if you don't find fraud you can't fight it.<sup>27</sup>

## E10. Counter Fraud, Bribery and Corruption Training

Counter fraud, bribery and corruption training is integral to an effective counter fraud environment and culture. Educating colleagues about fraud across an organisation raises awareness of the fraud risks faced by the organisation, helping everyone to understand and recognise what fraud might look like, what to look out for and how to report any concerns. Having regular fraud, bribery and corruption training empowers all staff to feed into the wider fraud response of an organisation. Training may include<sup>28</sup>

- How counter fraud aligns with the organisation's strategic goals and values
- Why it is important
- The responsibilities for all officials to control fraud and corruption risks in their day-to-day work
- What fraud and corruption looks like, including common red flags, how to respond to the red flags, including how to report suspected fraud or corruption confidentially
- Counter fraud training content should be refreshed regularly

## E11. Communication and Engagement

Building and maintaining strong working relationships and effective communication with a range of stakeholders is crucial for fraud detection. Internally and externally, these relationships help identify key information sources, uncover gaps in data or processes, and improve collaborative efforts. By engaging with different departments, agencies, or external partners, organisations can share expertise, technical knowledge, and methodologies to detect fraud more effectively. This collaboration also helps address limitations in knowledge or resources to find mutually beneficial solutions. Whether through local, department level cooperation or longer term partnerships, fostering these relationships enhances the ability to work jointly toward positive outcomes, ultimately improving fraud detection capabilities.

## E12. Horizon Scanning

Horizon scanning is a proactive approach that involves identifying emerging threats, trends, early signs of potentially important

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

27 <https://www.gov.uk/government/publications/government-counter-fraud-functional-strategy-2024-2027>

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

developments or significant incidents that may require further investigation within an organisational context. The objective of horizon scanning is to anticipate future risks that could affect the organisation, put in controls and management information to manage emerging risks, and design and prioritise detection actions accordingly. For example, a new regulatory report might uncover a new type of fraud, prompting the need for a horizon scan to assess its relevance and potential impact. Organisations may horizon scan through technology and people to enable them to anticipate and prepare for future fraud risks. By systematically examining potential threats and opportunities, horizon scanning helps organisations detect early signs of fraud developments.

When undertaking horizon scanning consider the following

- Define the objective or purpose for the horizon scan
- Identify stakeholders and agree method for reporting back
- Set a time frame, review and end the scanning when no longer required
- Use tools for automatic feeds on keywords and location
- Agree reporting frequency
- Set up email alerts for specific subjects
- Scan media reports appropriate to organisation

## E13. Media

The media can support potential detection activity by bringing fraud and other forms of economic crime to the attention of both the public and victim organisations, either by identifying a specific issue within the organisation or within comparable organisations. This may be a result of tip-offs they received or from focussed

investigative journalism. The media and investigative journalists can play a particularly prominent role in bringing bribery and corruption issues to light.<sup>29</sup>

## E14. Legal Obligations

Those operating at all levels should be familiar with the legislative and regulatory frameworks in which they operate and the powers available to them. It is important that those most senior and accountable in the organisation understand the purpose and implications of the Acts and regulations, for example, data protection legislation and its impact on data sharing.



29 <https://doi.org/10.1787/7590ec9d-en>

# Supplementary Information

## E15. Fraud Indicators

Every type of fraud affecting the public sector will display distinct fraud indicators specific to that type of fraud. An understanding of these specific fraud indicators in a given area can enable practitioners to more quickly and accurately identify and assess discrepancies, and will be drawn from a practitioner's own experience or be informed by experts in the subject or service area. The following tool can assist in identifying fraud indicators.



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



The International Public Sector Fraud Forum provides the below high level fraud indicators<sup>30</sup>

### Fraud Indicators in Policy Design

- Systems managed across different government portfolios, service providers or jurisdictions
- Programs managed across different jurisdictions
- Opportunities for exploitation by industry or professional facilitators
- Expanding unregulated industry or expanding a regulated industry to new providers
- The need for verification or authentication of identity, particularly online
- Electronic submission, verification, claims, assessments and payments
- Low verification thresholds
- Need to deliver program quickly
- Policies developed without critical analysis for vulnerabilities
- Prioritising customer convenience
- Policies developed in isolation from area responsible for implementation
- Vulnerabilities in similar programs

30 <https://assets.publishing.service.gov.uk/media/6369038cd3bf7f75553de44e/GuideToManagingFraudForPublicBodies.pdf>

### Fraud Indicators in Internal Fraud

- Unwillingness to share duties
- Refusal to take leave
- Refusal to implement internal controls for example skipping approvals
- Replacing existing suppliers with suppliers that have an unusually close connection
- Living a lifestyle above apparent means
- Lavishing gifts on colleagues
- Failure to keep records or receipts
- Bullying colleagues, especially if the colleagues question the person's activities
- Seeking access to areas which the person should not be able to access
- Chronic shortage of cash or consistently seeking loans or advances
- Past legal or compliance problems
- Addiction problems for example gambling or drugs
- Under financial stress
- Significant personal stress for example divorce or failing business
- Disgruntled with employer
- Strong sense of entitlement

### Fraud Indicators in Contracting/Accounting

- Financial information reporting is inconsistent with key performance indicators
- Abnormally high costs in a specific cost
- Centre function
- Dubious record keeping
- High overheads
- Bank reconciliations not up to date
- Inadequate segregation of duties
- Reconciliations not performed on a regular basis
- Payments continuously just below reporting thresholds
- Duplicate invoices
- Sequential numbers on invoices
- Pricing does not adjust with changes in the value of goods or services in the market
- Owners of company not identifiable
- Owners of company with unusually close links to officials in the department
- A history of fraud in the type of contract or with the contracting organisation



## E16. After a Detection Exercise

The outcome of a detection exercise may lead to one or several possible follow-up actions depending on the outcome.

### Follow-up actions

<b>Issue communications</b>	→ Engaging with a communications team, for example, to promote successful outcomes.
<b>Amend or adjust fraud risk assessments</b>	→ When a fraud has been detected the relevant parts of the fraud risk assessments need to be reviewed and revised as appropriate.
<b>Inform intelligence</b>	→ Refer results of detection for intelligence development where the threshold is not met for full investigation.
<b>Refer for investigation</b>	→ Refer results of detection for a full investigation where information meets the threshold.
<b>Develop new or existing technology</b>	→ Develop new or existing automated processes where possible to detect further or similar instances of fraud. For example, create or update algorithms and refining monitoring techniques.
<b>Revise and strengthen policies</b>	→ Recommend changes to policies or procedures to reduce or capture instances of fraud at the earliest opportunity. Lessons learnt or redesigning to close gaps that were identified.
<b>Revise and strengthen processes</b>	→ Recommend changes to processes to reduce or capture instances of fraud at the earliest opportunity. Lessons learnt or redesigning to close gaps that were identified.
<b>Enhance prevention controls</b>	→ Recommend new and/or strengthened controls to minimise the risk that the detected fraud will reoccur.
<b>Enhance staff counter fraud training</b>	→ Educating staff as to the frauds that have been detected, why they occurred and the steps that they can take to minimise a reoccurrence of the fraud.
<b>Refine detection methods</b>	→ Detection methods may need to be refined if it has taken a long time to detect a fraud or where current techniques, methods and procedures have fallen behind recognised best practice.
<b>Trigger regular audits</b>	→ A detected fraud may trigger a local counter fraud review or a wider internal audit or compliance review to establish what happened and strengthen procedures and controls to minimise the likelihood of a recurrence.

## E17. Categories of Fraud Detection

Detection involves identifying anomalies, irregularities, or deviations that may suggest fraud. These typically fall into one of four categories

1. **Legitimate** – Valid and correct but initially appearing suspicious (including malicious allegations)
2. **False Positive** – A legitimate transaction or activity incorrectly flagged as fraudulent
3. **Fraud** – An intentional act to dishonestly make a gain or cause a loss
4. **Error** – Losses arising from unintentional events, processing errors and official errors. Where on the balance of probabilities fraud has not occurred, then it would be classified as an error

It is important to distinguish between these categories at the appropriate time. Depending on the organisation's structure, a detection practitioner might conduct preliminary inquiries to assess and triage cases or pass all discrepancies to others for further evaluation.

The timing of differentiation depends on the specific circumstances. For instance, data analytics may quickly differentiate transactional or quantitative fraud from errors or legitimate activities. However, when discrepancies arise it is important to assess whether an anomaly is a false positive before concluding that fraud may be present. Acting on a false positive could have a number of consequences for example, damage to reputations and legal challenges.

Practitioners should appropriately distinguish between potential fraud, error, false positives and legitimate activity, based on their role and level of responsibility. When internal errors are identified, it is best practice to communicate these to the relevant departments to rectify the issue, cleanse organisational data, and

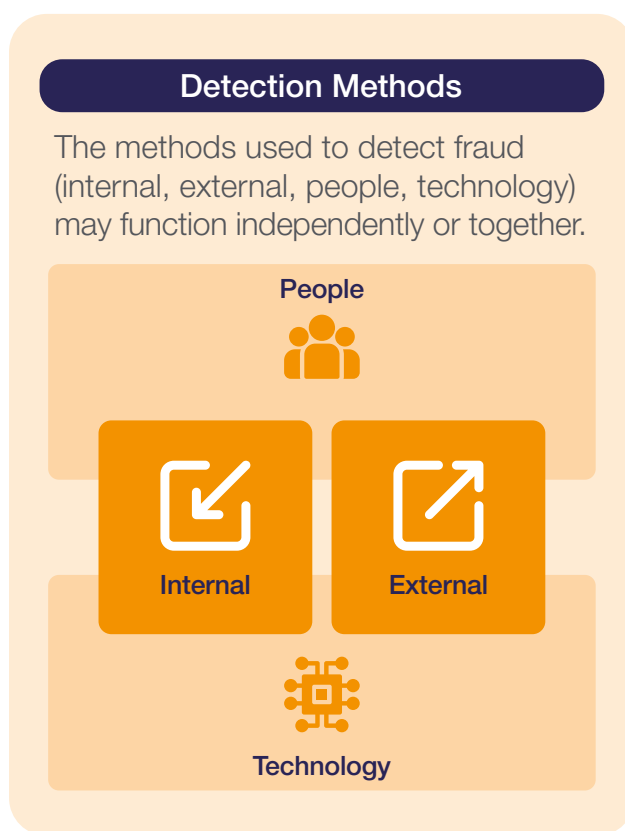
prevent future false positives.

## E18. Fraud Detection Methods

The methods used to detect fraud will depend on the area and nature of the fraud being detected, as well as the information or data available, all of which will vary within and across organisations. The use of specific detection techniques may be dependent on the availability of specialists within an organisation. However, all detection practitioners should be aware of, and explore, the potential methods available in order to consider applying them directly in their field, or to engage the required resources or specialists who can. As with any counter fraud work, there must be appropriate mechanisms in place to ensure all activity is conducted in accordance with the law. Fraud detection methods can be broadly classified into internal and external methods derived from technology or people.

- **Internal** methods of detection are those originating from within an organisation and can range from standalone proactive exercises examining a specific area, to reactively responding to internal events
- **External** methods of detection are those originating from outside an organisation which an organisation responds to. Although the methods are generally reactive (with exceptions), organisations can nonetheless be proactive in how they promote and harness them
- **Technology** based methods present opportunities to develop insights on known areas susceptible to fraud as well as identifying new areas of possible fraud. Many tools integrate both prevention and detection capabilities and are capable of handling vast data sets to identify patterns of fraudulent behaviour. Technology still requires oversight and the human element of detection cannot be ignored

- **People** based methods, for example, fraud reporting is an important way in which frauds are detected.<sup>31</sup> Effective fraud detection combines human judgement with specialist knowledge and experience to scrutinize the outputs of technology methods. There will always be occasions when human based detection is the only or most appropriate approach



## E19. Fraud Control Testing

Within fraud detection consideration may be given to the following

### Pressure Testing

Pressure testing involves examining fraud controls and systems under various conditions to measure their effectiveness and uncover control gaps or vulnerabilities. In some circumstances this can involve covert testing, where officials simulate methods used by fraudsters to identify how controls respond and how they could be circumvented by malicious actors. Pressure testing is an effective method to proactively identify and eliminate vulnerabilities that could lead to fraud. By understanding where processes, systems, or controls are susceptible, organisations can make informed decisions to mitigate fraud risks.

Benefits of pressure testing<sup>32</sup>

- Find weaknesses or gaps in controls that individuals or criminal groups could exploit
- Improve understanding of different functions, programs and risks within an organisation
- Provide assurance that an organisation's fraud risks are being effectively managed
- Develop closer working relationships between counter fraud officials and stakeholders
- Increase awareness of fraud across an organisation and help officials to acknowledge the risk of fraud and the potential for vulnerabilities
- Maintain program integrity during organisational change

### Control Testing

Control testing involves the assessment and evaluation of controls, processes, and procedures to detect, prevent and deter fraud. It aims to provide assurance that public funds

<sup>31</sup> <https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf>

<sup>32</sup> <https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/a-guide-to-pressure-testing-html>

are managed appropriately. It also helps public bodies examine the effectiveness of their fraud controls using different testing methods. It involves applying creative and critical thinking and examining processes and systems from the perspective of a fraudster. It also involves employing a range of different testing methods to examine how controls work, eliminate blind spots to uncover vulnerabilities and challenge unthinking assumptions around what are effective ways to manage fraud by public bodies.<sup>33</sup>

Control Testing provides an assessment of whether the counter fraud measures in place are functioning as intended, providing assurance that fraud risks are being appropriately managed.

The benefits of fraud control testing go well beyond identifying control vulnerabilities. Fraud control testing<sup>34</sup>

- Enhances operational efficiency
- Enhances operational effectiveness
- Supports the prevention of financial loss
- Increases fraud awareness
- Enables and supports fraud measurement and detection activities
- Provides insight that can reduce the cost of controls
- Preserves public trust

## E20. Fraud Detection Software<sup>35</sup>

Fraud detection software can be deployed either as a standalone application across the entire organisation or as specialised software within specific departments, tailored to the unique requirements of a service area. In both cases, collaboration with the relevant system administrators is essential to ensure appropriate access and reporting functionalities. Implementation must also comply with relevant data governance policies.

Fraud detection software often uses machine learning which allows it to learn and adapt to new fraud schemes making it effective in detecting fraud. Fraud detection software can handle vast amounts of data and transactions and has the ability to detect fraud early therefore preventing losses due to fraud.

Fraud detection software can assist in detecting fraud by

- Automatically reviewing system access logs to detect unauthorised access
- Scanning for suspicious changes to client or provider bank accounts, such as common accounts being used
- Monitoring the use of compromised personal identity information
- Monitoring for suspicious changes to provider bank accounts, including matching the user or recipient to the bank account
- Analysing bulk data sets to identify suspicious patterns and anomalies
- Detecting irregularities in online traffic through, for example, device and voice detection software

33 [https://assets.publishing.service.gov.uk/media/650c652e27d43b000d375b2a/3340\\_IPSFF\\_FCTF-01\\_Fraud\\_Control\\_Testing\\_Framework\\_V5\\_1\\_1\\_.pdf](https://assets.publishing.service.gov.uk/media/650c652e27d43b000d375b2a/3340_IPSFF_FCTF-01_Fraud_Control_Testing_Framework_V5_1_1_.pdf)

34 <https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/fraud-control-testing-framework-fctf-01-html#appendix-c--the-benefits-of-fraud-control-testing>

35 Adapted from <https://www.counterfraud.gov.au/fraud-countermeasures/fraud-detection-software>

## E21. System Monitoring

System monitoring continuously observes and analyses systems in real time to search for anomalies which may indicate unusual or unexpected patterns or events and can have a wide range of applications. The precise nature of the monitoring will depend on the system or data set, and development and implementation is likely to be in collaboration with an organisation's IT department or a third party provider. An example of system monitoring would be if an employee attempted to process multiple high-value payments just below the approval threshold, the system could flag this activity for further investigation. Proactive systems monitoring in this way can improve the performance and effectiveness of fraud detection.

## E22. Data Matching

Data matching is a type of data analysis which, in the context of detection, involves establishing commonalities or discrepancies between data sets to identify fraud. These data sets can be internal, external, or both and can help identify a number of fraud types to enable fraud detection and prevention. For example data matching can be used to identify service user fraud, where an individual is found to be receiving the same service from multiple providers, or discrepancies may be found in one service area which may preclude them being eligible for a service in another.

An example of data matching is the National Fraud Initiative (NFI), a government data matching exercise which matches electronic data within and between public and private sector bodies to prevent and detect fraud.<sup>36</sup>

Effective data matching exercises are dependent on the quality of data available to reduce instances of false positives and errors. Such exercises should take into account the organisational risk areas,

consider what data is held and what other internal or external data sets might assist in identifying fraud.

As with other detection methods, the outputs of data matching exercises may need to be managed on a risk assessed basis, depending on volume and available resources. However, the results assessed as low risk should also be reviewed periodically to check for potential unknown or novel fraud types.

When undertaking data matching and analytics exercises, organisations must

- adhere to legislative requirements and relevant codes of practice
- consider and test the validity of any results
- consider the ethical implications associated with their activities

Lawfully sharing data can be a powerful tool to detect fraud and corruption. Detection is crucial to revealing fraud and other forms of economic crime and enabling entities to effectively deal with them, thereby minimising the consequences through earlier intervention.<sup>37</sup>

## E23. Exception Reporting

An exception report highlights activities or transactions which vary from an established norm in a given area, generally over a period of time rather than live or continuous monitoring. Spotting things that look unusual or out of place is an important way of detecting fraud and identifying anomalies. Comparing actual performance to expected outcomes can help identify potential risks before they become issues. Exception reports have a wide variety of possible applications and can be regular, business as usual activities or be the basis of a standalone detection exercise.

Lack of exception reporting may lead to

<sup>36</sup> <https://www.gov.uk/government/publications/national-fraud-initiative-case-studies/nfi-public-sector-case-studies>

<sup>37</sup> <https://www.counterfraud.gov.au/sites/default/files/2024-06/info-sheet-element-6-detecting-fraud-and-corruption.pdf>



- Fraud or corrupt activity going unnoticed or unchallenged
- Increased fraud risk
- Increased losses due to fraud

Exception reporting can be applied to various types of events or transactions to flag unusual frequencies, locations, high or low turnovers or multiple failed attempts of the given event, for example

- Unusually high or low value transactions in relation to payment cards, invoices or programs
- Payments or claims repeatedly just below reporting thresholds
- High value or volume expenses being claimed or paid
- Excessive ordering of assets
- Staff who have made more claims than usual within a month

Ensuring the effectiveness of exception reporting

- Ensure that the exception parameters are appropriate and not widely known to prevent manipulation of processes
- Review who has access to exception reports and confirm that those who review exceptions are separate from processing teams
- Review a sample of reports to see if they are clear, relevant to the user and would help detect fraud
- Continually review the content of exception reports to ensure that they continue to meet business needs

## E24. Random Sampling<sup>38</sup>

Random sampling can be an effective tool in fraud detection by selecting a subset of data for review and analysis, helping to uncover anomalies or patterns that may indicate fraudulent activity. A sample size refers to the number of observations or data points included in the sample. A statistically valid sample size reduces the margin of error and increases the accuracy of the conclusions drawn from the sample. A higher confidence level typically requires a larger sample size. A random sampling process for fraud detection may include

- **Data Collection** – Gather a comprehensive dataset that includes data representative of the processes or transactions you want to analyse for fraud
- **Random Sample Selection** – Use statistical techniques to randomly select a subset of records from the larger dataset. The randomness ensures that no bias affects the selection process, allowing for an unbiased examination of the data
- **Examine Patterns and Anomalies** – Analyse the randomly selected records for signs of unusual behaviour, such as
  - Transactions outside normal operating hours
  - Inconsistent transaction amounts
  - Repeated transactions to the same account
  - Duplicate or missing data entries
  - Transactions outside normal operating parameters
- **Apply Fraud Detection Techniques** – Use analytical methods, such as data mining, statistical analysis, and machine learning, on the sample to identify potential fraudulent transactions. These techniques help highlight outliers or unusual patterns

<sup>38</sup> Random Sampling is covered in more detail in the GCFP Fraud Measurement Core Discipline available on request from GCFP.



that could be indicative of fraud

- **Expand Analysis** – If suspicious activities are detected in the random sample, you can expand the analysis to the entire dataset or to specific areas that show higher risk, applying targeted scrutiny or more advanced fraud detection tools
- **Cost-Effective Screening** – Since random sampling requires only a portion of the data to be analysed, it provides a cost-effective way to monitor large datasets for potential fraud without the need for a full scale review
- **Continuous Monitoring** – Incorporate random sampling as a regular part of fraud detection efforts. Periodic sampling can serve as a deterrent to fraudulent behaviour and ensure that emerging risks are quickly identified

By applying random sampling, organisations can efficiently monitor their data for fraud while maintaining a balanced use of resources.

## E25. Evolving Technology

As fraudsters adapt and change to develop new methods to defraud, organisations should also adopt innovative ways to tackle current and emerging fraud threats. Innovations in technology present opportunities to develop insights on known areas susceptible to fraud as well as identifying new areas of possible fraud.

Technological tools can integrate both prevention and detection capabilities. For example, transaction monitoring systems can be designed to prevent unauthorised transactions (prevention) while also identifying patterns of fraudulent behaviour (detection).

The rise of artificial intelligence (AI) presents a huge opportunity for those working in the public sector to detect and prevent fraud, using large quantities of information and data. AI can range from predictive algorithms

and machine learning all the way through to complex robotics. This supports the modern fraud approach focussing on a deep understanding of risk and the use of data and intelligence to find fraud.<sup>39</sup>

When using data and AI it is important that users consider potential strategic, operational and reputational risks that may arise if key principles, ethical considerations and data management processes are not adhered to. Technology still requires oversight and the human element of detection cannot be ignored.

Using data matching, analytics and AI to find indicators of fraud drives efficiency in counter fraud activities.

Proactive monitoring of emerging technologies allows for continuous investment in, and enhancement of, fraud detection capabilities, for example, by harnessing the power of artificial intelligence. Embracing a mindset of innovation and experimentation, exploring new technologies, analytical approaches and collaborative partnerships will ensure fraud detection techniques stay ahead of increasingly sophisticated fraud schemes.

---

39 <https://www.gov.uk/government/publications/introduction-to-ai-with-a-focus-on-counter-fraud>

## F. Further Guidance

### F1. Further Information

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

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

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

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

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

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

[GCFP@cabinetoffice.gov.uk](mailto: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](mailto:Correspondence@giaa.gov.uk)

## F2. Products From Other Standards

Product	GCFP Standards
Annual Action Plan (including the operational management cycle)	Leadership, Management and Strategy Standard and the Fraud Prevention Standard
Communications Plan	Leadership, Management and Strategy Standard and the Fraud Prevention Standard
Counter Fraud Policy	Leadership, Management and Strategy Standard
Fraud Awareness Training	Government Functional Standard GovS 013: Counter Fraud and the GCFP Standard for Counter Fraud Culture Practitioners
Fraud Measurement, Calculation and Reporting process	Fraud Measurement Standard
Fraud Risk Assessment and Plan <ul style="list-style-type: none"> <li>• organisational (enterprise) fraud risk assessments</li> <li>• thematic (grouped) fraud risk assessments</li> <li>• initial fraud impact assessments (IFIAs)</li> <li>• full fraud risk assessments</li> </ul>	Fraud Risk Assessment Standard
Fraud Risk Management Cycle	Fraud Risk Assessment Standard
Lessons Learned Reviews	Fraud Prevention Standard
Protocol Documents including MOU and partnership agreements	Fraud Prevention Standard
Strategy, counter fraud strategy and fraud control strategy which include the strategy management cycle	Leadership, Management and Strategy (LMS) Standard <sup>40</sup>

40 LMS Standards can be obtained by emailing [GCFP@cabinetoffice.gov.uk](mailto:GCFP@cabinetoffice.gov.uk)

## F3. Functional Standards<sup>41</sup>

Functional Standards	Standard Number
 <p><b>Government functions</b> – sets expectations for the direction and management of functions across government</p>	<a href="#">GovS 001</a>
 <p><b>Project delivery</b> – sets expectations for the direction and management of portfolios, programmes and projects in government</p>	<a href="#">GovS 002</a>
 <p><b>Human Resources</b> – sets expectations for the leadership and management of human resources across government</p>	<a href="#">GovS 003</a>
 <p><b>Property</b> – sets expectations for the management of corporate functions across government</p>	<a href="#">GovS 004</a>
 <p><b>Digital, Data and Technology</b> – sets out how all digital, data and technology work and activities should be conducted across government</p>	<a href="#">GovS 005</a>
 <p><b>Finance</b> – sets expectations for the effective management and use of public funds</p>	<a href="#">GovS 006</a>
 <p><b>Security</b> – sets expectations for the planning, delivery and management of government security activities</p>	<a href="#">GovS 007</a>

<sup>41</sup> <https://www.gov.uk/government/collections/functional-standards>

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

## F4. Further Reading

### **Fraud Prevention Standard for Counter Fraud Professionals**

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

### **Fraud Measurement core discipline**

Please contact [GCFP@cabinetoffice.gov.uk](mailto:GCFP@cabinetoffice.gov.uk)

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

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

### **Professional standards and guidance for fraud risk assessment in government**

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

### **GCFP standard for the counter bribery and corruption professional**

<https://www.gov.uk/government/publications/a-standard-for-the-counter-bribery-and-corruption-professional>

### **Enterprise Fraud Risk Assessment Practice Note**

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

### **Initial Fraud Impact Assessment Practice Note**

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

### **Counter Fraud Strategy Practice Note**

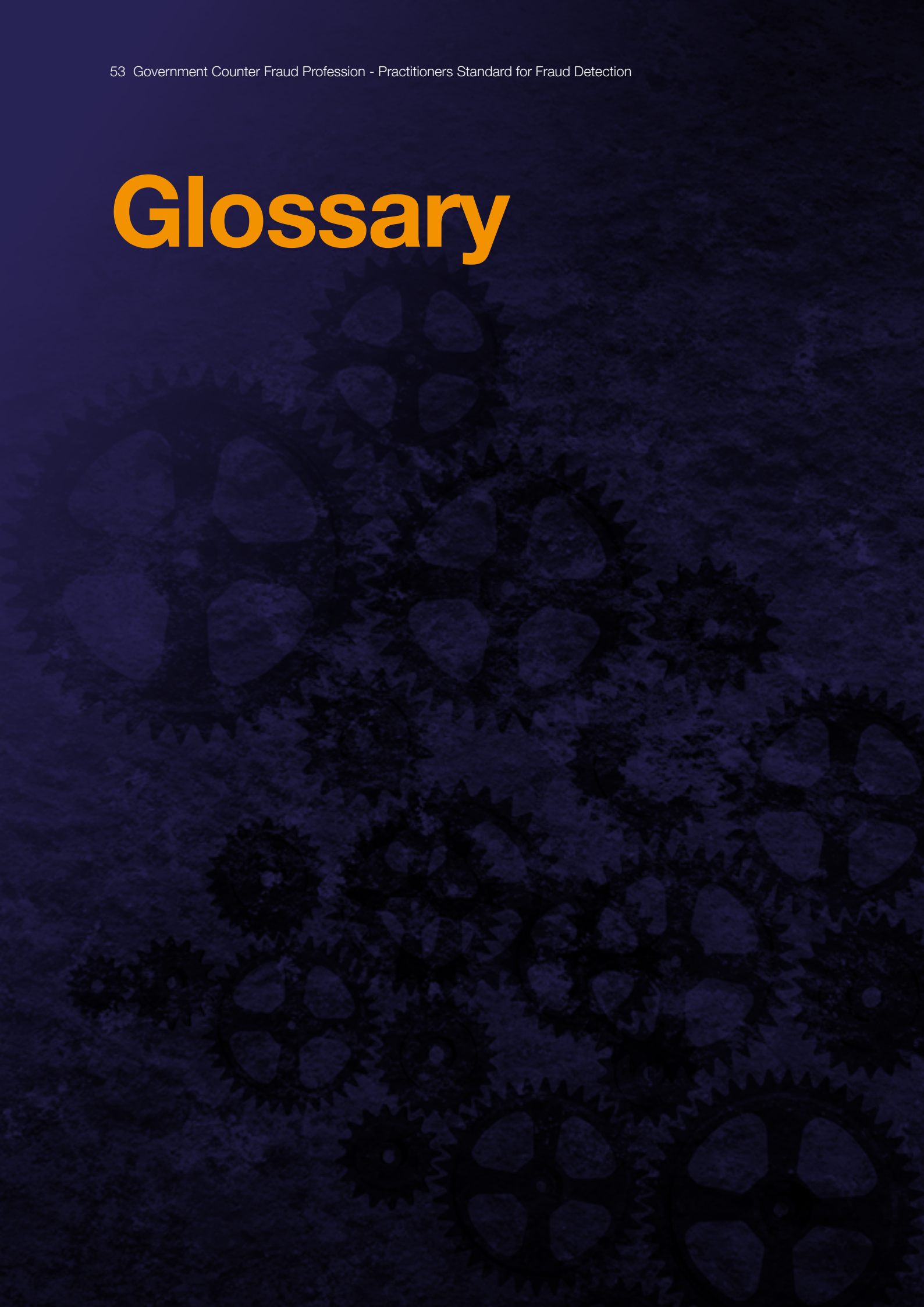
<https://www.gov.uk/government/publications/how-to-counter-bribery-and-corruption-practice-note>

### **Counter Bribery and Corruption Practice Note**

<https://www.gov.uk/government/publications/how-to-counter-bribery-and-corruption-practice-note>



# Glossary





# Glossary

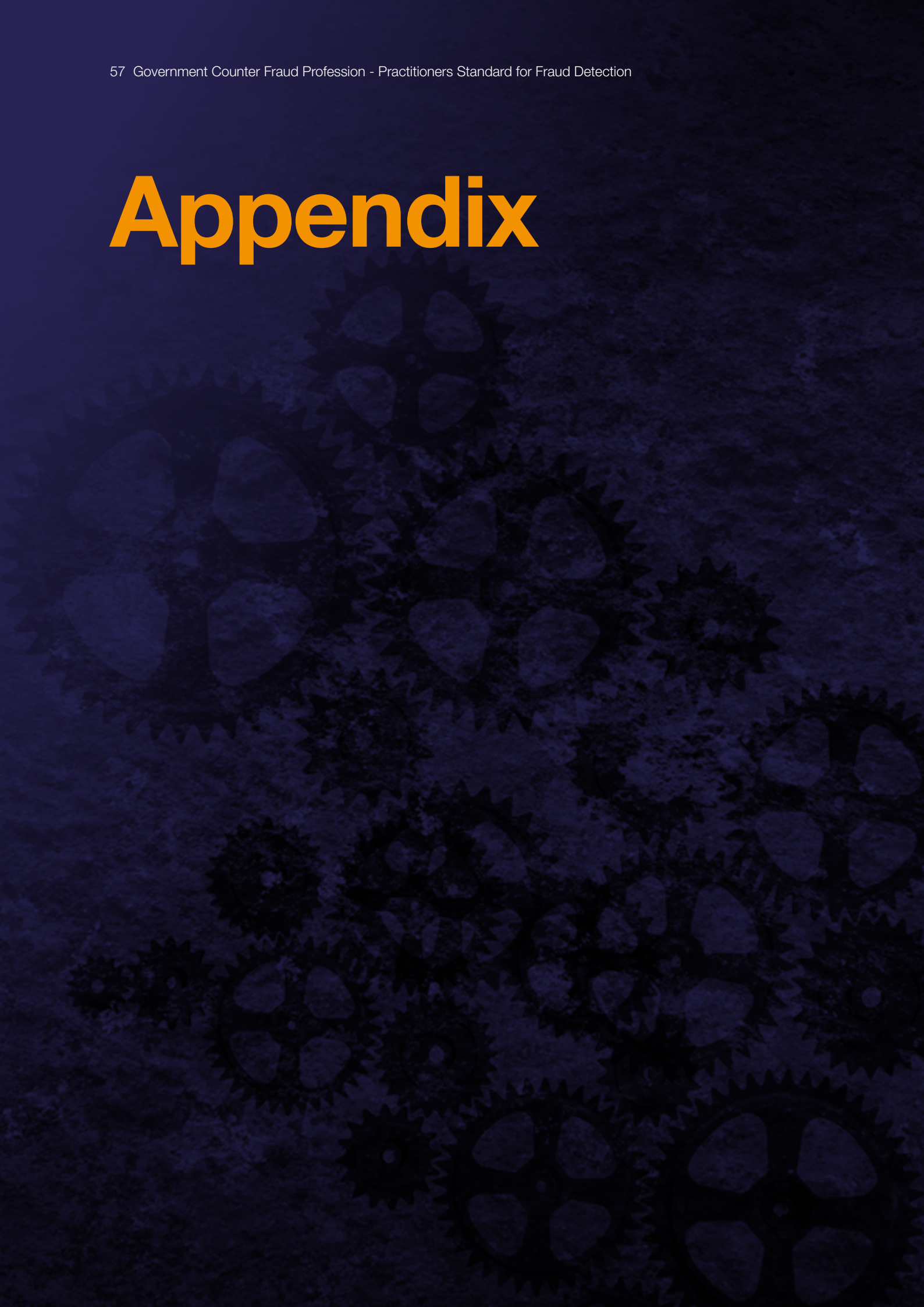
Frequently used terms	Definition
<b>Ability</b>	Skill / proficiency in a particular area
<b>Apply</b>	Make use of a skill/knowledge
<b>Awareness</b>	Knowledge of a fact
<b>Bribery</b>	Offering, promising or giving a financial or other advantage to induce or reward improper performance or the request or receipt of such an advantage. It includes the corporate offence of failing to prevent bribery
<b>Categories</b>	Defined combinations of elements, which show the expected knowledge, skills and experience for each core discipline. These enable a common assessment of skills and draw a distinction of those with a level of skill, and those without
<b>Competency Framework</b>	Group of elements found in core or sub disciplines. Grouped together, with varying levels of knowledge, skills and experience required
<b>Competency levels</b>	Used to identify progression within the standards and competencies. The competency levels are Foundation and Practitioner
<b>Core Components</b>	Behind each core and sub disciplines there are high components outlining knowledge, skills and experience required
<b>Core Disciplines</b>	Areas of expertise, knowledge, skills and experience that are needed for an effective counter fraud response. They are not people role or category specific
<b>Corruption</b>	Corruption is the abuse of entrusted power for private benefit that usually breaches laws, regulations, standards of integrity and/or standards of professional behaviour
<b>Demonstrate</b>	Show something and explain how it works
<b>Describe</b>	Give a report on how something is done or what something is like
<b>Design</b>	Make or draw plans for something

Frequently used terms	Definition
<b>Discuss</b>	Consider and offer an interpretation or evaluation of something or give a judgement on the value of arguments for and against something
<b>Error</b>	Is a similar occurrence to fraud, but where the elements of dishonesty or intent (see definition of fraud) are missing or cannot be proved. However, error also results in losses to public funds and for the purposes of this standard, is considered alongside fraud
<b>Evaluate/Assess</b>	Judge or calculate the quality, importance, amount, or value of something
<b>Explain</b>	Make something easier to understand by giving information about it and/or give a reason for an action
<b>Fraud</b>	Defined in the Fraud Act 2006. The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position
<b>Fraud Control cluster</b>	The Fraud Control cluster incorporates the Fraud Risk Assessment, Fraud Prevention, Fraud Detection, Counter Fraud Culture and Fraud Loss Measurement disciplines enabling the development of a career pathway for the counter fraud control practitioner
<b>Fraud deterrence</b>	The act of discouraging fraud by being clear of consequences. Sending out the message that committing fraud has adverse consequences for fraudsters, victims and society
<b>Fraud prevention</b>	To stop the likelihood and reduce the impact of fraud. To create an anti-fraud culture in which people and processes work together to minimise fraud risk
<b>Fraud risk assessment</b>	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
<b>Horizon scanning</b>	Exploring what the future might look like to understand uncertainties better. Horizon scanning helps organisations analyse whether it is adequately prepared for potential opportunities and threats. This helps ensure that policies are resilient to different future environments

Frequently used terms	Definition
<b>Identify</b>	Recognise a problem, need, fact, or other item and show that it exists
<b>Inherent risk</b>	Also defined as gross risk, is the risk to an organisation assuming there are no controls in place
<b>Know/ Knowledge</b>	Provide evidence of factual information or awareness gained through experience or education
<b>National Audit Office (NAO)</b>	The UK's independent public spending watchdog. The NAO supports Parliament in holding the government to account and in helping improve public services through high-quality audits
<b>Recognise</b>	Show from knowledge
<b>Residual risk</b>	Also defined as net risk, or fraud risk exposure, it is the risk remaining once the risk response has been successfully applied
<b>Risk</b>	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
<b>Risk appetite</b>	The amount of risk the organisation is willing to accept at the enterprise level, which manifests itself in the type and number of activities and associated risks that the organisation is willing to undertake
<b>Risk tolerance</b>	The threshold levels of risk exposure and target levels of incidences and losses that, with appropriate approvals, can be exceeded but which, when exceeded, will trigger some form of response for example, reporting the situation to senior management
<b>Subdisciplines</b>	Areas of additional knowledge, skills and experience that enhance capability in those areas across a number of core disciplines.
<b>Summarise</b>	A brief statement of the main points
<b>Threat</b>	A person or group, object or activity that has the potential to cause harm to the achievement of the organisation's objectives. It takes into account capability and intent to do so. * "can be described as" is used throughout this standard, where multiple definitions are available
<b>Understand/ Interpret</b>	Provide the intended meaning or cause of something



# Appendix



# Appendix 1 - Full Competency Framework

## 1. Counter Fraud, Bribery and Corruption Knowledge

Knowledge of fraud offences and typologies. Understanding the fraud landscape, why fraud is committed and its impact, in order to detect fraud

	Foundation	Practitioner
1.1	Explain the relevant legislation and offences for fraud	Demonstrate and apply the relevant legislation and offences for fraud
1.2	Explain different fraud, bribery, and corruption typologies and vulnerabilities across an organisation	Demonstrate knowledge of fraud, bribery, and corruption typologies and vulnerabilities across an organisation
1.3	Summarise why fraud, bribery and corruption are committed across the public sector and its impact across society	Demonstrate knowledge of why fraud, bribery and corruption are committed across the public sector and its impact across society
1.4	Recognise fraud landscape, scale and impact	Demonstrate knowledge of fraud landscape, scale and impact

## 2. Organisational Knowledge

### Knowledge of organisational structures and fraud response

	Foundation	Practitioner
2.1	Recognise how an organisation is structured, including roles and responsibilities relating to counter fraud	Demonstrate knowledge of how an organisation is structured, including roles and responsibilities relating to counter fraud
2.2	Describe the range of internal stakeholders within an organisation who can support fraud detection	Demonstrate knowledge of the range of internal stakeholders within an organisation who can support fraud detection
2.3	Summarise the organisational fraud risks and controls and how these impact on detection and detection methods	Apply knowledge of the organisational fraud risks and controls and how these impact on detection and detection methods
2.4	Recognise the contribution that fraud detection makes to effective fraud deterrence	Demonstrate an understanding of the contribution that fraud detection makes to effective fraud deterrence



### 3. Detection Methods

#### Knowledge and understanding of methods of detection and controls and how to apply them effectively

	Foundation	Practitioner
3.1	Explain the difference and connection between Fraud Detection, Investigation, Intelligence and Fraud Prevention	Demonstrate an understanding of the difference and connection between Fraud Detection, Investigation, Intelligence and Fraud Prevention
3.2	Summarise the different stages of the Fraud Detection Model and how these feed into and inform detection	Apply the different stages of the Fraud Detection Model and explain how these feed into and inform detection
3.3	Recognise the difference between proactive and reactive detection	Demonstrate an understanding of the difference between proactive and reactive detection
3.4	Explain the different detection techniques, methods and tools within the organisation	Demonstrate the application of detection techniques, methods and tools within the organisation, whilst actively seeking innovative ways to improve detection
3.5	Recognise the different types of data held by an organisation which can be used to detect fraud	Demonstrate an understanding of the different types of data held by an organisation which can be used to detect fraud
3.6	Summarise the factors which affect the quality of both the data and its analysis	Demonstrate an understanding of the factors which affect the quality of both the data and its analysis
3.7	Recognise the role of data analytics in fraud detection and evaluation	Demonstrate an understanding of the role of data analytics in fraud detection and evaluation and how it may be applied
3.8	Summarise the different types of audit, compliance and inspection activity and how these can assist fraud detection	Demonstrate an understanding of the different types of audit, compliance and inspection activity and how these can assist fraud detection
3.9	Describe how to create a fraud detection plan	Demonstrate the ability to create a fraud detection plan
3.10	Summarise how to use external data to support fraud detection	Demonstrate the ability to use external data to support fraud detection

## 4. Evaluation

Understanding how to evaluate detection outputs to identify appropriate next steps, and improve controls, methods and responses

	Foundation	Practitioner
4.1	Summarise the continuous Improvement Detection Framework	Demonstrate how to apply the continuous Improvement Detection Framework and identify opportunities for improving fraud control methods and responses as new risks emerge
4.2	Recognise the outcomes of detection and differentiating between potential fraud, error, and legitimate activities	Demonstrate how to assess and interpret the outcomes of detection by recognising and differentiating between potential fraud, error, and legitimate activities
4.3	Explain appropriate options and next steps for detection outcomes	Demonstrate the use of appropriate options and next steps for detection outcomes
4.4	Recognise how to create a report of detection activity	Demonstrate the ability to create a report of detection activity undertaken to record and communicate detection findings and recommendations
4.5	Summarise sources of information which inform the detection of fraud	Demonstrate the ability to identify, continually develop and refresh sources of information which inform the detection of fraud

## 5. Engagement and Communication

**Building and maintaining relationships with a range of stakeholders and understanding the internal and external communication landscape to inform and improve detection**

	Foundation	Practitioner
5.1	Describe a range of communication channels and techniques to promote fraud detection across the organisation	Demonstrate how to use a range of communication channels and techniques to promote fraud detection across the organisation
5.2	Describe external environment around emerging risks that could impact detection within the organisation	Demonstrate awareness of the external environment around emerging risks that could impact detection within the organisation
5.3	Recognise how to build and maintain stakeholder relationships through a range of communication mechanisms to identify and detect fraud	Demonstrate how to identify, build and maintain stakeholder relationships through a range of communication mechanisms to identify and detect fraud
5.4	Explain when to work collaboratively with relevant internal and external stakeholders and to bring in specialists from inside or outside the organisation	Demonstrate the ability to work collaboratively with relevant internal and external stakeholders and be able to identify when to bring in specialists from inside or outside the organisation
5.5	Recognise how to communicate the findings and outcomes of detection activities	Demonstrate how to effectively communicate the findings and outcomes of detection activities







Public Sector  
Fraud Authority

