



Government
Counter Fraud
Profession

Operated by the Public Sector Fraud Authority

Government Counter Fraud Profession

Fraud Prevention Standard for Counter Fraud Professionals

July 2023

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

Public Sector Fraud Authority

Publication date: July 2023

© Crown copyright July 2023

Produced by the Public Sector Fraud Authority.

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

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

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

Contents

A. Professional Standard and Competencies for the Fraud Prevention Discipline	5
A1. Purpose	5
A2. Introduction	6
A3. The Benefits of Preventing Fraud	6
A4. How This Document is Structured	7
A5. Feedback and Further Information	7
A6. Government Functions (UK)	8
A7. Public Sector Fraud Authority (PSFA)	9
A8. Government Counter Fraud Profession	10
A9. Government Counter Fraud Framework	10
A10. Roles and Responsibilities	13
A11. Key Components Explained	14
A12. Competency Levels	16
A13. Understanding Categories	16
B. Fraud Prevention Professional - Competency Framework	17
C. Guidance on Processes	27
C1. Introduction	27
C2. Proactive Prevention Approach	28
C3. Proportionality	28
C4. Develop or Amend Legislation, Policy or Working Practices	29
C5. Fraud Risk Management Cycle	30
C6. Counter Fraud Strategy	32
C7. Action Plans for Risk Mitigation	32
C8. Prevention Controls	33
C9. Types of Controls	34
C10. Primary, Secondary and Tertiary Controls	35
C11. Control Testing	36
C12. Pressure Testing	37
C13. Test and Learn	38
C14. Prevention Methodologies	39
C15. Business Process Mapping	43
C16. Business Analysis, and the Use of Data Analytics	44
C17. Stakeholders	46
C18. Behavioural Science	47
C19. Deterrence	47
C20. Communications	49
C21. Maximise the Effect of Fraud Messaging	50
C22. Measure, Monitor and Evaluate Effectiveness	50

D. Guidance on Products	52
D1. Introduction	52
D2. Products for Fraud Prevention Found in Other Government Counter Fraud Professional Standards	53
D3. Business Process Mapping	55
D4. Protocol Documents	57
D5. Control Assessment Tool	58
D6. Using Root Cause Analysis	60
D7. Cost Benefit Analysis	61
D8. Lessons Learnt Reviews	62
D9. Behavioural Science Models in Communication	63
D10. Other Sources of Information	64
E. Guidance for Organisations - Approved Professional Practice	65
E1. Introduction	65
E2. The Government Functional Standard - GovS 013 Counter Fraud	65
E3. Fraud Prevention Programme	66
E4. Fraud Prevention – Assurance Requirements	67
E5. Fraud Awareness Training	68
E6. Prevention Requirements in Addition to GovS 013	68
E7. Bribery Act 2010 (UKBA) Section 7 Failing to Prevent Bribery	68
E8. Counter Fraud Culture	69
E9. Strategic Threat Assessment	71
E10. Prevention by Design	72
E11. Lessons Learnt Reviews	73
E12. Communications Strategy	74
E13. Data and Analytics	75
Glossary	77

A. Professional Standard and Competencies for the Fraud Prevention Discipline

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 organisations' counter fraud work. Their aim is:

- to describe the knowledge, skills and experience (professional standards and competencies) needed for an individual to achieve practitioner level in counter fraud work in their desired discipline - 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 should seek to put in place in the organisation to deliver the discipline effectively

The organisational guidance, also known as 'Approved Professional Practice', can also be referenced when considering what should be in place in an organisation in order to use this discipline effectively.

These standards form the basis of the Prevention and Deterrence discipline that is being established within government. To be acknowledged as a counter fraud professional, these standards will have to be met. Guidance is being developed and will be made available on Civil Service Learning counter fraud pages regarding how you can be recognised as a member of the Government Counter Fraud Profession (GCFP).

These standards have been developed in conjunction with a range of stakeholders, including the Commonwealth Fraud Prevention Centre (CFPC) in Australia. This is the first GCFP Standard to be launched internationally, with a common focus on preventing fraud and reducing the impact fraud has on public services.

This document focuses on an individuals' fraud prevention capability.

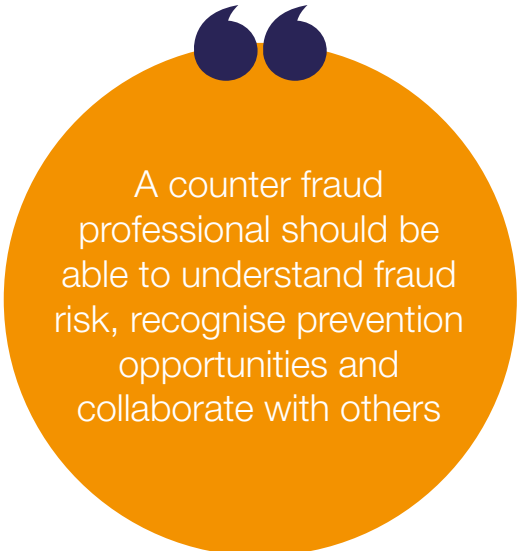
The professional standards and competencies are not intended to cover every eventuality or every specific issue that may arise and should be adapted to the organisation's resources and fraud risk profile.

A2. Introduction

A counter fraud professional should be able to understand fraud risk, recognise prevention opportunities and collaborate with others to design, implement and evaluate controls.

Fraud has an impact at a personal, organisational and societal level;

- at a personal level, it can cause anxiety, depression, a loss of money and potential injury from goods and services that are not fit for purpose
- at an organisational level, it can cause significant financial losses, a loss of employment, lower staff morale, reputational damage and a loss of public confidence in the public body concerned
- at a societal level, it can lead to the loss of large sums to the economy, higher public spending, an increase in national debt, an increase in pressure on law enforcement and can fund other forms of crime such as terrorism



A counter fraud professional should be able to understand fraud risk, recognise prevention opportunities and collaborate with others

A3. The Benefits of Preventing Fraud

✔ Improves the effectiveness and integrity of government services

Payments and services are delivered to citizens who need them - not to fraudsters

✔ Reduces administrative costs to the government

Fraud adds to the cost of programmes and services that taxpayers pay for, such as costly investigations and prosecutions

✔ Reassures the public

The government is serious about protecting the integrity of its services and remains vigilant against fraud

✔ Protects vulnerable citizens

Those who rely on government services, such as the elderly, the vulnerable, the sick and the disadvantaged, are often the ones most harmed by fraud. Fraud can have a devastating and compounding effect on victims; amplifying the disadvantage, vulnerability and inequality they suffer

✔ Reduces debt

Fraud can raise the level of debt for service users. An increase of debt can provide a greater motivation to commit further fraudulent actions

A4. How This Document is Structured

This document contains the following:

- **The Competency Framework** outlining the knowledge, skills and experience required by those undertaking fraud prevention to operate effectively, and how these develop through the competency framework levels: Trainee, Foundation and Practitioner.
- **Guidance for professionals** includes:
 - **process guidance** describing the recommended processes to implement fraud prevention processes
 - **product guidance** setting out the recommended guidance on developing good quality outputs in relation to fraud prevention
 - **organisation guidance** - Approved Professional Practice¹ (APP) is the official source of professional practice for the Government Counter Fraud Profession (GCFP) - it has been agreed as best practice and should be followed by all counter fraud professionals and their organisations

The standards have been created, reviewed and agreed by the Government Counter Fraud Profession 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 group² (CSAG).

A5. Feedback and Further Information

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

If you would like to give feedback, or require further information about this standard, please contact GCFP@cabinetoffice.gov.uk

1 Agreed by the GCFP Board in January 2022.

2 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.

A6. Government Functions (UK)

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

The Government Counter Fraud Function (GCFF) is one of the government's fourteen functions. The GCFF has published a Functional Standard, a Strategy and in 2018 launched the world's first Counter Fraud Profession. The vision of the GCFF is:

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

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

The Government Functions

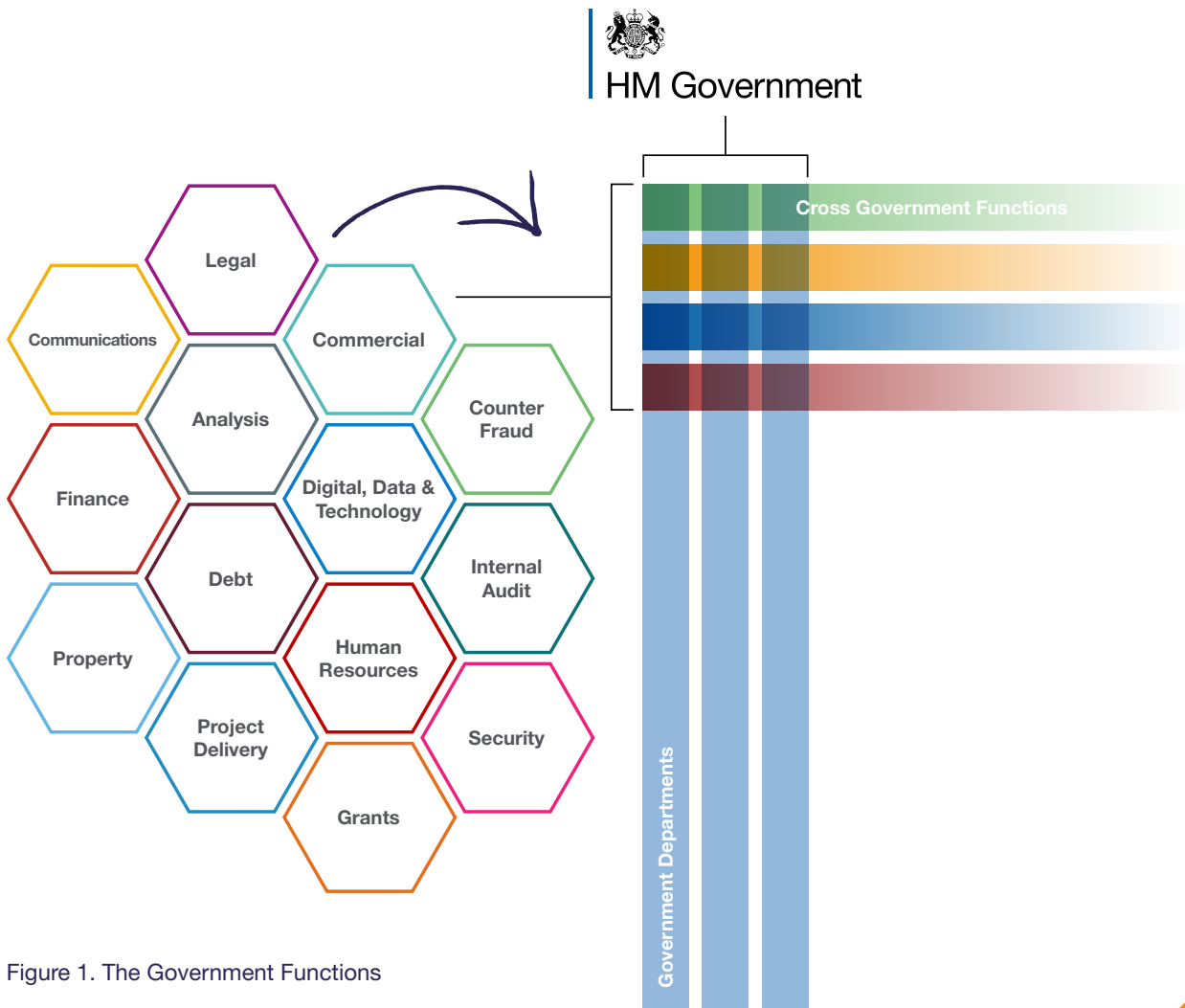


Figure 1. The Government Functions

A7. Public Sector Fraud Authority (PSFA)

The 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 will bring:

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

The PSFA will change the way that government manages fraud.

Its mission is to:

- ✓ 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 and error - 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 3 service and 3 function 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). PSC works with 17 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.

A8. Government Counter Fraud Profession

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

A9. Government Counter Fraud Framework

The framework covers all of the core disciplines and subdisciplines that a public sector organisation needs when dealing with the fraud threat that the public sector faces. Organisations will use these to different extents depending on the nature of their business and services, and the associated fraud threat, as assessed through their fraud risk assessment.

- **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 coordinating an organisation's overall response to fraud and economic crime. The main area is in the functional delivery level, this details the core disciplines that an organisation may use in an effective counter fraud response. Within these core disciplines are details of the knowledge, skills and experience needed to undertake these disciplines effectively
- **Sub disciplines:** the subdisciplines is an area of additional knowledge, skills and experience that enhance capability across a number of core disciplines



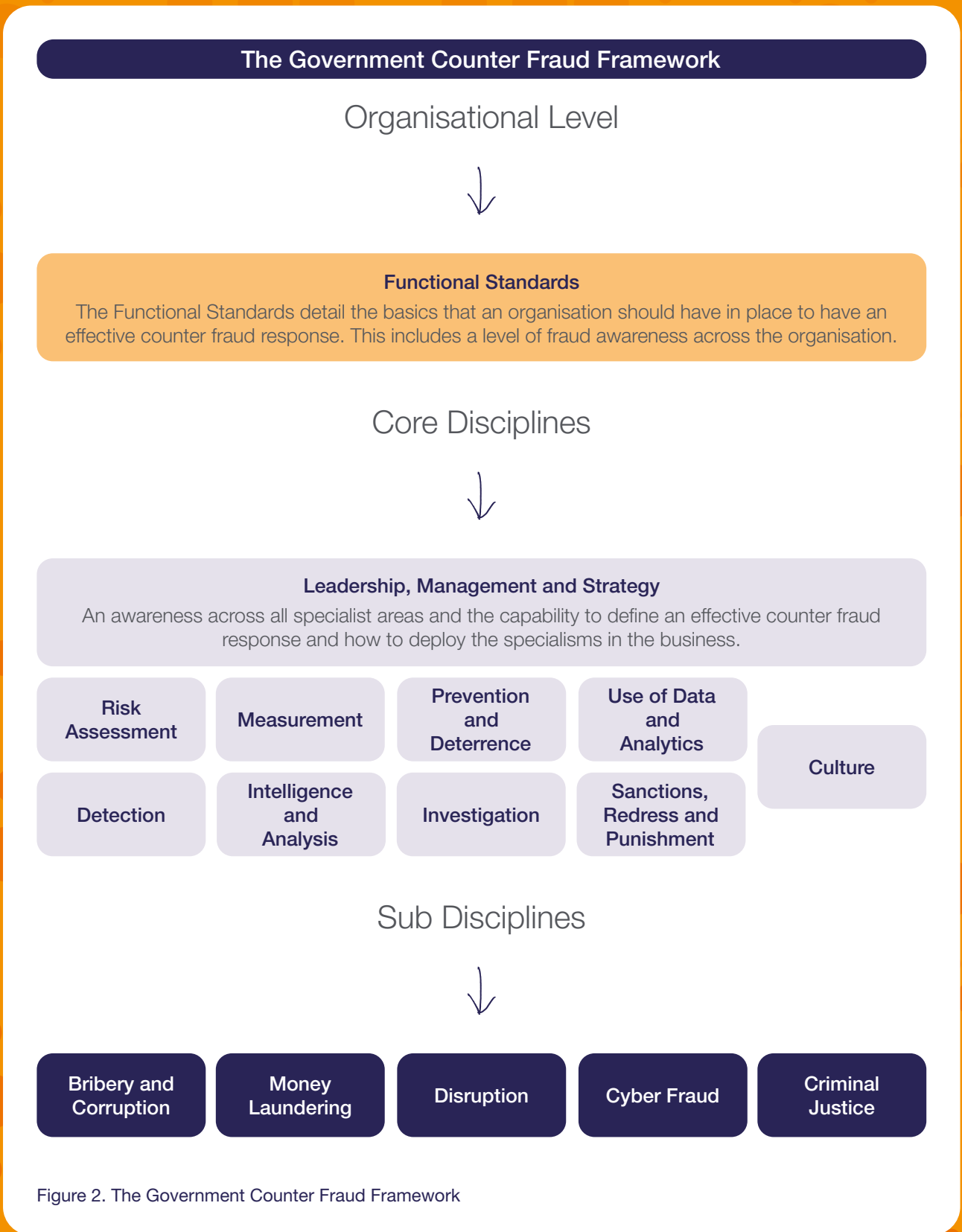


Figure 2. The Government Counter Fraud Framework

The Counter Fraud cluster incorporates the Fraud Risk Assessment, the Fraud Measurement and Fraud Prevention disciplines enabling the development of a career pathway for the counter fraud practitioner which is equitable with those of the other 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.

The Counter Fraud cluster forms a robust counter fraud response, the disciplines cover: Risk Assessment, Prevention and Deterrence, and Fraud Measurement.

By building the clusters, we are showing a commitment to increasing capability now and for the future.

The Prevention Standard will therefore form part of the Counter Fraud cluster that is being established³.

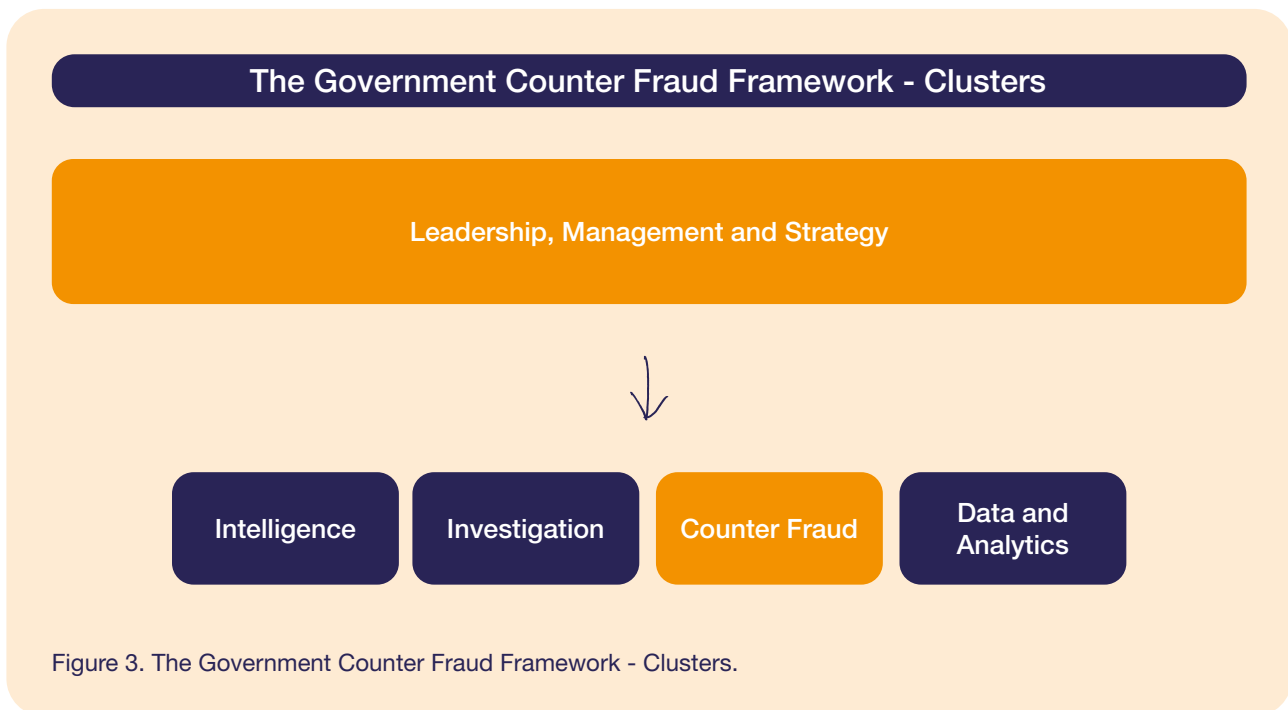


Figure 3. The Government Counter Fraud Framework - Clusters.

3 The Government Counter Fraud Profession's ambition is that a counter fraud professional will meet these standards, alongside risk assessment and fraud measurement.

A10. Roles and Responsibilities

Counter Fraud Professional (CFP)

For the purpose of this standard, a CFP focuses on fraud prevention. They will be conducting activities to embed proactive and reactive preventative controls within their organisation. In some organisations, the person undertaking the fraud risk assessment, may also be responsible for developing controls or policies or processes to prevent fraud. Other organisations may have different structures that separate the roles, and have individuals responsible for looking at different parts of the process.

The individual working in counter fraud will need an understanding of the different types of fraud, as well as its causes and motivators. They will also need an understanding of the fraud landscape across their organisation and the wider context.

Effective fraud prevention cannot be undertaken in isolation. For fraud prevention to be effective, it should link to understanding the risk and threat of fraud, measuring the levels of fraud, having the means and capability to detect fraud and prosecuting fraud criminals through use of the range of sanctions available.

Counter Fraud Functional Lead⁴


The counter fraud functional lead within an organisation, reports to the Board member accountable for counter fraud and the day-to-day management of fraud, bribery and corruption risk in their organisation.

Senior Responsible Officer (SRO)⁵

For the purpose of this standard, the SRO is the official responsible for ensuring that fraud risks identified during the fraud risk assessment process, and are monitored and treated with fraud controls in a timely and effective manner within an organisation.

The responsibilities of the SRO are to ensure that:

- risks identified are assessed, managed and monitored
- risks are clearly articulated in risk statements
- appropriate level of risk tolerance is determined
- stakeholders are assigned responsibility for each of the risks identified within an enterprise; each risk and its associated activities are coordinated
- risk management is integrated into operational activities
- gaps in mitigation and monitoring activities are remediated



Effective fraud prevention cannot be undertaken in isolation

4 See GovS 013: Counter Fraud for further information - <https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud>.

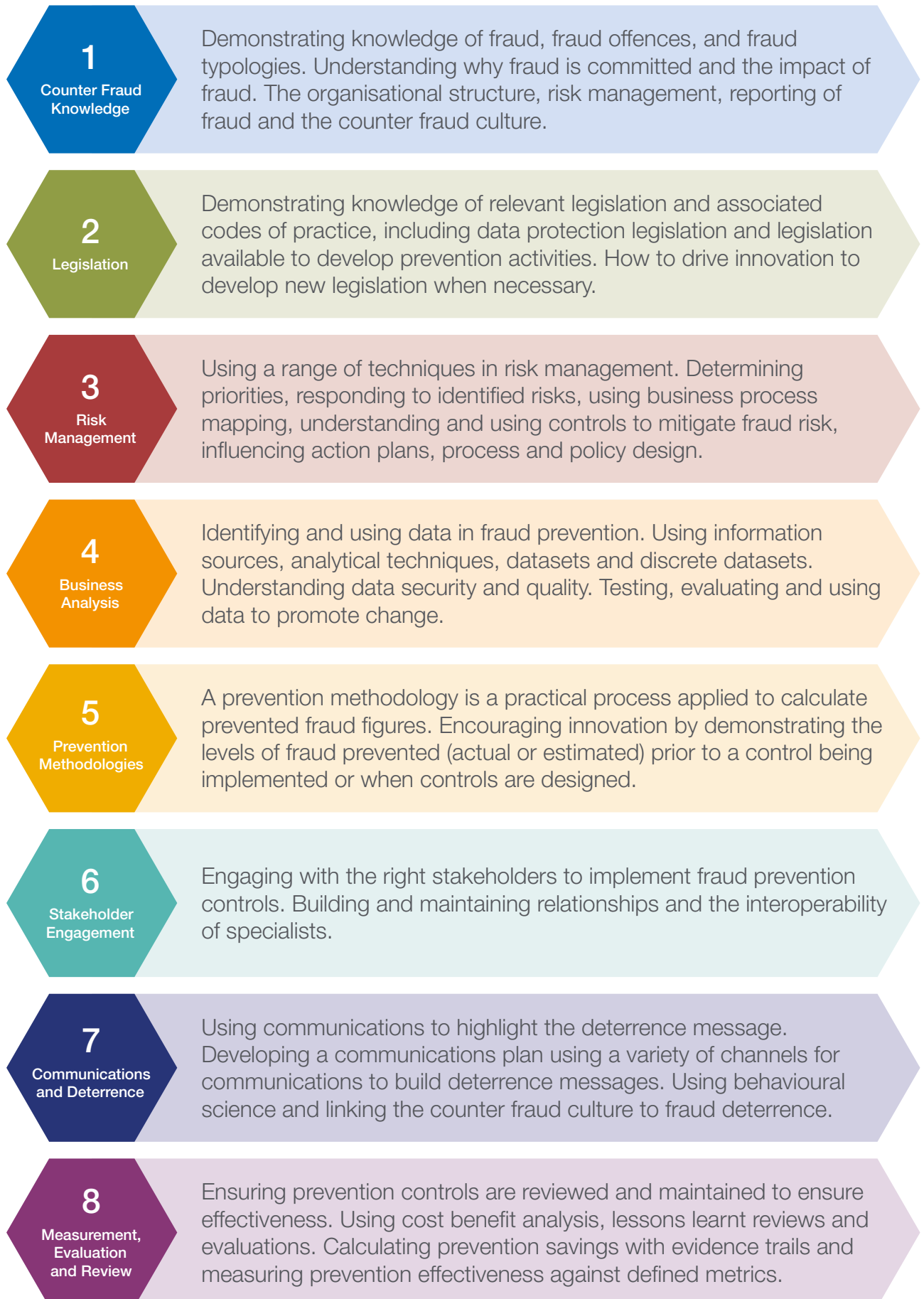
5 Definition of the SRO from the Fraud Risk Assessment Standard.

A11. Key Components Explained

Components outline at a high level, the knowledge, skills and experience required for each core and sub discipline. There are 8 key components for the Fraud Prevention 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.



Figure 4. Fraud Prevention Standard Key Components.



Within the competency framework are three competency levels, these are **Trainee**, **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.

A12. Competency Levels

General rules about the competency levels are set out below:

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

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

A13. Understanding Categories

Categories are defined combinations of elements, which show the knowledge, skills and experience expected for each category within a standard. Categories are not people or grade specific and the title or description used by organisations may be different to those described in the relevant standard.

The initial version of this standard is intended to be a published and recognised fraud prevention standard for counter fraud professionals across government.

The next stage will entail considering the components of this standard, alongside measurement and risk assessment, to establish the requirements for and entry routes into the Profession as a counter fraud professional.

B. Fraud Prevention Professional - Competency Framework

3. Counter Fraud Knowledge Competency			
	Trainee (T)	Foundation (F)	Practitioner (P)
3.1 Counter Fraud Knowledge - Understanding Fraud Offences⁶	Identify the principal offences as set out in key legislation and statutory frameworks, used in the UK for fraud, bribery and corruption.	Explain the principal offences as set out in key legislation and statutory frameworks, used in the UK for fraud, bribery and corruption.	Apply the principal offences as set out in key legislation and statutory frameworks, used in the UK for fraud, bribery and corruption.
3.2 Counter Fraud Knowledge - Understanding Fraud and Error Typologies	Identify the various ways to categorise fraud into types, for example, by modus operandi (misappropriation of assets, financial statement fraud, and bribery) or by victim.	Explain the various ways to categorise fraud into types, for example, by modus operandi (misappropriation of assets, financial statement fraud, and bribery) or by victim.	Apply the various ways to categorise fraud into types, for example, by modus operandi (misappropriation of assets, financial statement fraud, and bribery) or by victim.
3.3 Counter Fraud Knowledge - Fraud in the Public Sector	Identify a few types of fraud across different sectors and those within public sector including procurement fraud, corruption, and grant fraud.	Explain a few types of fraud across different sectors and those within public sector including procurement fraud, corruption, and grant fraud.	Apply knowledge of a few types of fraud across different sectors and those within public sector including procurement fraud, corruption, and grant fraud.
3.4 Counter Fraud Knowledge - People Who Commit Fraud and their Motivations	Identify the key theories about who commits fraud (individuals, organised crime groups, etc.) and their motivators.	Explain the key theories about who commits fraud (individuals, organised crime groups, etc.) and their motivators.	Apply knowledge of theories about the variety of people who commit fraud and their motivators.
3.5 Counter Fraud Knowledge - Understanding Victims of Fraud	Identify that there are a range of people and organisations that may be victims of fraud.	Explain who may be the victim of fraud in a variety of scenarios.	Apply knowledge of who the victim of fraud may be, in a variety of scenarios.

6 Including bribery and corruption relating to the public sector, where it leads to financial gain, or the avoidance of financial loss.

3. Counter Fraud Knowledge Competency

	Trainee (T)	Foundation (F)	Practitioner (P)
3.6 Counter Fraud Knowledge – Role of Different Business Units in Combatting Fraud	Identify all the business units with responsibility for different aspects of fraud risk management.	Explain the role of the business units in managing fraud risk, for example, policy, operations, finance, legal, human resources, risk management, internal and external audit (National Audit Office or NAO) and other relevant business units.	Apply an understanding of how different business units manage the risk of and the response to fraud. Also, apply an understanding of the roles of various BUs in this process, such as finance, legal, human resources, risk management, internal and external audit (National Audit Office or NAO) and other relevant business units.
3.7 Counter Fraud Knowledge - Impact of Fraud	Name the different ways that fraud impacts on victims (beyond financial, for example, reputational).	Describe the different ways fraud impacts victims (beyond financial, for example, reputational).	Explain the different ways that fraud impacts on victims (beyond financial, for example, reputational).
3.8 Counter Fraud Knowledge - Counter Fraud Techniques	Identify a range of techniques that can be used to detect, prevent and record fraud and error loss.	Describe a range of techniques that can be used to detect, prevent and record fraud and error loss, with insight to cross-sector application.	Apply a range of techniques that can be used to detect, prevent and record fraud and error loss, with insight to cross-sector application.
3.9 Counter Fraud Knowledge - Reporting Fraud	Identify fraud reporting processes for the organisation and the fraud response plan and relevant policies.	Describe the fraud reporting processes for the organisation and the fraud response plan and relevant policies.	Explain the different ways in which fraud is reported, both internally and externally, for the organisation and the fraud response plan and relevant policies.
3.10 Counter Fraud Knowledge - Organisations Counter Fraud Culture	Identify that developing or improving or enhancing the organisation's counter fraud culture, helps prevent fraud within the organisation.	Describe how developing or improving or enhancing the organisation's counter fraud culture, helps prevent fraud within the organisation.	Explain how developing or improving or enhancing the organisation's counter fraud culture, helps prevent fraud within the organisation and with wider stakeholders.
3.11 Counter Fraud Knowledge – Bribery Prevention	Identify the six principles of bribery prevention.	Explain the six principles of bribery prevention.	Demonstrate and apply knowledge of the six principles of bribery prevention.

4. Legislation Competency			
	Trainee (T)	Foundation (F)	Practitioner (P)
4.1 Legislation - Relevant Legislation and Organisational Policies	Identify relevant organisational policies and their interaction with the relevant legislation and associated codes of practice (relating to counter fraud).	Describe the relevant legislation and associated codes of practice (relating to counter fraud) and describe how they interact with organisational policies and the development of fraud prevention.	Apply the relevant legislation and associated codes of practice (relating to counter fraud) and explain how they interact with organisational policies and the development of fraud prevention.
4.2 Legislation - Data Protection Legislation	Identify data protection legislation for obtaining, disclosing and sharing information.	Explain the principles of data protection legislation for when obtaining, disclosing and sharing information. Explain what legal gateways your organisation has in place.	Apply the principles of data protection legislation when obtaining, disclosing and sharing information, using legal gateways where appropriate.
4.3 Legislation - Data sharing	Identify legislation and organisational policies to facilitate data sharing	Explain the principles of data sharing legislation and organisational policies and how they can facilitate information sharing across organisations.	Apply the principles of data sharing legislation and organisational policies and explain how they can facilitate information sharing across organisations.
4.4 Legislation - Existing Legislation to Drive Prevention	Identify your organisation's legal powers that can aid the development of fraud prevention.	Describe your organisation's legal powers and how they aid the development of fraud prevention.	Explain your organisation's legal powers and how they could be applied to prevent fraud.
4.5 Legislation - Driving Innovation	Identify how your organisation develops or amends legislation.	Describe how you would develop or amend legislation to allow you to innovate in fraud prevention.	Explain how you would develop or amend legislation to allow you to innovate in fraud prevention.

5. Risk Management Competency

	Trainee (T)	Foundation (F)	Practitioner (P)
5.1 Risk Management - Understanding Fraud Risk	Outline how fraud risk assessments effectively identify, describe and assess fraud risks.	Explain how fraud risk assessments effectively identify, describe and assess fraud risks.	Apply knowledge of fraud risk assessment to effectively identify, describe and assess fraud risks.
5.2 Risk Management- Levels of Fraud Risk Assessment (Organisational (Enterprise), Thematic (Grouped) or and Full)	<p>Identify the differences between the four different levels of fraud risk assessment:</p> <ul style="list-style-type: none"> • Organisational (Enterprise) • Thematic (Grouped) • Initial Fraud Impact Assessment • Full Fraud Risk Assessment 	<p>Explain the differences between, and appropriate use of, the four different levels of fraud risk assessment:</p> <ul style="list-style-type: none"> • Organisational (Enterprise) • Thematic (Grouped) • Initial Fraud Impact Assessment • Full Fraud Risk Assessment 	<p>Demonstrate the appropriate use of fraud risk assessments at the four different levels:</p> <ul style="list-style-type: none"> • Organisational (Enterprise) • Thematic (Grouped) • Initial Fraud Impact Assessment • Full Fraud Risk Assessment
5.3 Risk Management - Fraud Risk Management	Identify the various elements of the Fraud Risk Management Cycle.	Explain the elements of the Fraud Risk Management Cycle in simple terms.	Apply knowledge of the Fraud Risk Management Cycle, championing it to all stakeholders.
5.4 Risk Management - Determining Priorities for Action	Identify how risk is prioritised in the organisation.	Explain how to prioritise identified risks to inform fraud prevention.	Apply risk management knowledge to inform the prioritisation of risks and to inform fraud prevention.
5.5 Risk Management - System and Procedure Documentation	Identify the benefits of business process mapping and the key elements required.	Explain how to conduct and analyse a business process mapping exercise, including the key things to include in a recommendation report.	Demonstrate business process mapping, identifying vulnerabilities and potential control failures. Analyse the result, producing a report, making cost effective recommendations for improvement.
5.6 Risk Management - Responding to Identified Fraud Risk (4Ts)	Outline how fraud risks can be managed by an organisation, for example, treated, tolerated, transferred or terminated.	Explain how fraud risks can be managed by an organisation, for example, treated, tolerated, transferred or terminated.	Apply risk management options, for example, treated, tolerated, transferred or terminated.
5.7 Risk Management - Controls	Identify the strengths and weaknesses of a variety of controls available to mitigate risk.	Explain the strengths and weaknesses of a variety of control options to mitigate fraud risk. Explain the rationale behind selecting the controls to mitigate the fraud risk.	Demonstrate knowledge of the strengths and weaknesses of a variety of controls to mitigate identified fraud risks. Explain the rationale for applying the selected controls.

5. Risk Management Competency			
	Trainee (T)	Foundation (F)	Practitioner (P)
5.8 Risk Management - Control Impact	Identify that controls applied to fraud risks will impact in different ways. Identify the requirement to record and analyse the effectiveness of the control and identify any weaknesses.	Describe the impact of controls applied to fraud risks. Describe how you would record and analyse the effectiveness of the control and identify any weaknesses.	Assess the impact of controls applied to fraud risks. Record and analyse the effectiveness of the control and identify any weaknesses.
5.9 Risk Management - Action Plan for Risk Mitigation	Identify the minimum requirements for a fraud risk action plan.	Explain the key parts of a fraud risk action plan (as per the Fraud Risk Management Cycle).	Produce a fraud risk action plan (as per the Fraud Risk Management Cycle).
5.10 Risk Management - Delivery of Action Plan	Identify that residual risk will need to be assessed after controls have been tested and evaluated.	Describe how residual risk is assessed following the implementation of controls.	Test and evaluate controls, as identified on the fraud risk action plan. Assess the residual risk and report findings.
5.11 Risk Management - Policy and Programme Design	Identify how counter fraud knowledge informs policy, programme and system design.	Explain how counter fraud knowledge informs policy, programme and system design.	Apply counter fraud knowledge to inform policy, programme and system design.
5.12 Risk Management - Mid-Cycle Reviews	Identify the requirement to undertake mid-cycle assessments of controls.	Explain how you would undertake a mid-cycle review of controls, and how you could evaluate the review.	Demonstrate undertaking mid-cycle assessments of a business process or scheme, evaluating the effectiveness of the controls in place.
5.13 Risk Management - Due Diligence Checks	Identify the strengths and weaknesses of due diligence checks used to detect and prevent fraud.	Describe the strengths and weaknesses of due diligence checks used to detect and prevent fraud.	Explain the strengths and weaknesses of due diligence checks used to detect and prevent future fraud.

6. Business Analysis Competency

	Trainee (T)	Foundation (F)	Practitioner (P)
6.1 Business Analysis - Using data	Identify how data can be used to prevent fraud. Identify that data used in fraud prevention has strengths and weaknesses.	Explain how data can be used to prevent fraud and describe the strengths and weaknesses and limitations of use.	Apply knowledge of how data can be used to prevent fraud, evaluating the strengths and weaknesses and limitations of use.
6.2 Business Analysis - Information Sources	Identify a variety of information sources that aid the development of fraud prevention (including: methodologies, activities, strategies, etc.).	Explain how to identify and develop new information sources to aid development of fraud prevention (including: methodologies, activities, strategies, etc.).	Identify and develop new information sources to aid development of fraud prevention (including: methodologies, activities, strategies, etc.).
6.3 Business Analysis - Data Security	Identify data security requirements for receipt, storage, processing, sharing and disposal of information.	Explain how to use data security knowledge to manage the receipt, storage, processing, sharing and disposal of all information.	Apply data security knowledge to put in place secure arrangements for the receipt, storage, processing, sharing and disposal of all information.
6.4 Business Analysis - Analytic Techniques	Identify a variety of analytical techniques and tools available for counter fraud purposes.	Describe a variety of analytical techniques and tools that can be used for counter fraud purposes.	Explain a variety of analytical techniques and tools, and how they can be used for counter fraud purposes.
6.5 Business Analysis - Discrete Dataset or DataSet Analysis	Identify the difference between datasets and discrete datasets.	Describe how you would work with others to identify and evaluate datasets and discrete datasets.	Demonstrate application of, by working with others, the use of datasets or discrete datasets, including identification and evaluation of data sources.
6.6 Business Analysis - Data Analytic Pilots	Identify how to develop and implement a data analytic pilot, working with others when required.	Describe how to develop and implement a data analytic pilot, working with others when required.	Demonstrate developing and implementing a data analytic pilot, working with others when required.
6.7 Business Analysis - Data Quality	Identify issues that can affect data quality.	Describe how to assess the quality of data. Identifying the strengths and weaknesses and addressing issues.	Explain how to assess the quality of data. Identifying the strengths and weaknesses and addressing issues.
6.8 Business Analysis - Promoting Change	Identify how data analytics can be used to inform amendments or new controls.	Explain how you could use data analytics to inform amendments or new controls.	Analyse data analytics to inform amendments and new controls.
6.9 Business Analysis - Review Counter Fraud Data Analysis	Identify how data analysis findings require review of accuracy and cost effectiveness.	Explain how you would review the data analysis findings for accuracy and cost effectiveness.	Review data analysis findings for accuracy and cost effectiveness.
6.10 Business Analysis - Management Information (MI)	Identify how MI can be used to monitor the effectiveness of prevention activity.	Explain how MI can be used to monitor the effectiveness of prevention activity.	Demonstrate using MI to monitor and assess the effectiveness of prevention activity.

7. Prevention Methodologies Competency			
	Trainee (T)	Foundation (F)	Practitioner (P)
7.1 Prevention Methodologies - Applying Methodologies	Identify a variety of prevention methodologies that can be utilised at a local, organisation and/or national level.	Explain a variety of prevention methodologies that can be utilised at a local, organisation and/or national level.	Apply a variety of prevention methodologies at a local, organisation and/or national level, taking an innovative and forward thinking approach.
7.2 Prevention Methodologies - Proportionality	Identify the reasons proportionality is important when developing prevention methodologies, understanding the difference between high likelihood and high impact when addressing and mitigating risk.	Explain proportionality, when introducing prevention methodologies, understanding the difference between high likelihood and high impact when addressing and mitigating risk.	Apply proportionality, when introducing prevention methodologies, understanding the difference between high likelihood and high impact, when addressing and mitigating risk.
7.3 Prevention Methodologies - Reviews	Identify the requirement to undertake reviews of the prevention methodology.	Explain how you would undertake a review of the prevention methodology, and how you would evaluate the review.	Demonstrate undertaking a review and evaluation of the prevention methodology.
7.4 Prevention Methodologies - Innovation	Identify how applying a fraud mindset helps to identify vulnerabilities, when designing and evaluating prevention methodologies.	Explain how to apply a fraud mindset when identifying vulnerabilities, when designing and evaluating prevention methodologies.	Apply a fraud mindset to think like a fraudster to identify vulnerabilities, when designing and evaluating prevention methodologies.
7.5 Prevention Methodologies - Prevention Evaluation	Identify the requirement for a prevention methodology that calculates savings from preventing fraud from occurring in the first place.	Explain how prevention methodologies should be used to calculate savings made by preventing fraud from occurring in the first place.	Develop a methodology to calculate savings achieved by preventing fraud from occurring in the first place; at a local, organisation and/or national level, taking an innovative and forward-thinking approach.
7.6 Prevention Methodologies - Future Loss Prevented	Identify that the prevention methodologies for future loss prevented, differs from fraud prevented from the outset.	Explain how to develop a prevention methodology, based on new controls put in place, to calculate the future loss prevented.	Develop a prevention methodology, based on new controls, to calculate the future loss prevented at a local, organisation and/or national level, taking an innovative and forward-thinking approach.
7.7 Prevention Methodologies - Cognitive Diversity⁷	Identify how cognitive diversity, (seeking a variety of views and opinions) can lead to greater innovation when problem solving to achieve common goals.	Describe how cognitive diversity, (seeking a variety of views and opinions) can lead to greater innovation when problem solving to achieve common goals.	Explain how cognitive diversity, (seeking a variety of views and opinions) can lead to greater innovation when problem solving to achieve common goals.

7 Cognitive diversity can be described as the variety of ways that people think. It includes things like the way we process information, how we see the world and how we make decisions.

8. Stakeholder Engagement Competency

	Trainee (T)	Foundation (F)	Practitioner (P)
8.1 Stakeholder Engagement - Building Stakeholder Relationships	Identify potential stakeholders (including cross-sector).	Explain how to identify, build and maintain new and existing stakeholder (including cross-sector) relationships.	Identify, build and maintain new and existing stakeholders,(including cross-sector) relationships to achieve common aims.
8.2 Stakeholder Engagement - Protocol Document	Identify the reasons why a protocol document or memorandum of understanding (MOU) is required.	Explain why a protocol document or memorandum of understanding (MOU) is required when working with stakeholders and the minimum requirements.	When working with third parties, produce a protocol agreement or memorandum of understanding (MOU) which sets out the respective responsibilities of all parties involved.
8.3 Stakeholder Engagement - Specialists	Identify a variety of specialist teams or stakeholders that could be key to fraud prevention.	Explain how you would engage with relevant specialists (such as data analysts, behavioural scientists, or other specialists, from inside or outside your organisation).	Engage all relevant stakeholders to identify when to bring in specialist skills (such as data analysts, behavioural scientists, or other specialists, from inside or outside your organisation).

9. Communications and Deterrence Competency			
	Trainee (T)	Foundation (F)	Practitioner (P)
9.1 Communications and Deterrence - Communications to Deter Fraud	Identify how to deter fraud using communications. Describe the strengths and weaknesses of a variety of approaches.	Explain how to deter fraud using communications. Describe the strengths and weaknesses of a variety of approaches.	Demonstrate knowledge of how to deter fraud using communications. Explain the strengths and weaknesses of a variety of approaches.
9.2 Communications and Deterrence - Communication Channels	Identify the different communications channels and methods that can be used to promote counter fraud awareness.	Explain the different communication channels and methods that can be used to promote counter fraud awareness.	Apply different communication channels and methods, to promote counter fraud awareness, including sharing to internal and external stakeholders to deter future fraud.
9.3 Communications and Deterrence - Deterrence Statements	Identify the purpose of deterrence messaging within business processes to prevent fraud.	Explain the relevance of deterrence messaging within business processes to prevent fraud.	Understand and seek out opportunities to build in deterrence messaging within business processes to prevent fraud.
9.4 Communications and Deterrence - Using Behavioural Insight Models	Identify a variety of different behavioural insight models and how they link to fraud theories that explain offending.	Explain how behavioural insight can encourage compliance with business processes and aid identification of barriers to change.	Demonstrate, using a variety of behavioural insight models, knowledge of how to encourage compliance with business processes, identifying and addressing the barriers to change.
9.5 Communications and Deterrence - Counter Fraud Culture for Prevention	Identify a variety of measures that could be used to support employees and promote a counter fraud culture at organisational level.	Explain how a variety of proactive measures, that can be used to prevent and deter fraud, can promote a counter fraud culture that supports employees, at an organisational level.	Apply a variety of proactive measures, to shape and promote an effective counter fraud culture that supports employees, at an organisational level.

10. Measurement, Evaluation and Review Competency

	Trainee (T)	Foundation (F)	Practitioner (P)
10.1 Measurement, Evaluation and Review - Cost Benefit Analysis	Identify how a cost benefit analysis can demonstrate the effectiveness of prevention activity.	Explain how to conduct a cost benefit analysis to demonstrate the effectiveness of prevention activity.	Produce a cost benefit analysis which demonstrates the effectiveness of prevention activity using SMART principles.
10.2 Measurement, Evaluation and Review - Lessons Learnt Reviews	Identify how lessons learnt reviews can be used to outline the successes and limitations of fraud prevention.	Explain how to gather and use lessons learnt reviews, outlining successes and limitations, to improve fraud prevention.	Apply knowledge of gathering and using lessons learnt reviews, outlining successes and limitations, to improve fraud prevention. Share knowledge with relevant team members and stakeholders.
10.3 Measurement, Evaluation and Review - Relevant Stakeholders	Identify that all relevant stakeholders need to agree on the calculator of prevented savings and that evidence is required.	Describe the process and evidence required, for all relevant stakeholders to agree, and sign off on, attribution of prevented savings calculations.	Establish or assess the process and evidence required, for all relevant stakeholders to agree and sign off on, attribution of prevented savings calculations.
10.4 Measurement, Evaluation and Review - Monitoring Effectiveness of Fraud Prevention	Identify the requirement for metrics to measure prevention outcomes.	Describe how metrics benchmark, measure, monitor and assure effectiveness of improvements or new processes of prevention outcomes.	Explain how metrics benchmark, measure, monitor and assure the effectiveness of improvements or new processes for prevention outcomes.
10.5 Measurement, Evaluation and Review - Monitoring Effectiveness of Fraud Deterrence	Identify the requirement for metrics to measure deterrence outcomes.	Describe how metrics benchmark, measure, monitor and assure effectiveness of improvements or new processes of deterrence outcomes.	Explain how metrics benchmark, measure, monitor and assure the effectiveness of improvements or new processes for deterrence outcomes.

C. Guidance on Processes

C1. Introduction

This guidance covers effective prevention processes. Individuals must be able to plan, identify and embed these processes in organisations in order to effectively counter fraud, bribery, corruption and associated error. All processes and procedures should be regularly revised and evaluated to ensure they are of the required standards and remain current. Set out below is the process to identify, develop, implement, measure and evaluate controls to prevent fraud.

The design of fraud prevention procedures and controls cannot be undertaken in isolation from the rest of the organisation.

Individuals should have access to, and an understanding of, an organisation's:

- strategy, structure and key target operating models
- priorities, policies and guidelines, operating procedures, and performance data
- intelligence and other threat assessments, risk management models, risk registers and assessments
- internal audit, compliance, investigation and other inspection and regulatory reports

To identify the potential fraud risks and the actors that are likely to exploit these, individuals should understand how the organisation's service users interact with it and access its services.

These actors may include, but are not limited to, the following:

- **insiders** - occupational fraudsters (employees and contractors)
- **external parties** - service users, customers and suppliers

- **motivated individuals** - those with the motivation and the capability to commit fraud
- **opportunists** - those who take advantage of weaknesses in systems or processes
- **combinations** - a mixture of insiders and external parties with the potential for collusion which may manifest itself in the form of bribery and corruption
- **Organised Crime Groups (OCGs)** - groups of criminals, who may be involved in other types of crime
- **terrorists** - raising funds for terrorist activity
- **state actors** - people working for other governments

Other teams involved in managing fraud and fraud risk may include:

- **strategy** - those responsible for developing the overarching strategic plan and the counter fraud strategy which sits beneath and contributes to this
- **policy** - those responsible for developing and maintaining all key policies, including the counter fraud policy - this latter policy should be developed in conjunction with the counter fraud function
- **risk management** - those responsible for risk identification, assessment, measurement and monitoring - including fraud risk. There must be effective liaison between the risk management and counter fraud functions to ensure that all fraud risks have been identified and appropriately assessed. This will help to ensure that activities remain within the organisation's fraud risk appetite

C2. Proactive Prevention Approach

Individuals should undertake proactive activity to identify areas where fraud prevention could be developed and embedded in business processes to reduce fraud in specific areas.

This activity should include, but is not limited to:

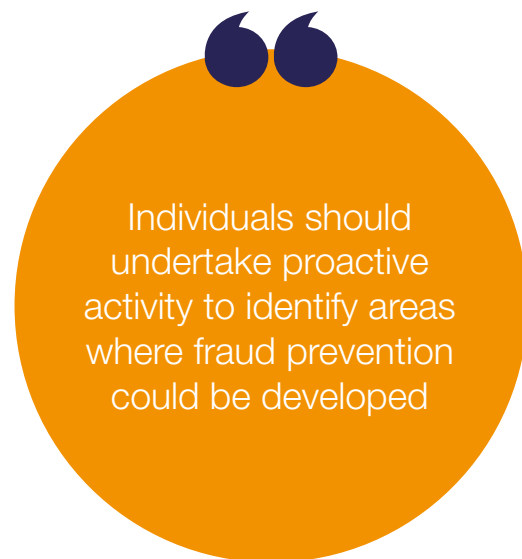
- maintaining close links with other business areas and providing expertise to develop and implement high-quality, professional prevention activities within all parts of the business
- conducting horizon scanning exercises to identify key areas of change that could result in an increased risk of fraud
- engaging with risk assessment teams to gain a comprehensive understanding of the threats that the organisation faces
- conducting business mapping exercises to review business procedures and identify areas of concern
- the use of data analytics and data sharing to inform counter fraud operations and deter potential fraudsters
- engaging behavioural scientists to develop and use behavioural insight to understand and influence behaviours to prevent and deter fraudulent actions
- promoting an iterative approach to review and evaluate controls within a process, including conducting periodic and mid-cycle reviews of existing processes and controls
- commissioning or responding to strategic threat assessments

C3. Proportionality

All fraud prevention must be proportionate to the risks or threats identified.

It is generally acknowledged that there are four stages to a proportionality test⁸, namely:

- there must be a legitimate aim for a measure
- the measure must be suitable to achieve the aim (potentially with a requirement of evidence to show it will have that effect)
- the measure must be necessary to achieve the aim, there cannot be any less onerous way of doing it
- the measure must be reasonable, considering the competing interests of different groups at hand



8 European Union Law: proportionality - EN - EUR-Lex - <https://eur-lex.europa.eu/EN/legal-content/glossary/principle-of-proportionality.html>


C4. Develop or Amend Legislation, Policy or Working Practices

Individuals may come across new and evolving fraud threats or risks, where legislation, policy or working practices do not currently exist to tackle the fraud.

Where this occurs, they should work with cross-government stakeholders to identify whether new or amended legislation, policy or working practices are needed.

Evidence should be gathered to prove the case for change. This could include, but is not limited to:

- business process reviews to identify gaps or weaknesses in the control
- investigation reviews to establish how a fraud has occurred and the changes needed to prevent a recurrence
- case failure or Crown Prosecution Service (CPS) reviews
- judicial review decisions
- intelligence reports, management information and trend analysis
- internal policy reviews and internal legislation reviews
- the modus operandi of any new fraud and why current legislation cannot deal with this
- a review of legislation to reflect changing circumstances (for example, Proceeds Of Crime Act (POCA) re-wording to include cryptocurrency)
- new schemes with non-public sector organisations
- powers given to external partners, with no recourse to public sector recovery



Evidence should be gathered to prove the case for change

When the evidence for new or amended legislation has been gathered, the individual⁹ should collaborate with policy professionals to submit an options or proposal paper to senior management and/or ministers for approval. The proposal should include:

- the problem or issue to be addressed
- options for resolution (including if nothing was done)
- what the recommended proposal entails
- whether ministerial approval is likely to be required
- the level of approval being sought

⁹ If no internal mechanism to develop or propose new legislation, counter fraud professionals should contact their sponsoring department policy team for further guidance or advice.

C5. Fraud Risk Management Cycle

The Fraud Risk Management Cycle has four component parts, namely:

- fraud risk assessment identification
- fraud risk assessment - evaluation and prioritisation
- evaluating controls
- reviewing and reporting

A Fraud Risk Assessment (FRA) is fundamental to any Fraud Risk Management (FRM) programme. It helps to understand the risks that are unique to the organisation, identify gaps or weaknesses in controls, to mitigate those risks, and develop a practical action plan for targeting resources to reduce risks, all of which form an integral part of an effective counter fraud strategy and response.

An FRA should be viewed as a continuous cycle of activity to ensure that new risks and emerging threats are considered, evaluated and prioritised. Fraud does not just reduce the availability of public funds being used correctly across government, but it threatens financial stability and reputation. Detailed information can be found in the Government Counter Fraud Profession (GCFP) Leadership Management and Strategy (LMS) Standards¹⁰ and on the core discipline of FRA in the Government Counter Fraud Professional Standards and Guidance.¹¹

FRAs form part of the fraud risk management cycle. This cycle offers an illustration of the end-to-end FRM process, which starts from using research to identify known risks and ends with the completion of an FRA.

The information contained in the FRA is used to design, implement and monitor the controls needed to mitigate all identified fraud threats and vulnerabilities.

The first half of the cycle deals with the FRA, which is outside the scope of this standard. The second half of the risk cycle is where fraud prevention actions should be implemented to mitigate the identified risks.

The individual should liaise with the FRA team to understand how risks are evaluated and scored. Knowledge of the scoring process is needed to prioritise the prevention activities linked to these assessments.

Fraud Risk Assessments

FRAs have a clear structure. They must be captured as:

- **actor:** who commits the fraud (may be an individual or a group of people)
- **action:** what the fraudulent action is or may be
- **outcome:** what is the resulting impact or consequence(s) should the fraud risk occur? These may be more than financial and may include, but are not limited to, one or more of the following:
 - harm to national security
 - the undermining of policy
 - adverse effects on the delivery of services
 - social and psychological harm
 - physical harm
 - environmental damage

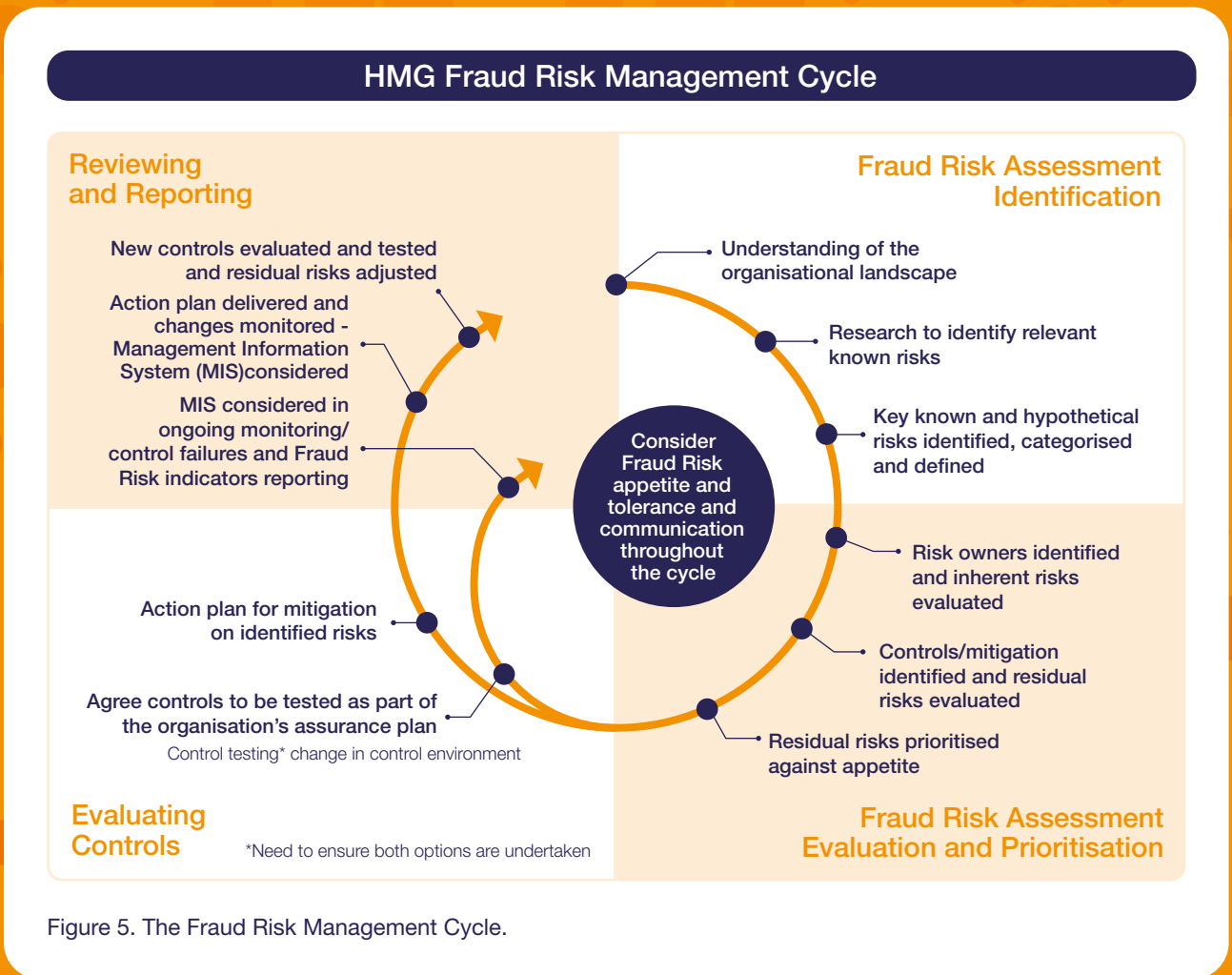
The FRA should be used to:

- establish the controls identified that require testing
- feed into the counter fraud strategy
- produce an action plan to mitigate identified risks
- assess the residual risk¹²
- consider ways to improve controls

10 See GCFP Leadership Management and Strategy Standard. This can be requested by emailing: gcfp@cabinetoffice.gov.uk

11 See the GCFP Standards and Guidance on Fraud Risk Assessment - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069745/Fraud-Risk-Assessment-Standards-2022-03-25.pdf

12 The risk that remains after controls and other mitigating actions have been applied to a risk.



“

The information contained in the FRA is used to design, implement and monitor the controls needed to mitigate all identified fraud threats and vulnerabilities

C6. Counter Fraud Strategy¹³

Counter fraud professionals may be involved in the development of the fraud strategy, sharing their knowledge and their work to design, implement, monitor and review all relevant mitigating actions. The strategy should also contain details of planned prevention activities including:

- the span of the planned prevention work
- the objectives to be achieved
- the resources and specialist skill sets required
- the metrics required to measure and evaluate the effectiveness of prevention controls

To manage risk effectively, controls need to be applied to fraud risks. Each control, or suite of controls, must be effective¹⁴ and operate continuously. The operation of controls should be monitored and monitoring routines should be data-driven, if possible. Further information on developing strategies can be found in the Government Counter Fraud Profession (GCFP) Leadership Management and Strategy Standards.

C7. Action Plans for Risk Mitigation

When assessing whether a risk needs an action plan, the 4T's model should be used.

- **Treat** - improve or develop mitigation controls, this can include setting a target risk level based on risk tolerance
- **Tolerate** - accept the current level of risk
- **Terminate** - stop the activity as the risk is deemed as too high to continue and cannot be sufficiently mitigated within risk tolerance
- **Transfer** - pass the risk on to a third party, such as when a person or organisation takes out an insurance policy

Risks designated as needing 'Treatment' should have an action plan which should include control design, implementation and monitoring.

Action plans may cover:

- a summary of fraud risks, threats and vulnerabilities associated with the organisation
- treatment strategies and controls put in place to manage fraud risks, threats and vulnerabilities
- information about implementing fraud control arrangements and other changes within the organisation
- strategies to ensure the organisation meets the training and awareness needs associated with the action plan
- mechanisms for collecting, analysing and reporting fraud incidents
- protocols for handling fraud incidents
- an outline of key roles and responsibilities for fraud control within the organisation
- review dates and progress monitoring and reporting

Examples of activities that could be included within an action plan include, but are not limited to:

- designing compliance into schemes to prevent incorrect or fraudulent actions
- promoting good compliance through education, customer and employee support
- carrying out additional checks on high-risk areas
- risk assessing services and where specific risks were detected, nudging service users to review and voluntarily repay any overpayments
- identifying data solutions that can be utilised to aid fraud prevention
- carrying out post-payment checks on selected claims and enforcing recovery of overpayments, where necessary

¹³ See GCFP Leadership Management and Strategy Standard. This can be requested by emailing: gcfp@cabinetoffice.gov.uk

¹⁴ Controls, where possible, should be designed to meet all aspects of the risk(s) they control and be tested prior to implementation.

C8. Prevention Controls

In conjunction with key stakeholders, the Senior Responsible Officer¹⁵ (SRO) should agree which controls will be tested as part of the organisation’s fraud prevention programme and review the decisions to reflect business circumstances.

Following evaluation and testing, the effectiveness of the reviewed controls should be ranked.¹⁶ All controls which are deemed:

- Poor or Inadequate or Unsatisfactory should then be reviewed and fed into the process set out for a change in the control environment
- Satisfactory or Limited or Good or Moderate may then be reviewed and fed into the process set out for a change in the control environment

SROs should work with counter fraud professionals to:

- review the issues raised in the FRA and suggest options for mitigating the identified fraud risks using the 4Ts model¹⁷
- review suggestions, and, either consult more broadly or work up a plan with the risk managers to implement new or improved mitigation which considers the cost-benefit analysis and impact - other evaluation tools may also be considered

The action plan will identify the risk and what current controls do, and do not do, to reduce the fraud risk. Controls can be informed by policies, operational procedures and stakeholder insight. It can be helpful to plot the risks using the format below:

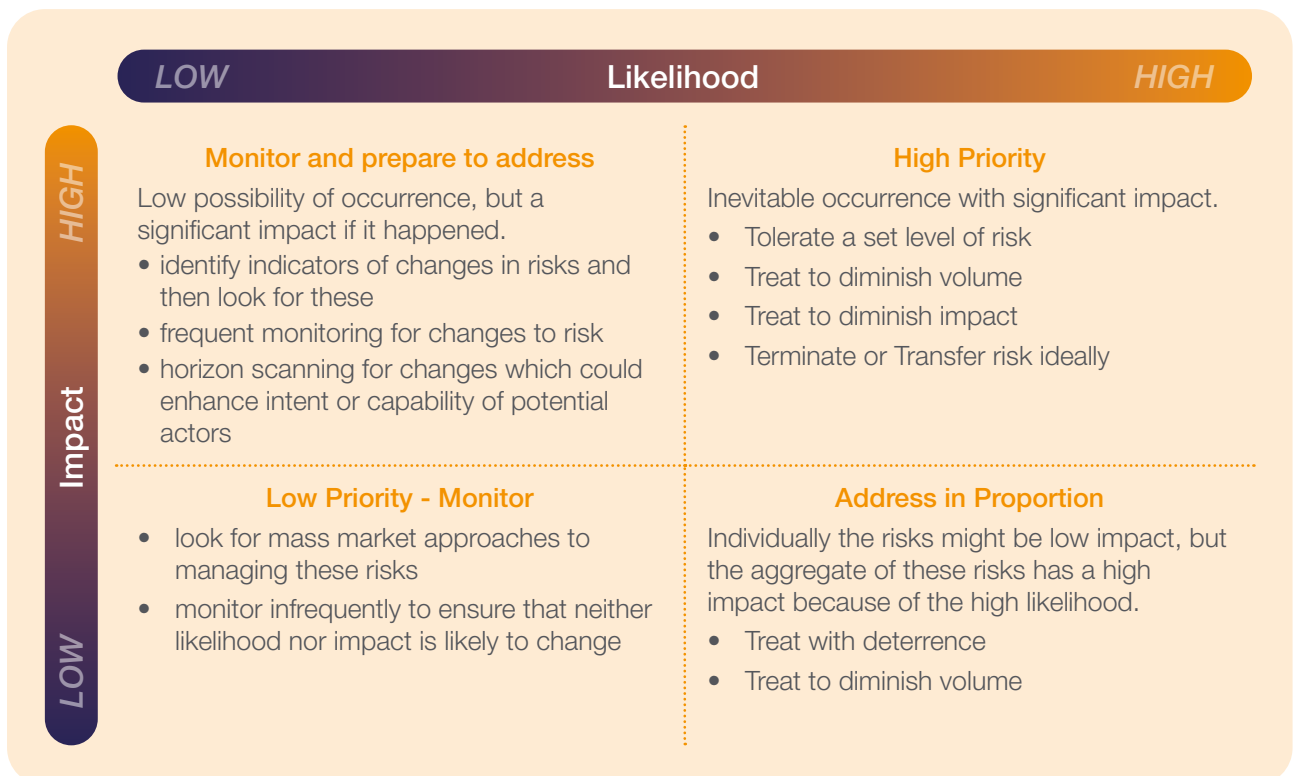


Figure 6. Assessing and managing risks¹⁸.

15 See A6. Roles and Responsibilities.

16 An organisation could use its own agreed definitions or may follow those provided by GIAA.

17 Functional Leads and SROs should have wider awareness (including other functions) as suggested controls or changes may impact on other business areas. See section E8 for further information.

18 Assessment and scoring of risks (impact versus likelihood) is detailed in the Government Counter Fraud Professionals Standards and Guidance on Fraud Risk Assessment. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1069745/Fraud-Risk-Assessment-Standards-2022-03-25.pdf

C9. Types of Controls

Individuals should understand what effect the control has on the risk. They should be able to describe what each fraud control does to mitigate the risk and how it operates. They should also describe what the control cannot do in relation to mitigating the risk.


After identifying the controls, the next stage is to “assess” them by categorising what they do. Controls can be categorised as:

- **promote** - deterrence controls
- **prevent** - controls to prevent the risk occurring
- **respond** - how to correct the outcomes of the identified risk

When considering new controls, or addressing gaps and vulnerabilities in existing controls, a co-design approach with stakeholders will achieve greater engagement and buy-in to effectively treat fraud risks.

Each of the 3 categories can then be broken down further to detail the response required:

- **deterrent** - these aim to put people off of fraud, deterrent controls could include the publication of consequences or investigation sanctions
- **directive** - these controls give direction, they include guidance, policies and legislation - directive controls state the practice to be followed, but do not stop fraud and bad practice occurring, for example, expenses policies.
- **preventative** - these aim to stop the fraud entering the system or reduce its impact - preventative controls could include: due diligence, two factor authentication or segregation of duties for payment approvals
- **detective** - these aim to find or identify fraud after it has happened and can impact on its duration and impact- these controls could include audits and financial reports and they will often lead to corrective actions
- **corrective** - these aim to make post-event corrections and could include the recovery of overpaid expenses direct from wages or terminating a process



Individuals should be able to describe what each fraud control does to mitigate the risk and how it operates

C10. Primary, Secondary and Tertiary Controls

The Commonwealth Fraud Prevention Centre¹⁹ recommends considering fraud in three phases: primary, secondary and tertiary.

Primary

1

This phase reduces the likelihood of the fraud occurring, through the use of fraud controls; these prevention controls could include:

- conducting integrity or suitability checks
- system or physical access controls
- user permissions
- confirming and authenticating identity
- pre-filling data from a reliable source
- the segregation of duties

Secondary

2

This phase reduces the impact of fraud through early identification and detection using techniques involving people, processes, technology and data analytics. This phase is also used to formulate a response to detected fraud. Practical secondary prevention controls could include:

- verifying information provided by an applicant, including data screening and matching, post claim
- compliance or performance reviews
- tip off and whistleblowing²⁰ processes²¹
- automatic notifications of high risk transactions
- fraud detection software

Tertiary

3

This phase reduces the impact and severity of fraud that has already occurred. Practical tertiary prevention controls could include:

- trained fraud analysts and investigators
- incident response plans
- coordinated disruption activity
- fraud investigations
- penalties for fraud and non-compliance

¹⁹ Used by the Commonwealth Fraud Prevention Centre, Australia.

²⁰ Whistleblowers can be described as concerned members of staff.

²¹ Whistleblowing for employees <https://www.gov.uk/whistleblowing>

C11. Control Testing

Controls should be regularly tested²² to ensure that they are being consistently applied and working continuously. The testing of the key controls within fraud risks could be undertaken by the counter fraud professional (CFP), internal audit or some other team independent of those responsible for the operation of the control(s).

Individuals should take a proportionate approach to testing of controls, prioritising controls in operations, functions and programmes which have been identified as having the highest risk of fraud. Testing should also focus on the controls that are critical for mitigating the risks of fraud. The value of controls can be assessed using the control assessment tool.²³

The frequency of control testing should be guided by:

- the nature, frequency and severity of the risk
- the control's importance in mitigating the risk

Where control testing is undertaken by someone other than a CFP, they should ensure that they are notified of the outcome of this testing.

Where controls have been found to have failed, or are performing below their design specification, action plans will need to be drawn up to deal with this.

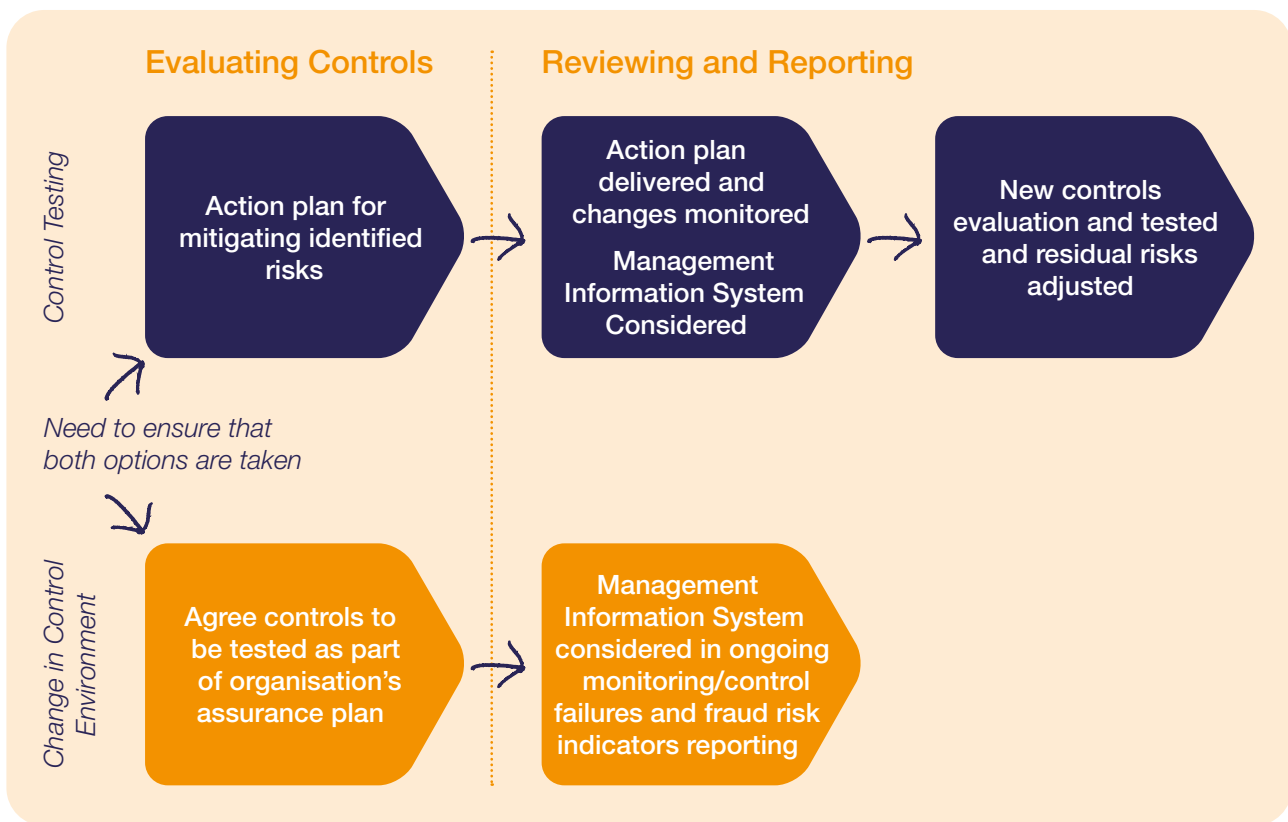


Figure 7. Implementing and amending controls (as per Fraud Risk Management Cycle).

22 This type of testing is called compliance testing - which identifies whether or not a control is working.

23 Products section D* has further information on the control assessment tool.

How an individual 'tests' a control will always depend on the type of control. They may also need to test controls in different ways. The primary methods include:

- research - such as desktop reviews and looking at case studies
- observation - such as process walk-throughs or workshops with stakeholders
- analysis - such as sample reviews or data analysis
- pressure testing - such as technical testing or covert actions to breach controls

Some common vulnerabilities you might find could include, but are not limited to:

- a lack of fraud awareness
- inadequate quality assurance
- staff or processes not verifying information or evidence
- a lack of effective oversight
- weak technology controls
- inadequate detection controls
- a lack of reporting or reconciliation

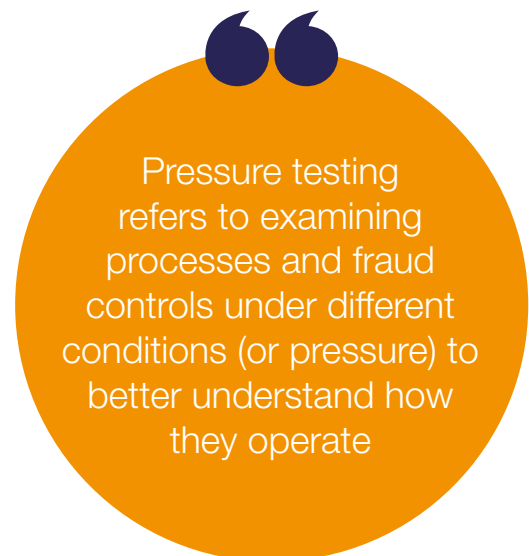
After you have considered the effectiveness of the control, consider if the whole control environment is adequate to mitigate the risk. This will help identify gaps in controls.

C12. Pressure Testing²⁴

Pressure testing is a proven way for public bodies to proactively identify and eliminate blind spots. If organisations know where their programmes and functions are vulnerable, they are better equipped and informed to reduce the opportunity for fraud.

Pressure testing refers to examining processes and fraud controls under different conditions (or pressure) to better understand how they operate, to measure their effectiveness and proactively identify any control gaps or vulnerabilities.

This involves applying creative and critical thinking to examine 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, uncover vulnerabilities and challenge assumptions about how fraud is managed by the organisation.



24 Further details on pressure testing see - <https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance/a-guide-to-pressure-testing-html>


C13. Test and Learn

A test and learn process should be utilised to evaluate controls following the National Audit Office's (NAO's) fraud and error framework²⁵.

'Test and Learn' is also a valuable method to gain insight, by running discovery tests on new data sources. The purpose of this is to identify areas where fraud prevention could be introduced and strengthened.

When conducting Test and Learn exercises, the following should be considered:

- have controls been evaluated to ensure risks were proportionately and effectively mitigated and have any new risks been identified?
- what are the key performance indicators or metrics?
- should key performance indicators or metrics be updated following evaluation?
- can root cause analysis be used to identify new risks?
- to what extent is internal and external stakeholder assurance needed?
- have existing controls been evaluated to assess the extent to which they represent the most cost-effective defence to fraud and associated error?
- can each control be assessed and evaluated?
- what measures are being used to evaluate different controls and to what extent are these measures consistent with one another?
- can other measures be used to verify that the results arising from the controls evaluation are reliable?



'Test and Learn' is a valuable method to gain insight, by running discovery tests on new data sources

25 National Audit Office Good practice guidance: Fraud and error - <https://www.nao.org.uk/wp-content/uploads/2021/03/010381-001-Fraud-and-Error-Accessible.pdf>

C14. Prevention Methodologies

A prevention methodology is a practical process applied to calculate prevented fraud figures. Prevention methodologies will vary depending on the fraud risk and the business line, service, benefit, or grant and the type of control being implemented.²⁶

When developing prevention methodologies, consider the flowcharts below:

Does the control or intervention apply to:

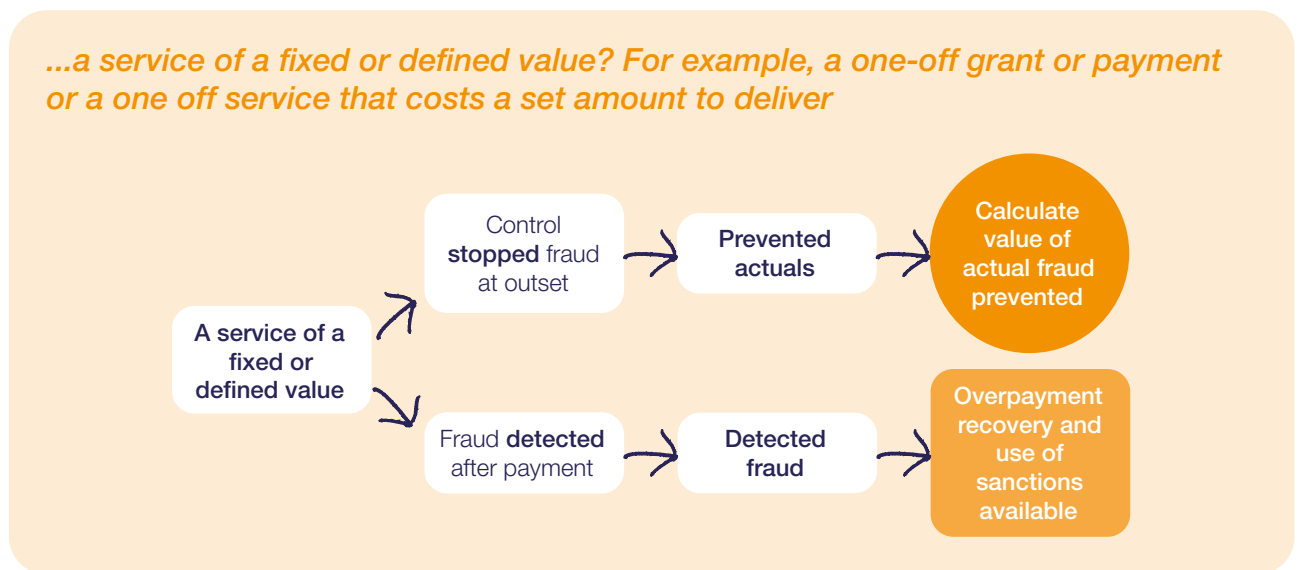


Figure 8. Flowchart for reporting prevented fraud of a fixed or defined value.

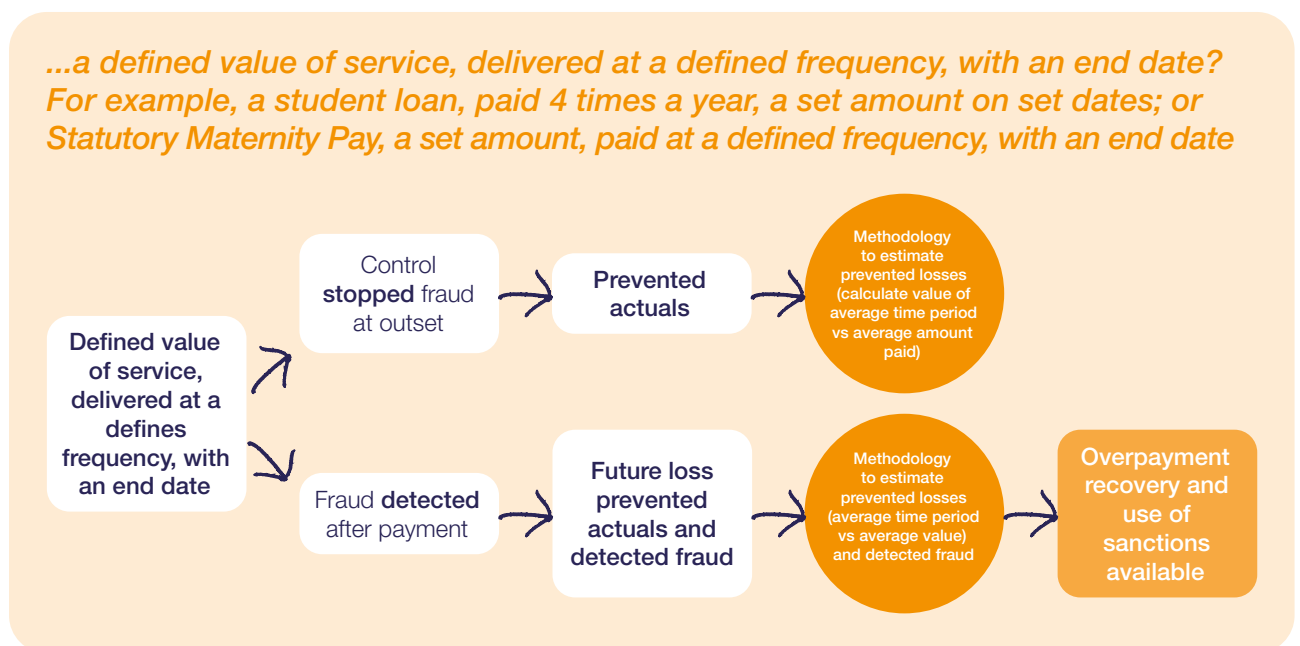


Figure 9. Flowchart for reporting prevented fraud of a fixed or defined value over a set period.

26 More information on calculating fraud savings can be found in the Government Counter Fraud Profession Fraud Measurement Standard.

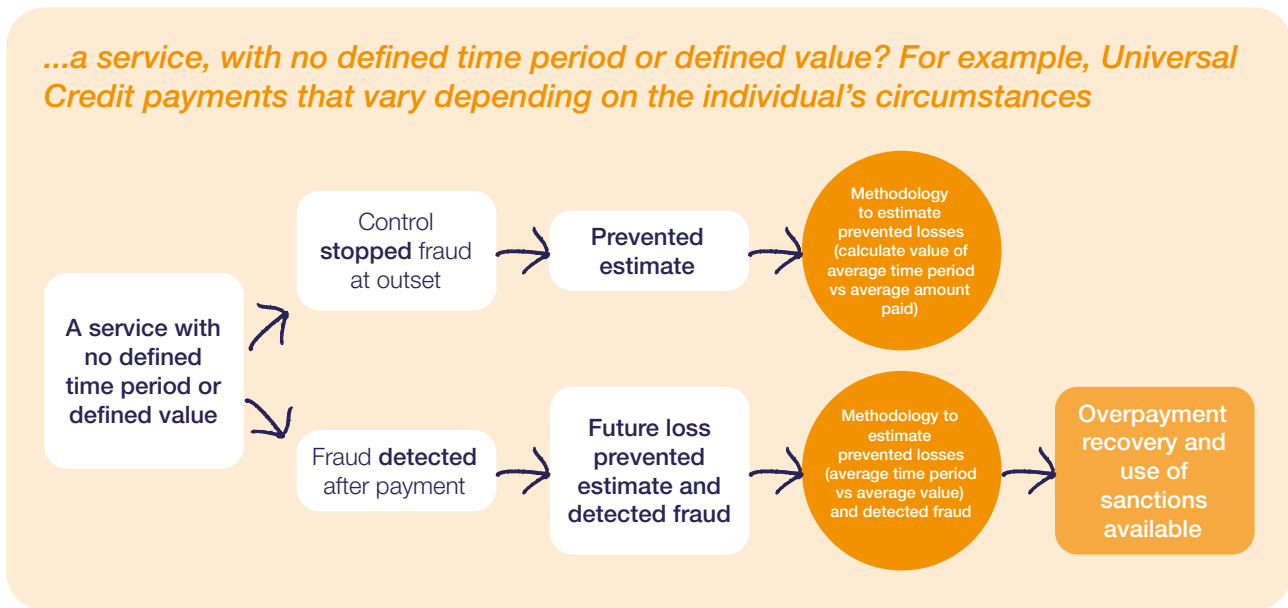


Figure 10. Flowchart for reporting prevented fraud without a fixed or defined value or time period.

A prevention methodology for prevented fraud is a multiplier applied to the weekly or monthly or annual figure, for projected fraud losses had the control not been put into place or, if action had not been taken. Assumptions should be made using the risk assessment residual risk score, on the likelihood of the fraud occurring if the control had not been implemented. This will be the basis of the prevention methodology.

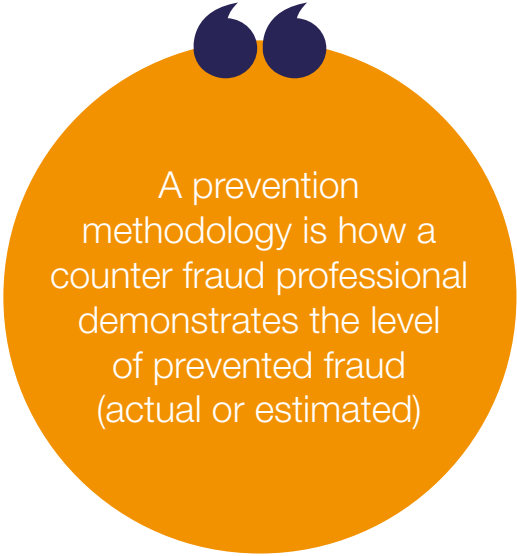
A prevention methodology for future loss prevented is a multiplier applied to the weekly or monthly or annual value of the future loss prevented by the control, implemented after fraud has been detected²⁷. The multiplier will vary according to the specific fraud type and the level of controls that exist. This is because the level of control has a direct bearing on the likely time the fraud would have continued before these controls would have identified and stopped the loss.

A prevention methodology is how a counter fraud professional demonstrates the level of prevented fraud (actual or estimated), prior to a control being implemented or when controls were designed.

All prevention methodologies should be:

- clearly linked to the intervention
- evidence-based
- logical
- data-driven (where possible)
- reasonable


27 The value of “detected fraud” can be used to help estimate or quantify the future loss prevented.



A prevention methodology is how a counter fraud professional demonstrates the level of prevented fraud (actual or estimated)

To establish a prevention methodology, the individual should²⁸:

- establish the risk to the organisation - what is the risk to the organisation? What type of fraud? If fraud occurred, what damage could it do? (financial loss, reputational damage, victim protection compromised, physical and national security breached)
- if not obviously financial - think creatively for potential savings
- research organisational policies that are linked to the area of risk - think about bigger policies, hone in on what the control will do, ways in which the control could affect that risk area - are there any contra indications?
- establish the percentage chance of the fraud occurring - use all available evidence to establish the likelihood of the fraud occurring
- seek advice from practitioners - early engagement with staff working to deliver the service helps build a picture of how the service is used
- research all available statistics linked to the components that may make up a methodology - for example, costs, frequency and/or duration; national, organisational and/or stakeholder groups - establish all available data
- collate all information - consider quantifying the potential savings
- make evidence-based assumptions on the time period to be included in the prevented fraud calculation
- evidence the link between the control or intervention and the saving
- estimate the level of savings that could be made based on the control being implemented - factor in any third party influence - adjust accordingly
- set review dates proportionate to the control
- undertake retrospective testing - ensure that it is the control that is making the saving
- review the methodology (if required)



If not obviously financial - think creatively for potential savings

28 Although every step should be considered, steps may not apply depending on the type or complexity of the savings being quantified.

Prevented actuals²⁹ should be reported when a fraud has been prevented from occurring and the actual value of the fraud is known. If part of the money has been paid out and the rest stopped due to fraud, the amount paid out should be reflected in the detected and/or recovered fraud category and the known future payments stopped, due to counter fraud activity, should be reflected within prevented actuals.

Example 1

An application for a one-off grant of £10,000 is received. A whistleblower contacts the organisation with information indicating the application is fraudulent. This is reviewed pre-payment and a payment that otherwise would have been made, is stopped. The actual prevention reported is £10,000.

Example 2

An application for a one-off grant of £10,000 is received, processed and the first instalment of £2,500 is paid. A whistleblower contacts the organisation with information indicating that the application was fraudulent. This is reviewed and it is determined that fraud has taken place, meeting the civil test. Subsequently recovery action takes place and £2,500 is repaid. Detected fraud of £2,500 is reported. Actual prevention of £7,500 is also reported. Recovered fraud of £2,500 is also reported.

Prevented estimates are where the value of prevention savings are not immediately obvious and require some form of estimation or modelling to derive an appropriate value. This could be when a control is put in place to prevent fraud, and the amount of fraud the control prevents is estimated via seeing reduced losses through fraud measurement. It can also be when an ongoing fraud is detected and future payments are stopped as a result, yet we do not know the exact quantum of the future payments so this needs to be estimated.

Example 1

Fraud and error loss was measured on a £10m a year payment stream at a rate of 4%. A preventative control, where new data to prove the accuracy of the claim, was introduced as part of the application process. Fraud and error loss is measured post-implementation at a rate of 2%. The reduction in losses from 4% to 2% is calculated at £200,000. The £200,000 saving is reported as a prevented estimate.

Example 2


Fraud is detected by using data matching to identify a business that had falsely declared property ownership, when applying for an ongoing annual grant of £50,000. All fraudulent claims are stopped, and the value of the amount prevented has to be estimated. Data is obtained to show the average length of claim is three years, and the fraud was stopped after one year. A saving of £100,000 is reported as a prevented estimate.

²⁹ Prevented Actuals and Prevented Estimates terminology from Consolidated Data Request (CDR) Guidance - this can be requested from: APM@cabinetoffice.gov.uk

C15. Business Process Mapping

Business process mapping should be used in conjunction with fraud risk assessments. Business process mapping³⁰ should be used to gain a full understanding of processes, as well as to proactively seek identification of where and how fraud could enter the system.

Business process mapping provides a concise picture of all steps that need to be taken to deliver a product or service from start to finish, and it details relationships with other processes and areas. In particular, it is a visual aid to highlight weaknesses in existing processes and controls for future action.



Business process mapping provides a concise picture of all steps that need to be taken to deliver a product or service from start to finish

The counter fraud professional (CFP) should:

- engage with all stakeholders involved in the process, to ensure a clear understanding of all the steps required, and it should contain sufficient detail to understand the fraud opportunities in the process, and how effective existing control measures are in preventing and deterring this
- research organisational guidance, processes, staff training and other areas to understand the wider picture and how existing fraud risks are connected - understanding the actions the fraudster is required to take and the lifecycle of any possible fraud, will aid the understanding of how parts of the process could be exploited to commit fraud
- understand the controls already in place in response to the risk or fraud, to give clarity to potential areas of weakness
- cross reference the complete business process map with the fraud risk assessment to pinpoint where fraud and associated error can enter the system and highlight areas to strengthen or develop prevention controls
- apply a fraud mindset - to think like a fraudster, discover the ways in which the process could be exploited - this will help when reviewing the process, to identify where and how existing controls can be strengthened or new prevention controls implemented
- regularly review and update the process map to ensure relevance to current processes and risks

30 Products section D3 has further information on conducting a business process mapping exercise.

C16. Business Analysis, and the Use of Data Analytics³¹

Business analysis³² should be used when developing new controls, as well as when evaluating existing controls that are already identifying areas of weakness.

The process outlined reflects a general approach to delivering counter fraud data analytics. This process should be adapted according to the fraud risks being addressed and the organisation's counter fraud data analytics requirements.

Business analysts³³ can help teams to:

- analyse and understand a business risk or opportunity
- undertake research and analysis to understand how a business area works, considering the people, organisation, processes, information, data and technology
- identify areas for improvement, explore feasible options, analyse the effects of change and define success measures
- identify and elaborate user and business needs to enable effective design, development and testing of services and business change
- make decisions related to prioritisation and minimum viable product by using analysis-led insights
- ensure new products and services meet business and user needs, and are aligned with organisational goals
- understand any business and policy constraints that need to be considered, and assess the implications

Data analytics can be a powerful tool for maintaining the integrity of processes and systems and preventing fraud.

For example, matching and analysing data can be used for, but not limited to:

- risk-scoring applications to streamline processes, and directing high risk applications to different pathways for additional checks
- monitoring and flagging high-risk transactions, such as changes to bank details, prior to payment
- quantifying instances of fraud and associated error being prevented and detected on an organisational, departmental scheme or service level
- identifying and calculating the benefit from improvements to existing business processes that prevent, identify and detect instances of fraud and associated error
- testing for and measuring levels of undetected fraud and associated error - gaining further assurance of current estimated levels of fraud and associated error
- enabling more informed and transparent conversations within the organisation on its fraud risks and the material nature of the threat they present to the organisation
- testing new approaches to preventing, identifying, detecting and measuring potential fraud and associated error

All counter fraud data analytics processes and activities should be regularly reviewed and evaluated to ensure they are of the required standard and remain current.

31 Further information can be found in the publication: Best-Practice Guidance for Implementing Data Analytics to Counter Fraud in Government. This can be requested by emailing: gcfp@cabinetoffice.gov.uk

32 Business analysis can be described as: an approach focussed on identifying business needs and determining solutions to business problems.

33 <https://www.gov.uk/guidance/business-analyst--2>

Engagement with data teams

It is accepted that organisational structures will differ across organisations. In some organisations the counter fraud professional (CFP) may also be the person undertaking the data and analytical processes.

When engaging counter fraud data analytics teams, factors to consider include:

- what is the purpose of engaging?
- how are the individuals or teams identified?
- how can the engagement be mutually beneficial?
- what is the most appropriate mechanism for engagement?
- what value does the use of data analytics add?

The CFP should work with the data analytics team in exploring risks to understand the underlying issue(s), exploring how controls could still allow fraud to occur, highlighting where new prevention controls are required and identifying how prevention solutions could be embedded.

This activity may include, but is not limited to:

- how and where could the fraud occur within business processes?
- what is it about the activity that makes it fraudulent?
- how likely is the fraud to occur and to what extent?
- can data analysis be utilised to identify and prevent this fraud?
- any other information needed to understand how data analytics can provide insight

Data analytics and ethics³⁴

When undertaking data analytics, all stakeholders engaged in this process must behave ethically and safeguard the data at all times from unauthorised use and disclosure. Data analytics should be approached with:

- an open mind with no preconceptions
- the appropriate knowledge, skills and competence to undertake the work
- integrity when undertaking all work and associated analyses
- objectivity and honesty when presenting the results from data analysis - data tables and reports should be prepared in a way that minimises the risk of misinterpretation

CFPs should be aware of the impact data quality³⁵ can have on findings and should recognise that some of the anomalies raised by data analytics will be false positives. They must, therefore, carry out discrete checks on all anomalies raised by data analytic routines prior to making any conclusions about whether fraud is present.



34 See the <https://www.gov.uk/government/publications/data-ethics-framework> for more information on how public sector organisations should use data appropriately.

35 <https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework>

C17. Stakeholders

Individuals should identify, build and maintain effective internal and external stakeholder relationships to successfully design, build and embed fraud prevention solutions.

It is important that interoperability³⁶ exists between the counter fraud professional (CFP) and identified stakeholders. This ensures organisational practices, policies, technological requirements, legal and organisational aspects are considered. This develops efficient collaboration between individuals and organisations.

Interoperability can be achieved by:

- having clear common goals and expectations to promote a mutual understanding
- transparency between teams and organisations
- empowering individuals with new skills and trusted collaboration
- sharing functionality and accesses where possible
- collaborating beyond internal silos

They should clearly identify which stakeholders are required to progress prevention activities. This can be achieved through stakeholder mapping.

Stakeholder mapping will highlight key stakeholders who have the ability to influence the prevention activity and take the necessary actions to implement fraud prevention within their part of the business.

A stakeholder management plan should be prepared and reviewed regularly ensuring the relevance of all stakeholders to the wider prevention environment.

When engaging with stakeholders, they should clearly identify:

- what is the objective to achieve?
- who will be critical to your success with the ability to influence change?
- how will engagement with them take place?
- has this engagement met the pre-set objectives? - if not, ask who else needs to be involved and what else might be required - the answers to these questions require continuous evaluation

The CFP is not expected to conduct the full range of prevention activities.

Some specialist areas may need to be undertaken by expert stakeholder teams, for example: data analysis teams or behavioural science teams.

Where this is the case, the involvement of two or more teams should be overseen by a protocol document or memorandum of understanding (MOU).

³⁶ Interoperability can be described as: how people, systems and processes talk and work together across organisational structures and professions, supported through technology.

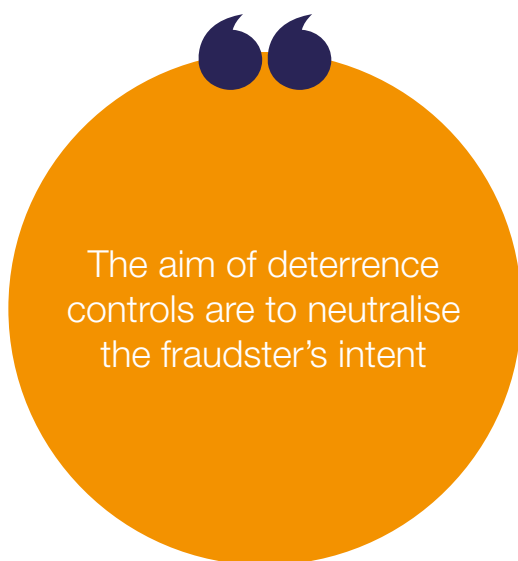
C18. Behavioural Science³⁷

Public messaging can change behaviour by changing beliefs about situations, risks and benefits. A person who otherwise would have been motivated to defraud organisations, may be deterred from doing so, through minimising their ability to rationalise fraudulent behaviour.

This can be done in three ways:

- increasing the level of perceived risk of committing fraud (for example, communicating the likelihood that they will be caught)
- reducing the perceived benefit of engaging in fraud (for example, showing the consequences if they are caught)
- influencing emotions and appealing to moral identity (for example, making them aware of the impact their actions have on others)

Applying a counter fraud lens to existing messaging about organisations can strengthen it without changing the focus or tone.



C19. Deterrence

The aim of deterrence controls are to neutralise the fraudster's intent. The individual should work with behavioural scientists and communications teams to successfully embed deterrence controls and messaging throughout the organisation.

Deterrence can be characterised in many cases as:

“I would commit this fraud. I could do it, and have no moral objection, but I have no intent because I fear x”

or

“I could commit fraud, but the complexity or cost to undertake it is too high in comparison to the return on my investment, which makes this fraud unappealing”

They should embed deterrence controls throughout business processes to deter fraudulent intent. This may include, but is not limited to:

- clear consequences of non-compliance
- statements communicating that fraud is an offence
- statements communicating that the organisation will actively detect fraud and take action
- statements communicating that the organisation will consider applying sanctions, including criminal prosecutions, where appropriate
- statements to influence emotions appealing to morals and ethics (such as, how fraud impacts victims)

Thinking about compliance behaviour, the table below assists in addressing the actual causes of non-compliance, rather than its outcomes.

37 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60539/BIT_FraudErrorDebt_accessible.pdf

Understanding Compliance Behaviour

	Status	Attitude	Behaviour	Approach	Action	Tool	
HIGH	Voluntarily complies	*Willing to do the right thing *Committed	Compliance orientated	Make it easy	Guide and support	*Compliance checks Information	LOW
Percentage %	Accidental non-compliance	Tries to do the right thing but does not always succeed *Careless	Attempting to comply	Help to comply	Educate and provide feedback	*Audits *Workshops *Notices	Cost
	Opportunist non-compliance	*Does not want to do the right thing *Resistant	No sign of intention to comply	Deter by detection - fear of being caught	Correct behaviour according to severity	*Monitoring *Inspections *Notices *Infringements	
	Intentional non-compliance	*Has decided not to comply *Disengaged	Deliberate intention not to comply	Use the full force of the law	Deter by punishment - fear of consequences	Investigation	

Figure 11. Understanding compliance behaviour³⁸.

Accordingly, a structured and evidence-based risk management approach can be used to determine compliance intervention priorities and actions. Seeking to understand the reasons for non-compliance and respond accordingly and by identifying and deterring those who choose not to comply.

38 Adapted from the Australian Maritime Safety Authority <https://www.amsa.gov.au/amsas-compliance-strategy-2023-2027/understanding-compliance-behaviour>

C20. Communications³⁹

Successful fraud prevention and deterrence requires clear communications to stakeholders, internal and external.

The individual should be aware of the organisation's communications strategy and structure and how it interacts with the counter fraud programme. Some organisations will have a dedicated communications team that should be a key stakeholder in the implementation of prevention controls.

Communications purposes can be explained using the CORE model:

- Changing behaviour
- Operational effectiveness
- Reputation management
- Explaining policies

To ensure effective communication, they should consider the purpose and intended audience of the communication:

- **external communications** - build and maintain relationships with individuals and external organisations for public benefit
- **marketing** - raise awareness of policies, influences, attitudes and behaviours, supporting the operation of services
- **internal communication** - engage with staff delivering operational priorities and support organisational and cultural change
- **strategic communication** - set, co-ordinate and guide the implementation of activity based on insight, as part of an overarching plan - to deliver against agreed priorities, to measurable effect
- **media** - contribute to media management, input could include proactive and reactive handling of the press, relationship management and content creation, insight and evaluation

When communicating change, the 4Ps⁴⁰ of communication should be considered. The 4Ps are:

- **Purpose** - explain why we are doing what we are doing
- **Picture** - tell people what the change will look and feel like when we reach our goal
- **Plan** - tell people how we will get from A to B
- **Part** - explain what people need to do to help make the change a reality and a success

The Behavioural Insights Team provides the following advice for simplifying public messages:

- make sure that the key message is presented early
- keep language simple
- be specific about recommended actions
- provide a single point of contact for responses
- remove all information that is not absolutely necessary for performing the action⁴¹

Breaking down complex processes into simple, logical and easy steps can also help people to understand what to expect.

Behavioural science offers an approach to prevent fraud from happening in the first place. In order to do so they should:

- undertake a review of existing communication methods to identify where fraud messaging could be applied
- pilot the change to confirm the effectiveness
- if effective, rollout across the organisation or business line

39 Further information relating to communications can be found at <https://gcs.civilservice.gov.uk>

40 <https://gcs.civilservice.gov.uk/guidance/internal-communication/using-internal-communications-to-support-change/>

41 The Behavioural Insights Team <https://www.bi.team/publications/east-four-simple-ways-to-apply-behavioural-insights/>

C21. Maximise the Effect of Fraud Messaging⁴²

The following advice should be considered for maximising the effectiveness of fraud messaging:

- **prompt people when they are likely to be most receptive:** consider where and when in the programme or policy process you include your fraud messaging. It should be when a claim is initiated, approval is sought or for any other notifiable events and changes that impact on ongoing eligibility
- **attract attention:** people are more likely to do or engage with something that draws their attention - consider the use of images, colour or personalisation in combination with deterrence messaging
- **use plain language and direct questions:** presenting information using plain and direct language increases response rates - also, simple and binary questions make it more difficult for a person to rationalise providing false or misleading information
- **reinforcing positive social norms showing that most people perform the desired behaviour:** communicating that most people perform a desired behaviour (for example, do not defraud, behave honestly, report fraud) encourages others to do the same, because social norms often guide behaviour
- **order effect:** the order in which things are presented influences our choices - place deterrence messaging upfront in a claim or application form
- **make reporting fraud easy:** if the effort required is high, it can put people off reporting suspected fraud - providing obvious links and direct avenues for responding to and reporting suspected fraud can increase responses

Fraud messaging can be used and adapted to help with fraud communications, such as:

- creating website content
- preparing talking points or media releases
- developing content for social media channels
- designing processes, application forms, contracts

C22. Measure, Monitor and Evaluate Effectiveness⁴³

The Government Counter Fraud Profession's Fraud Measurement Standard should be followed to identify the knowledge, skills and experience required when:

- measuring and estimating levels of fraud and associated error
- reporting instances of prevented and detected fraud and associated error

All prevention controls must be measured, monitored and evaluated to establish the successful outcomes and cost effectiveness. The use of the SMART model (see table) will ensure effectiveness of controls.

The following table outlines the 'SMART' principle which can be applied to help co-design controls with key risk stakeholders:

42 <https://www.bi.team/publications/east-four-simple-ways-to-apply-behavioural-insights>

43 The HM Treasury Magenta book gives a detailed methodology and guidance for evaluation within government. It gives clear guidance on when and how to evaluate outcomes using a variety of methods. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/879438/HMT_Magenta_Book.pdf

Specific	The control should have a clear and concise objective. It should also be well defined and clear to anyone with a basic knowledge of the work. Consider: who, what, where, when and why.
Measurable	The control and its progress should be measurable. Consider: <ul style="list-style-type: none"> • what does the completed control look like? • what are the benefits of the control and when will they be achieved? • the cost of the control (both financial and staffing resources)
Achievable	The control should be practical, reasonable and credible and should also consider the available resources. Consider: <ul style="list-style-type: none"> • is the control achievable with available resources? • does the control comply with policy and legislation?
Relevant	The control should be relevant to the risk. Consider: <ul style="list-style-type: none"> • does the control modify the level of risk (through impacting the causes and consequences)? • is the control compatible with the organisation's objectives and priorities?
Timed	The control should specify timeframes for completion and when benefits are expected to be achieved.

Preventing fraud is an iterative process. The individual should measure prevention success by:

- baseline levels of fraud using fraud measurement results
- implement controls or interventions
- remeasure the fraud levels
- review the results
- evaluate the effectiveness of the control or intervention
- adjust or change the controls or interventions, if required
- remeasure, review and evaluate as required

Comparison of the results could take time to gather a meaningful measurement.

They should conduct a fraud related cost-benefit analysis⁴⁴ of all proposed changes and the prevention controls needed to minimise fraud risk. Questions to ask when undertaking a cost-benefit analysis⁴⁵ include, but are not limited to, the following:

- do the proposed interventions provide value for money?
- by investing in a preventative approach, can local partners reduce the levels of fraud and therefore increase budgets?
- what is the payback period for the project and is this short enough to invest, based on a spend to save approach?
- where an organisation invests in a programme or project or pilot, to what extent are other organisations likely to benefit?
- are the impacts of a proposal financial, or a matter of public interest or confidence?

Prevention controls should aim to reduce fraud to the lowest feasible level. This is the level defined by the National Audit Office as reached when the cost of preventative controls exceeds the amount of prevented fraud savings.

44 Products section D6 has further information on conducting a cost-benefit analysis exercise.

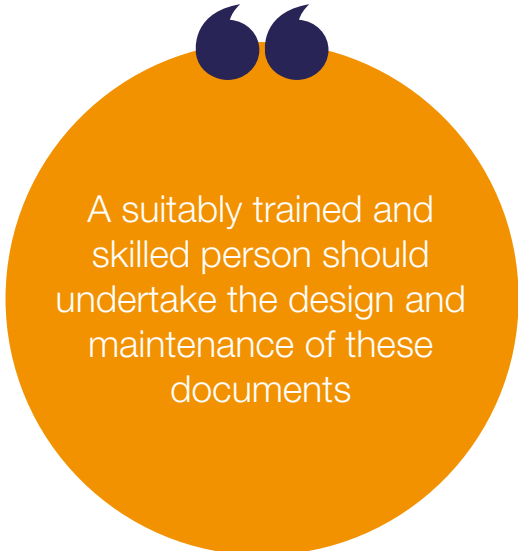
45 A detailed methodology for cost-benefit analysis is within the HM Treasury Green Book. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1063330/Green_Book_2022.pdf

D. Guidance on Products

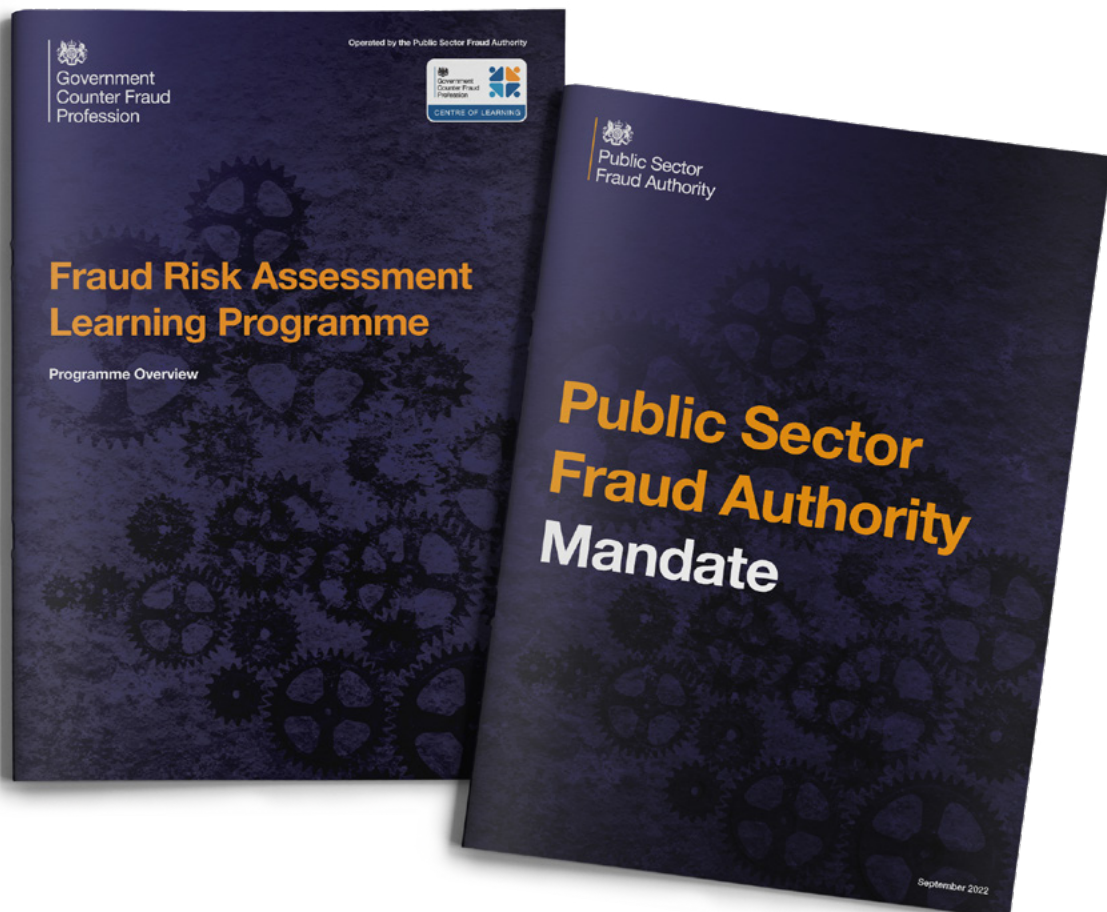
D1. Introduction

This guidance covers what good quality products should include to enable an effective fraud prevention response and strategy for government. The design and content of these documents should be unique to the organisation's activities, factors to be taken into consideration include:

- the nature of the organisation's activities, internal and external context
- the size and complexity of the organisation
- geographical location of these activities
- the breadth and depth of its supply chain
- who it does business with



A suitably trained and skilled person should undertake the design and maintenance of these documents



D2. Products for Fraud Prevention Found in Other Government Counter Fraud Professional Standards

Within the Government Counter Fraud Profession's (GCFP's) Standards, there are a variety of products that should be used fully when developing a successful fraud prevention programme.

Product	GCFP Standards
Strategy - counter fraud strategy and fraud control strategy which include the strategy management cycle	Leadership, Management and Strategy (LMS) Standards ⁴⁶
Annual Action Plan that includes the operational management cycle	LMS Standards
Counter Fraud Policy	LMS Standards
Fraud Response Plan	LMS Standards
Communications Plan	LMS Standards
Annual Reports	LMS Standards
Stakeholder Mapping	LMS Standards
Fraud Risk Assessment (FRA) <ul style="list-style-type: none"> organisational (enterprise) fraud risk assessments thematic (grouped) fraud risk assessments initial fraud impact assessments (FIAs) full fraud risk assessments 	Fraud Risk Assessment Standards ⁴⁷
Risk scoring matrix	FRA Standards
Risk prioritisation and heat maps	FRA Standards
Fraud measurement, calculation and reporting process	Fraud Measurement Standards ⁴⁸

46 LMS Standards can be obtained by emailing: gcfp@cabinetoffice.gov.uk

47 Government Counter Fraud Professional Fraud Risk Assessment Standards - <https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government>

48 Government Counter Fraud Professional Fraud Measurement Standards can be obtained by emailing: gcfp@cabinetoffice.gov.uk

Developing a fraud prevention programme may require cross-functional working. The following functional standards cover the expectations of relevant functions that could aid the counter fraud professional.

Functional Standards ⁴⁹	Standard Number	
	<p>Government functions - sets expectations for the direction and management of functions across government.</p>	<p>GovS 001</p>
	<p>Project delivery - sets expectations for the direction and management of portfolios, programmes, and projects in government.</p>	<p>GovS 002</p>
	<p>Digital, Data and Technology - sets out how all digital, data and technology work and activities should be conducted across government.</p>	<p>GovS 005</p>
	<p>Finance - sets expectations for the effective management and use of public funds.</p>	<p>GovS 006</p>
	<p>Security - sets expectations for the planning, delivery and management of government security activities.</p>	<p>GovS 007</p>
	<p>Communication - sets expectations for the management and practice of government communication in order to deliver responsive and informative public service messaging.</p>	<p>GovS 011</p>

49 Functional Standards - <https://www.gov.uk/government/collections/functional-standards>

D3. Business Process Mapping

Business process mapping identifies potential fraud risks within an established process. It can be conducted at any time and is not limited to a full fraud risk assessment.

Individuals should work with stakeholders with expertise within the specific part of the business detailing the who, what, when, where and how.

Analysing each step in a process will show where a fraud risk can develop and what implications new controls could have.

The business process map below illustrates potential fraud risks in an invoice payment process and where additional fraud prevention controls should be considered.

Process maps provide valuable insight into how an organisation can improve processes by including prevention controls.

Identify the problem	What is the process that needs to be visualised?
Discuss and consider activities involved	At this point, sequencing the steps is not important, but it may help you to remember the steps needed for your process. <ul style="list-style-type: none"> • decide what level of detail to include • determine who does what and when it is to be done
Define boundaries	Where or when does the process start? Where or when does the process stop?
Determine and sequence the steps	It is helpful to have a verb to begin the description. You can show either the general flow or every detailed action or decision.
Draw basic flowchart	See figure 7.
Finalise the process flowchart	Review the flowchart with other stakeholders (team members, supervisors, suppliers, customers, and so on) for agreement. Make sure important chart information, like a title and date, is included - which will make it easier to reference.
Helpful questions to ask	Consider: <ul style="list-style-type: none"> • is the process being run how it should be? • will team members follow the charted process? • is everyone in agreement with the process map flowchart? • is there anything redundant? • are there any steps missing? • are there opportunities to prevent fraud?

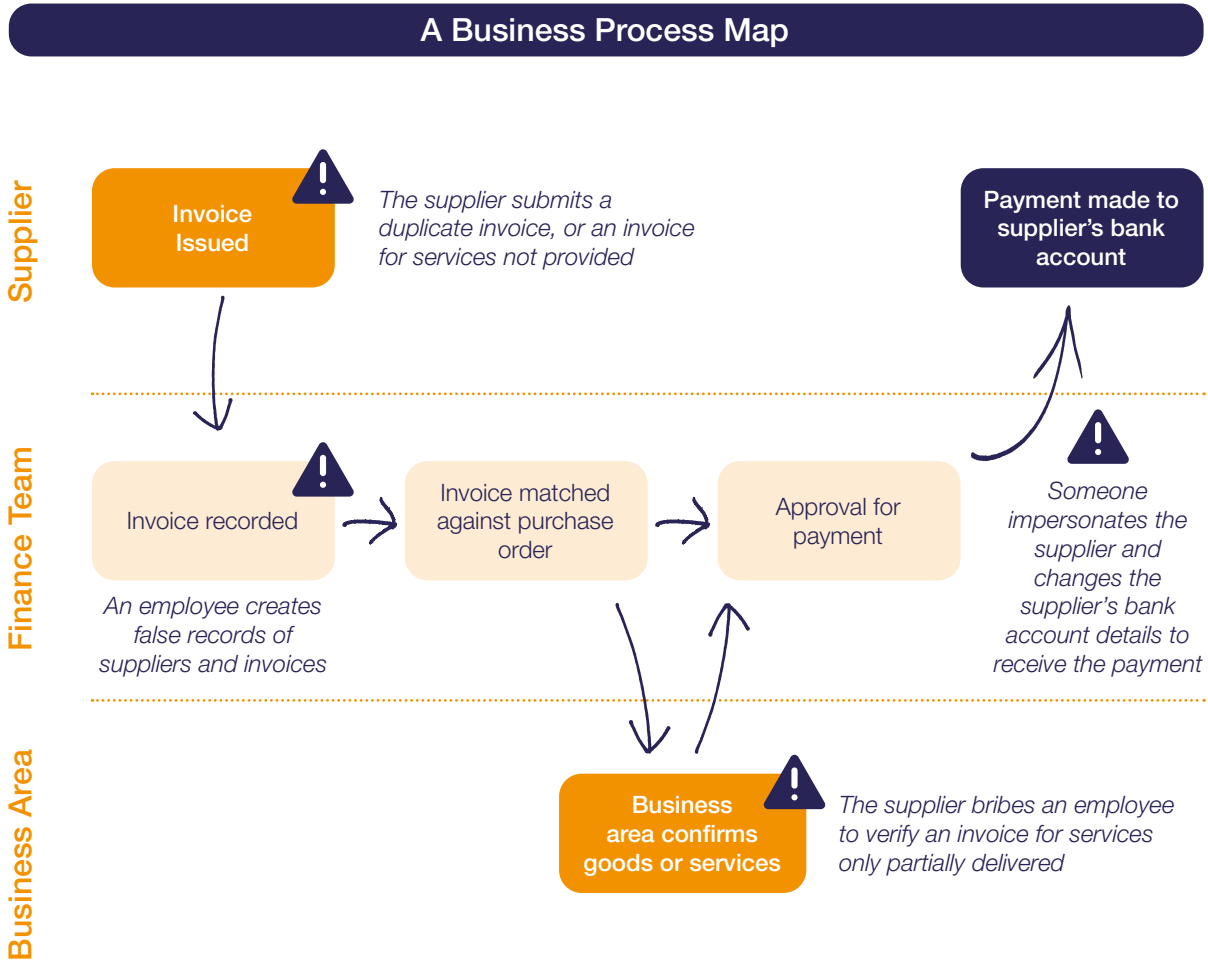


Figure 12. An example of a business process map.⁵⁰

50 Adapted from the Commonwealth Fraud Prevention Centre publication: Fraud Risk Assessment <https://www.counterfraud.gov.au/sites/default/files/2022-04/fraud-risk-assessment-leading-practice-guidance.PDF>

D4. Protocol Documents

Individuals will need to work collaboratively with other parts of the organisation or external partners.

Where this is the case, the involvement of two or more teams should be overseen by a protocol document or memorandum of understanding (MOU). Although not legally binding, a protocol document or an MOU, clearly defines the ways that the parties will work together and sets clear expectations and escalation routes.

A protocol document should contain the information listed in the following table.

<p>Scope and objectives</p>	<p>Detail which departments, organisations teams and counter fraud activities the protocol document will apply to.</p> <p>Provide clear objectives and desired outcomes as part of the joint working interactions between the covered parties.</p> <p>Include details of policies that will impact the work.</p>
<p>Defined roles and responsibilities</p>	<p>Clear, defined responsibilities must be documented to ensure consistency and avoid conflicts.</p> <p>Consideration should be given to priorities of actions and overall leading of the counter fraud activities.</p> <p>Clear details of how each party will impact or contribute to the fraud action plan and strategy should be recorded.</p>
<p>Information or intelligence sharing processes</p>	<p>What data, information and intelligence can be shared, which legislation or policies and processes to allow sharing and storage procedures of intelligence, should be documented.</p> <p>Who will be responsible for sharing information and when.</p>
<p>Working processes</p>	<p>The protocol document should be clear on joint working processes, procedures and co-operation required to be effective in meeting the objectives.</p>
<p>Monitoring and review</p>	<p>There should be clear review processes detailed for the protocol document, including responsibility for the review and timelines.</p> <p>It should detail how effectiveness can be reviewed and how to identify barriers and conflicts.</p> <p>It needs to include how the protocol document will be revised if required.</p>

D5. Control Assessment Tool⁵¹

Not all fraud controls have the same impact on the management and reduction of the risk. Some fraud controls, such as authentication controls, may be absolutely critical to the management of the risk, while other fraud controls may only have a minor impact on the risk. The control assessment tool may help the individual assess the value of fraud controls.

The tool uses a rating system against 4 criteria to help inform control criticality assessments. These 4 criteria are: probability, frequency, duration and impact, each criterion and its ratings are detailed on the next page.



Rating

The tool calculates a rating between 'absolutely critical' to 'little or no impact', using the highest score from the 4 criteria.

- 5 **absolutely critical** - to the management and reduction of the risk

- 4 **very important** - to the management and reduction of the risk

- 3 **important** - to the management and reduction of the risk

- 2 **has some impact** - on the management and reduction of the risk

- 1 **has little or no impact** - on the management and reduction of the risk

Probability – the likelihood of fraud occurring if the control is ineffective or partially effective

- 5 fraud is certain to happen if control is ineffective or partially effective
- 4 fraud is almost certain to happen if control is ineffective or partially effective
- 3 fraud is likely to happen if control is ineffective or partially effective
- 2 fraud is possible to happen if control is ineffective or partially effective
- 1 fraud is unlikely to happen if control is ineffective or partially effective

Frequency – the frequency of fraud occurring if the control is ineffective or partially effective

- 5 likely to be a substantial number of instances of fraud if control is ineffective or partially effective
- 4 likely to be several instances of fraud if control is ineffective or partially effective
- 3 a number of instances of fraud likely to occur if control is ineffective or partially effective
- 2 a few instances of fraud likely to occur if control is ineffective or partially effective
- 1 fraud will be infrequent if control is ineffective or partially effective

Duration – the length of time fraud could remain undetected if the control is ineffective or partially effective

- 5 fraud could remain undetected if control is ineffective or partially effective
- 4 fraud could go undetected for a long duration if control is ineffective or partially effective
- 3 fraud could go undetected for a period of time if control is ineffective or partially effective
- 2 fraud should still be prevented or detected quickly if control is ineffective or partially effective
- 1 fraud should still be prevented or detected immediately if control is ineffective or partially effective

Impact – the impact of fraud if the control is ineffective or partially effective.

- 5 could have an extreme impact if control is ineffective or partially effective
- 4 could have a major impact if control is ineffective or partially effective
- 3 could have a moderate impact if control is ineffective or partially effective
- 2 could have a minor impact if control is ineffective or partially effective
- 1 could have an insignificant or trivial impact if control is ineffective or partially effective

D6. Using Root Cause Analysis⁵²

Root cause analysis (RCA) is the use of a clearly defined methodology to investigate the causes of a problem.

Properly completed, an RCA will uncover all of the factors underlying a problem, help to identify other related risks and suggest appropriate solutions. RCA methodology combines basic principles with a series of connected techniques, in order to identify the factors that go into the successful performance of a process or system and where factors can combine to cause failure.

A Root Cause Analysis (RCA) can be used to highlight the cause of any policy, programme, system, process or control failures. An RCA can also identify the reason(s) for failure and can focus on the necessary remedial actions - including the design and implementation of new controls.

An RCA can be conducted in a variety of ways, one approach is the ‘5 whys technique’.⁵³

The ‘whys’ have identified that the initial design phase of the scheme did not include all relevant fraud risks. The control and monitoring routines built into the system were incomplete from the inception of the scheme.

Result

Action can now be taken to reduce fraud in this scheme by:

- updating the underlying scheme documentation
- identifying and designing a new control
- monitoring routines needed
- instructing system developers to make the necessary modifications through the approved change control process

Problem statement	<i>The new scheme has a high level of fraud.</i>
Ask why 5 times to delve into the root cause of the failure.	
Why is fraud occurring?	Information is not being verified
Why is information not verified?	The system does not ask for verification
Why is verification not requested?	It is not a built-in requirement
Why was it not built into the system?	That was not in the design criteria for the scheme
Why was it not in the design criteria?	There was insufficient understanding of scheme fraud risks at the design stage
Root cause of the problem	<i>There was an insufficient understanding of scheme fraud risks at the design stage.</i>

52 <https://www.gov.uk/government/publications/the-government-data-quality-framework/the-government-data-quality-framework-guidance#data-quality-root-cause-analysis>

53 The ‘5 whys technique’ is attributed to Sakichi Toyoda, founder of Toyota Industries Corporation.

D7. Cost Benefit Analysis⁵⁴

Cost benefit analysis⁵⁵ is a process through which rational and justifiable decisions can be made in relation to a policy, programme, scheme, service, project or other form of activity. It is broken down into 5 basic steps.

Describe - set out the process	Describe what you are trying to achieve and how you will go about it. This is known as a theory of change, a logic chain or a logic model.
Measure - quantify costs and benefits	There are three different types of cost which need to be considered: capital costs ⁵⁶ , day-to-day expenses, such as salaries ⁵⁷ , and in-kind costs ⁵⁸ .
Identify - assess the timing of your benefits and who benefits	What is the time horizon for your analysis? One year? Five years? Twenty-five years? And when are costs incurred and benefits realised?
Calculate - the ratio between your costs and the different types of benefit	Put all the data you have collected in a spreadsheet (there are multiple free templates available online).
Present - communicate what the figures mean	Having filled in all the elements of the cost-benefit analysis, look again at all your key assumptions and ensure that these are explained as fully as possible.

54 A detailed methodology for Cost-Benefit Analysis (CBA) is within the HM Treasury The Green Book - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1063330/Green_Book_2022.pdf

55 A systematic process for evaluating the desirability of a decision by weighing its potential benefits and costs.

56 Capital costs are those expenditures on assets which are expected to last more than one year and are used in delivering the associated activities.

57 Day-to-day expenses are those costs incurred as a result of the relevant programme or activity.

58 In-kind costs are contributions to a programme or activity which are of value but not charged to it.

D8. Lessons Learnt Reviews⁵⁹

Lessons learnt reviews on controls should include:

- the objectives set
- the outcomes achieved
- the successes
- the areas for further work
- recommendations for change or matters that require executive level discussion

The review report should contain explicit recommendations, with clearly defined responsibilities and timelines for action, and a process for escalation to executive level within the organisation. Review findings should be shared with stakeholders, including across government functions, if appropriate.

Utilising lessons learnt when considering prevention or deterrence controls

Lessons (both positive and negative) should be collected, recorded, written up and communicated, as part of the formal process.

Lessons learnt process includes 5 steps as shown below.

Identify	Identify comments and recommendations that could be valuable for future controls.
Document	Document and share findings within the organisation (and wider).
Analyse	Analyse and organise lessons learnt to see how they can be applied going forward.
Store	Store lessons learnt for future use.
Retrieve	Retrieve applicable lessons learnt for review or use on new controls.

Lessons learnt reviews can take any format; however, they should include:

- **event or activity** - describe what actually happened - for example, how a fraud occurred, how it was detected, investigated and dealt with
- **outcome** - describe the result of the event or activity and detail what went well, what didn't go well - for example, the prevention control inadvertently uncovered some loopholes in processes or policies that had been exploited, enabling the fraud
- **impact** - what was the impact of the actions or outcome on the investigation or project - for example, a shortcoming in current procedures allowed money to be obtained fraudulently
- **lessons or recommendations** - what would you repeat? What would you do differently? How can the actions be changed? For example, what changes need to be made to prevent a similar occurrence in other parts of the organisation?

Reports from lessons learnt exercises should be used to consider further controls and/or ensure that the functional lead is aware of any residual risk.

Lessons learnt reports could be available from a variety of sources, including, but not limited to:

- stakeholder reports
- intelligence reports
- other fraud prevention review reports
- data analytics
- investigation reports
- internal and external audit reports

⁵⁹ The Government Functional Standard GovS 013: Counter Fraud defines lessons learnt as: the practice of continuous improvement based upon organisational learning in a risk management context. <https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud>

D9. Behavioural Science Models in Communication

The purpose of the COM-B model is to identify barriers to change and introduce nudges and incentives to move towards an amended social norm⁶⁰ or norms. It explores behaviour as a result of interactions between 3 conditions that lead to a desired behaviour:

- **Capabilities** - refer to a person’s physical or psychological ability to perform the new or modified behaviour
- **Opportunities** - refer to anything in the physical or social environment that may encourage or discourage a behaviour
- **Motivations** - refer to internal reflective and automatic mechanisms that activate or inhibit a behaviour



This concept is summarised below.

Capability	Does your target audience: <ul style="list-style-type: none"> • have the right knowledge and skills? • have the physical and mental ability to carry out the behaviour? • know how to do it?
Opportunity	Does your target audience: <ul style="list-style-type: none"> • have the resources to undertake the behaviour? • have the right systems, processes and environment around them? • have people around them who will help or hinder them to carry it out?
Motivation	Does your target audience: <ul style="list-style-type: none"> • want to carry out the behaviour? • believe that they should? • have the right habits in place to do so?
Behaviour	

60 Social norms are defined as: a collectively shared belief about what others do (what is typical) and what is expected of what others do within the group (what is appropriate). See Social Norms - https://assets.publishing.service.gov.uk/media/597f335640f0b61e48000023/Social-Norms_RP.pdf

An alternative approach is to follow the EAST framework when communicating fraud messages by applying behavioural insights - make it: Easy, Attractive, Social and Timely.

Easy	<ul style="list-style-type: none"> • are you making the ask simple and straightforward, for example, by breaking bigger actions down into simple, concrete steps? • are you making the desired behaviour the default choice where possible? • are you requiring unnecessary additional effort to fulfil the task, such as, in the number of click-throughs required on online adverts?
Attractive	<ul style="list-style-type: none"> • does your communications attract attention from your target audience? • is it personalised?
Social	<ul style="list-style-type: none"> • do a majority of people already engage in the desired behaviour? Can you demonstrate that to your target audience? • could people commit to the behaviour upfront? • are you getting peers within your audience to advance your message?
Timely	<ul style="list-style-type: none"> • are you communicating with your audience when they will be most receptive to your message? • how immediate can you make the benefits of change? • can you get people to plan for future actions now?

D10. Other Sources of Information

Counter Fraud Data Analytics Best Practice Guide	Can be requested from gcfp@cabinetoffice.gov.uk
Public Sector Fraud Authority (PSFA) Prevention Panel and Methodology Bank	Information can be sought by contacting the PSFA at apm@cabinetoffice.gov.uk

E. Guidance for Organisations - Approved Professional Practice

E1. Introduction

The guidance set out below is the Approved Professional Practice for public sector organisations to help prevent fraud. In the United Kingdom, this includes aspects of mandated steps for HMG organisations as per the Government Functional Standard GovS 013: Counter Fraud and the Public Sector Fraud Authority (PSFA) mandate. Where steps are mandated, this is clearly signposted.

Fraud is the most commonly experienced crime in the United Kingdom (UK) today⁶¹ and is one of the main risks that all organisations managing public money face.

The impact of fraud on an organisation is more than just financial⁶². Fraud can directly affect how an organisation delivers its services to citizens. Fraud against organisations will redirect public funds away from vital services, into the pocket of the fraudster instead of going towards medical treatments, or healthcare staff salaries.

E2. The Government Functional Standard - GovS 013 Counter Fraud

The Government Functional Standard GovS 013: Counter Fraud⁶³ sets out the following areas, which should be followed to help understand, find and prevent fraud.

- counter fraud strategy
- annual action plans
- counter fraud and bribery and corruption policy
- fraud response plan
- assurance procedures
- fraud awareness training

Organisations should ensure that fraud prevention is specifically applied to these key areas to develop a fraud prevention programme that includes the above areas.

61 Fighting Fraud: Breaking the Chain - <https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf>

62 See the International Public Sector Fraud Forum's Guide to Understanding the Total Impact of Fraud - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866608/2377_The_Impact_of_Fraud_AW_4_.pdf

63 Government Functional Standard GovS 013: Counter Fraud - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014385/6.7628_CO_Govt-Functional-Std_GovS013-Counter-Fraud_v4.pdf

E3. Fraud Prevention Programme

Organisations should have a fraud prevention programme that is detailed in its counter fraud strategy⁶⁴, which should be approved by the organisation's management board and audit committee. In order to implement the strategy, an annual action plan⁶⁵ should be prepared.

This plan should outline those policies and procedures that are to be used to implement a fraud prevention programme and how this will reduce both fraud risk and fraud loss. This plan should identify the resources needed, the requirement for any specialist skills and the measures against which the prevention programme will be evaluated.

The fraud prevention programme should be proportionate to the level of assessed risk, be embedded into an organisation's corporate governance⁶⁶ arrangements, operate continuously and be an integral part of their internal control framework. The counter fraud functional lead (or senior responsible owner, if they hold delegated authority) should be able to determine what constitutes a proportionate response to assessed and measured fraud risk, and have this decision approved by the organisation's management board and audit committee.

Organisations should ensure fraud prevention is included in their counter fraud policy. This policy should articulate the organisation's approach to preventing fraud.

Organisations should have policies that support the delivery of the fraud prevention

programme, its assurance requirements and supporting fraud prevention procedures. These policies should be subordinate but aligned to the counter fraud policy.

Policies that support fraud prevention include, but are not limited to:

- recruitment and vetting policies and procedures
- employee code of conduct
- operational services - these will outline how the organisation interacts with members of the public using their services and products to prevent and deter fraud
- contract management
- data and information acquisition and management
- assurance on the operation of all corporate departments, systems and procedures
- whistleblowing
- dealing with the media

An organisation should also have a fraud response plan⁶⁷ that outlines the procedures that will be followed should a fraud be suspected. It should be clearly communicated to both internal and external stakeholders. Response plans should not be limited to investigations and intelligence responses only. They should include how a holistic systems approach (including root cause analysis and lessons learnt) will identify systemic issues and inform future prevention methodologies.

64 This is a recommendation under the Government Functional Standard GovS 013 for ministerial departments and public bodies. For more information see GCFP Leadership, Management and Strategy Standards.

65 Action plans are recommended under the Government Functional Standard GovS 013 and the Public Sector Fraud Authority mandate for ministerial departments and public bodies. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1104141/3042-PSFA-Mandate-V4-final.pdf


66 Corporate governance can be defined as a system of rules, processes and controls through which an organisation's activities are directed and controlled. It focuses on 4 Ps: purpose, people, process and performance.

67 Response plans are recommended under the Government Functional Standard Govs 013 and the PSFA mandate for ministerial departments and public bodies. <https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud>

The fraud response plan should detail how the prevention activities will be resourced. The budget must be consistent with what the counter fraud functional lead has defined as a proportionate response to the organisation's fraud risks.

The resources needed to complete the fraud prevention programme also extend to the tools required to undertake the work (for example, data analytics software) and access to the necessary specialist skills. These specialist skills should include, but are not limited to: risk assessment and management, data analytics, sampling, forensic accounting, cyber knowledge, system analysis and audit, legal advice and behavioural science.

Organisations are not expected to maintain all the relevant specialist skills themselves. They may enter into arrangements with other public sector bodies to share such skills or, where they exist within the Public Sector Fraud Authority, seek to use these on a call-off arrangement. Where organisations expect to share expert resources with other public sector organisations, these resource shares should be governed by an agreed memorandum of understanding.



The fraud response plan should detail how the prevention activities will be resourced

E4. Fraud Prevention – Assurance Requirements

The organisation should ensure it has processes in place to assure its prevention activities⁶⁸, areas that can be included in these processes are:

- culture
- data
- learning and development (and citizen education)
- validation
- deterrence

Typically, assurance should be on at least three separate and defined levels including:

- by or on behalf of operational management that own and manage fraud, bribery and corruption risk, to ensure that the GovS 013 standard is being used
- by or on behalf of senior management, independent of operational management; to ensure the first line of defence is properly designed, in place, and operating in line with this standard
- by independent bodies⁶⁹ to provide senior management with an objective opinion on the effectiveness of the organisation's overall counter fraud response and compliance with this functional standard

68 Assurance is recommended under the Government Functional Standard GovS 013 for ministerial departments and public bodies. <https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud>

69 Independent bodies such as the Government Internal Audit Agency - <https://www.gov.uk/government/organisations/government-internal-audit-agency>

E5. Fraud Awareness Training⁷⁰

All staff employed by the organisation should receive fraud awareness training that is proportionate to the risk profile of their role.

The International Public Sector Fraud Forum's (IPSFF's) Guide to Designing Counter Fraud and Corruption Awareness Training for Public Bodies⁷¹ recommends that a counter fraud awareness programme should:

- be endorsed by senior management
- consider job functions, roles and responsibilities
- be mandatory for all employees when joining the organisation or when being appointed to a new position
- be refreshed yearly or when targeted learning sessions are developed and delivered to address organisation-specific fraud concerns
- ensure the training is current, relevant and regularly updated
- be evaluated and measured

A training, recruitment or development programme should be implemented to ensure that counter fraud staff have and retain, appropriate skills to undertake their roles. This could involve qualification-based training, attending bespoke courses reflecting the experience of staff, or a combination of these.

Build a Counter Fraud Narrative

A clear counter fraud narrative is essential when seeking investment and engagement from stakeholders, to develop and embed sufficient controls to prevent fraud.

Building a clear narrative around information, using facts and statistics that demonstrates the benefits of fraud prevention, will present a compelling and persuasive case.

The narrative should link the organisation's future strategic priorities, with its current aims and objectives, demonstrating the importance of fraud prevention throughout.

E6. Prevention Requirements in Addition to GovS 013

Alongside the requirements of the Government Functional Standard GovS 013, organisations should continually seek opportunities to prevent fraud. This could include:

- developing a strong counter fraud culture
- applying behavioural science techniques to design out fraud
- developing and using data to prevent fraud

E7. Bribery Act 2010 (UKBA) Section 7 Failing to Prevent Bribery

Section 7 of the UK Bribery Act introduces an offence for commercial organisations where they fail to prevent bribery committed by a person associated with the organisation, where it is done to obtain or retain a business advantage.

The Ministry of Justice issues guidance on how an organisation can demonstrate they had adequate procedures to prevent bribery which an organisation can use as a defence for the section 7 offence⁷².

70 Fraud awareness training is recommended under the Government Functional Standard GovS 013 for ministerial departments and public bodies. <https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud>

71 IPSFF's Guide to Designing Counter Fraud and Corruption Awareness Training for Public Bodies - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864839/Counter_fraud_and_corruption_11.pdf

72 Guidance covering procedures relevant to commercial organisations that can be put in place has been produced by the Ministry of Justice. Bribery Act 2010 guidance - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/832011/bribery-act-2010-guidance.pdf

These adequate procedures are based on six principles:

- top level commitment
- proportionate procedures
- due diligence
- risk assessment
- communication
- training and monitor and review

Economic Crime and Corporate Transparency Bill 2022

The government is creating a new failure to prevent fraud offences, to hold organisations to account if they profit from fraud committed by their employees. This will improve fraud prevention and protect victims. Whilst there are some existing powers to fine and prosecute organisations and their employees for fraud, the new offence will strengthen these, closing loopholes that have allowed organisations to avoid prosecution in the past.

Under the new offence, an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place.

The offence applies to all large bodies, corporate and partnerships. This means that in addition to businesses, large not-for-profit organisations such as charities are also in scope, as well as incorporated public bodies.

The offence applies to all sectors. However, to ensure burdens on business are proportionate, only large organisations are in scope – defined (using the standard Companies Act 2006 definition) as organisations meeting two out of three of the following criteria: more than 250 employees, more than £36 million turnover and more than £18 million in total assets.

At the time of writing this, it was waiting to be enacted. Further information available via [GOV.UK](https://www.gov.uk)

E8. Counter Fraud Culture

Organisations should establish a counter fraud culture that develops fraud awareness throughout all counter fraud areas. Effective leadership in fraud prevention needs to be tailored to the organisation's size, management structure and circumstances.

Organisations should establish a workplace culture that encourages ethical and supportive behaviours, while discouraging fraudulent, corrupt or other criminal activities. Staff should be less able to rationalise fraudulent or criminal conduct and may be more responsive to identifying fraud and associated threats where a positive workplace culture exists. A culture built on honesty, transparency and integrity is a key organisational strength that can serve to reduce the risk of fraud from both external and internal threats.

Examples of encouraging a supportive culture within the workplace includes, but is not limited to:

- reward and recognition programmes
- health and wellbeing training and initiatives
- promoting an inclusive and supportive workplace culture
- training and promoting ethical conduct and decision-making
- open and transparent communication and decision-making
- commitment to taking action in relation to all concerns raised regarding workplace culture from staff surveys

Organisations should outwardly demonstrate to all their staff and others working with them - including all relevant stakeholders - that the Counter Fraud Function, of which fraud prevention is an integral part, has the full support of the management board and the audit committee.

There should be:

- a visible, consistent, top-down approach to fraud prevention, together with a similar attitude to business ethics and professionalism
- a commitment to protect the organisation's business and employees, this includes a 'duty of care' to ensure their staff are not put in a position where they could be compromised by accepting inappropriate gifts or inducements
- a clear policy on the acceptance and giving of gifts and hospitality, organisations should maintain a conflicts of interest register and a gifts and hospitality register - this policy should be clearly documented and circulated to employees, suppliers and clients⁷³
- an inclusive and supportive workplace, offering health and wellbeing policies and initiatives, as well as reward and recognition programmes with transparent messaging

Creating an organisational culture, based upon sound ethics and integrity, will help to effectively prevent, deter and respond to fraud.

It is essential that all staff have access to policies, documents and working practices that:

- promote the seven Nolan principles of public life⁷⁴ and expected behaviours
- encourage staff to speak up when they become aware of policy, system, procedural or control weaknesses that they work with
- emphasise the effect of fraud and the organisation's tolerance to it
- promote the organisation's response to fraud, with details of reporting lines and accountabilities
- enable staff to recognise when a fraud may be occurring
- promote a whistleblowing policy whereby all persons can raise concerns without fear of retaliation and are protected from any such actions
- advertise confidential fraud reporting methods, such as, postal, phone, online and that the use and effectiveness of these are evaluated



73 Refer to the Government Counter Fraud Profession Counter Bribery and Corruption Standard. <https://www.gov.uk/government/publications/a-standard-for-the-counter-bribery-and-corruption-professional/a-standard-for-the-counter-bribery-and-corruption-professional-html>

74 Selflessness, Integrity, Objectivity, Accountability, Openness, Honesty and Leadership. For more information see The Seven Principles of Public Life HTML - <https://www.gov.uk/government/publications/the-7-principles-of-public-life/the-7-principles-of-public-life--2>

E9. Strategic Threat Assessment

A strategic threat assessment is a professional judgement based on analysis, as to the intent and capability of a particular threat actor or multiple threat actors, against particular target(s)⁷⁵.

Organisations should consider the use of strategic threat assessments to identify threats against the organisation, which will aid in anticipating potential risks, enabling early action to mitigate the threat.

Threat assessments can also identify weaknesses in a control environment that increases an organisation’s exposure or susceptibility to potential threats and increased risk.

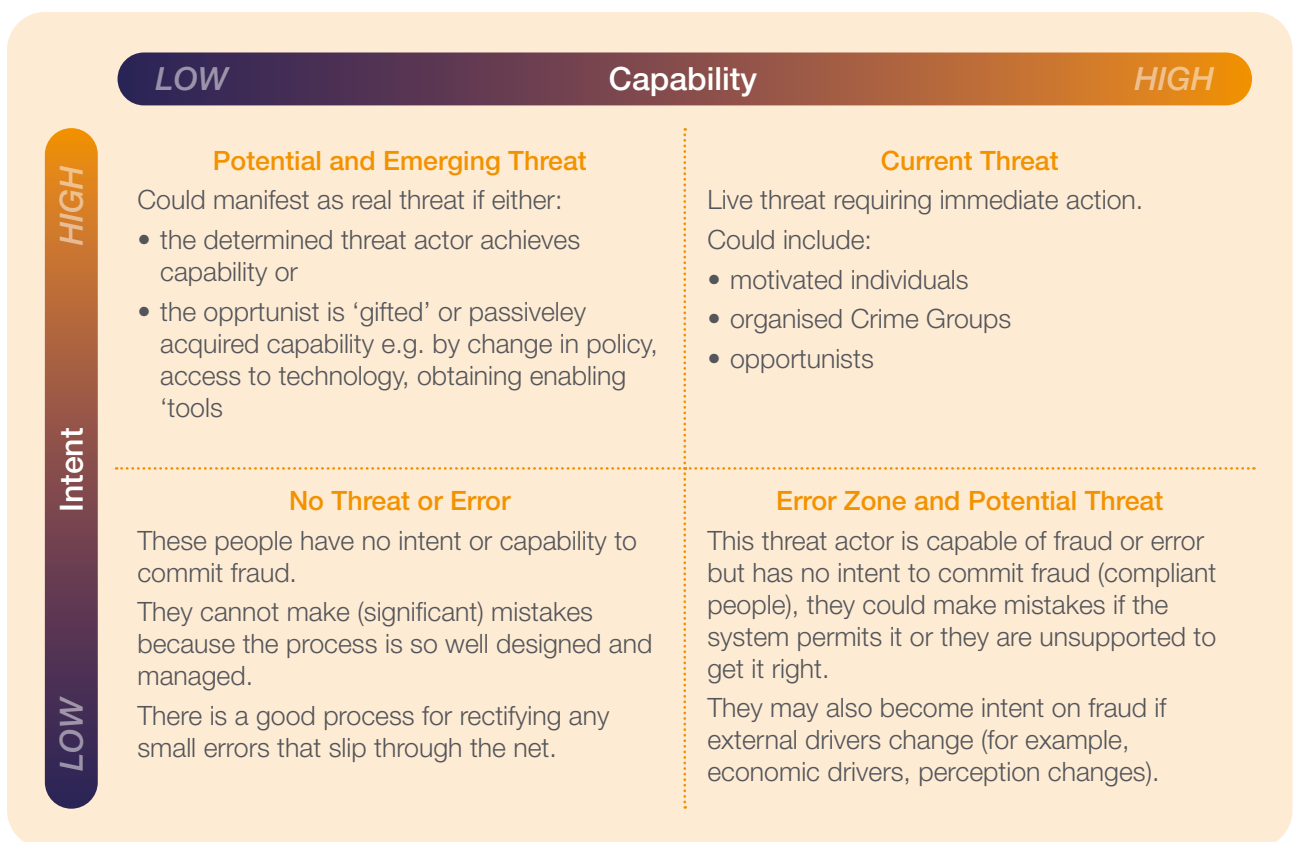


Figure 13. Assessing and managing threat actors.

E10. Prevention by Design

Fraud prevention should be considered at all times and not only in response to a fraud risk assessment or an initial fraud impact assessment. Individuals should actively collaborate with policy and design teams to provide expert advice and encourage fraud prevention being instilled into all stages of design with a view to target hardening⁷⁶.

Policies, processes, schemes and products should be reviewed throughout their life cycle ensuring that fraud prevention controls remain pertinent.

When looking to strengthen the counter fraud response, they should be aware of the motivations and capability of the fraudster. Some fraud may be driven by need (for example, debt, threats or addictions) heightening the motivation to commit fraud. Understanding where to focus prevention controls and how the controls can effectively remove or reduce the motivation, opportunities and capability to commit fraud will be key in preventing fraud in the organisation.

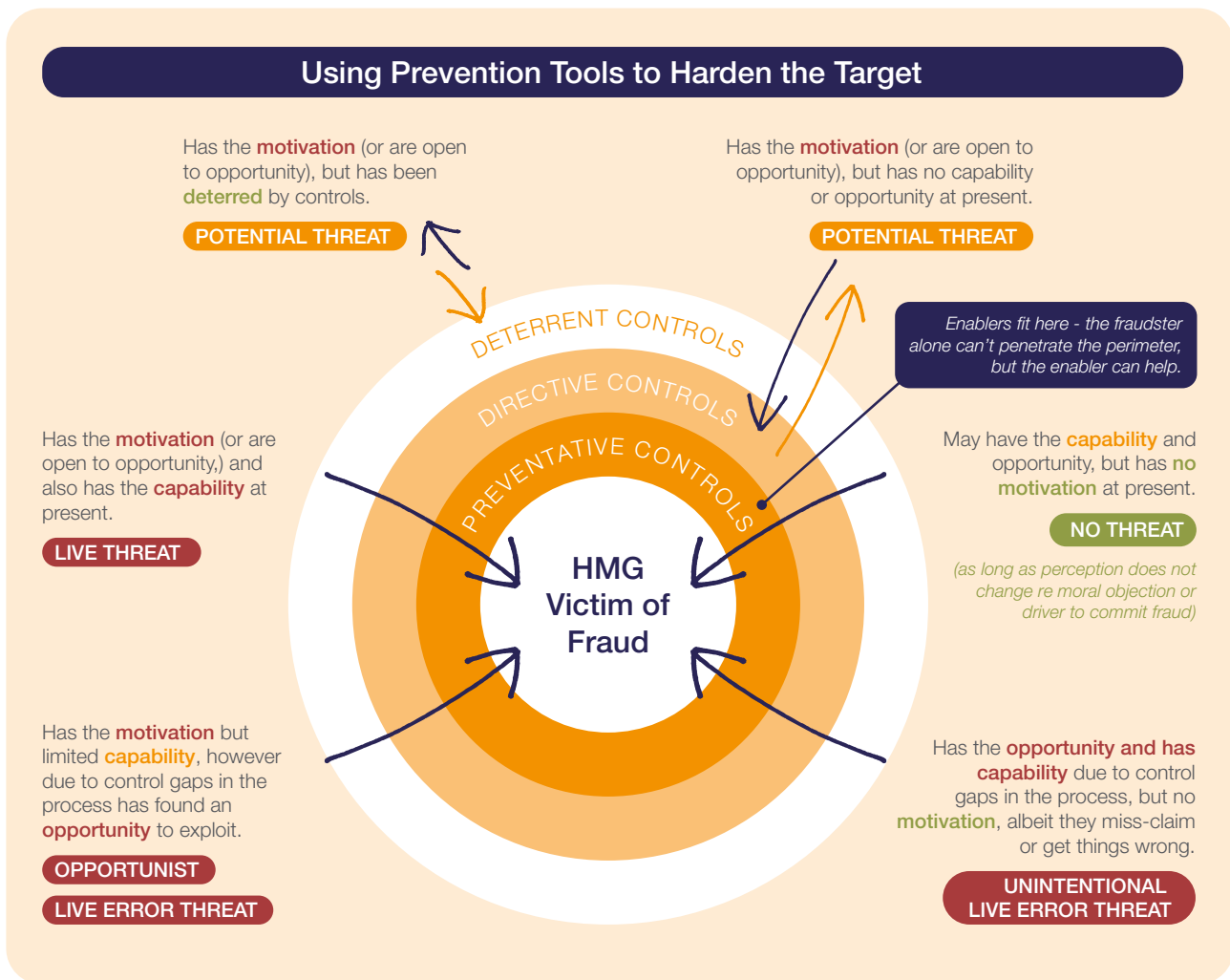


Figure 14. Using prevention controls to harden the target.

76 Target hardening aims to reduce opportunities for offending through a range of measures - British Society of Criminology.

Target hardening methods can be identified by:

- ensuring fraud expertise is involved in all policy consultation processes
- fraud experts are involved in product design at all stages
- reviewing existing controls with a view to understanding potential vulnerabilities at all stages

Counter fraud professionals should be involved at the earliest stage of all new schemes, processes and policy designs, to provide expert advice on:

- how counter fraud controls can be integrated into the design to manage fraud
- identified vulnerabilities
- strengthen processes to make them less vulnerable to fraud during the design stage

When designing services, advice provided could include, but is not limited to:

- how the process or policy could be targeted by fraudsters
- what enablers could be utilised by fraudsters
- how the process or policy could be used to protect the organisation
- potential wider consequences of tolerating any identified risks
- possible consequences and impact of changes
- any requirements for a full initial fraud impact assessment or fraud risk assessment

Careful consideration should be provided to ensure that services are not restricted in such a way as to make them difficult or unobtainable for the target demographic.

The counter fraud professional has a key role to raise awareness that target hardening is the responsibility of all employees within and all those associated with, the organisation. A comprehensive counter fraud awareness programme, tailored to individual job roles and the risks they face throughout their employment, can assist an organisation to strengthen their counter fraud response.

Further advice⁷⁷ on designing fraud out of online systems can be found at: Protecting your service against fraud - Service Manual - [GOV.UK](https://www.gov.uk/service-manual/technology/protecting-your-service-against-fraud)

E11. Lessons Learnt Reviews

Lessons learnt reviews⁷⁸ should be conducted as part of the evaluation process after:

- the completion of any counter fraud project or pilot scheme
- the implementation of a control(s)
- the completion of a system and procedure review whether instigated in response to a fraud or not
- the results produced by data analytics or an information review
- the implementation of a national, regional or local information campaign
- the implementation of a disruption measure(s)
- the structured debriefing of a fraud victim(s)
- the receipt of an investigation report

Lessons learnt reviews should be balanced and highlight what has gone well as well as those areas in need of improvement. They should also be supported by measurable action plans. Organisations are expected to act on the findings of all lessons learnt reviews and share these where this is in the public interest and such sharing is consistent with data protection legislation and regulations.

77 <https://www.gov.uk/service-manual/technology/protecting-your-service-against-fraud>

78 Products section D7 has further information on conducting lessons learnt reviews.

E12. Communications Strategy⁷⁹

The organisation should ensure that a communications strategy is in place that involves all the counter fraud functions and is available to all in the organisation and the third parties with whom they interact. These will include: members of the public applying for services or products, suppliers, contractors and agents. This will maximise the potential of getting the 'prevent message' out, with accurate data.

Consideration should be given to the information shared with the media, internal colleagues and third parties, to confirm that the 'right message' is being delivered and that any potential for reputational damage is minimised.

The communication strategy should consider:

- who is the communication aimed at and are they internal or external to the organisation?
- what is the purpose of your communication and what is the desired outcome?
- when is the best time to launch your communication?
- where should the message be delivered and should you use the internet or a webpage, email, text, posters, direct mail, the telephone or social media?
- why is the message being delivered now and what are the key actions needed?
- how will you communicate and will you use a variety of different formats and accessible options?
- how will you measure results and how do you know your communications have reached their intended audience?

Deterrence involves eliminating the factors that might lead to fraud. In particular, it is designed to stop the rationalisation of the act. Organisations actively need to create a strong deterrent effect through communicating:

- the commitment of the organisation to combat fraud
- the effectiveness of existing prevention and detection arrangements, including successful results
- the determination of the organisation to pursue sanctions and redress where fraud has occurred, publicising outcomes in the media where appropriate

Deterrence Messaging

It is important to target potential fraudsters with key messages. Publicity should be integrated into plans, initiatives and specific cases to have the maximum impact on the intended (or target) audience. The goal should be to change the fraudster's decision by altering the risk versus reward ratio; sometimes referred to as 'amplifying the risk'. Deterrent messaging will have varying levels of success against different groups of fraudsters. Organisations should vary their approach to deterrence messaging, for example, organised crime groups are unlikely to be deterred only by the prospect of having to repay their financial gain.

Behavioural Science

Organisations should consider behavioural science when developing communications to identify barriers and ensure that the deterrence messaging will be impactful.⁸⁰

⁷⁹ See Government Communication Service for more information. <https://gcs.civilservice.gov.uk/>

⁸⁰ For more information see <https://www.bi.team/>

E13. Data and Analytics

The organisation should clearly define what information⁸¹ and data⁸² they hold and how this can be used to prevent fraud. The insights that data analytics provides, means that the scope for using such techniques should be factored into the counter fraud strategy and fraud prevention plan.

Organisations should ensure that the right mixture of resources is in place to strengthen timely delivery of counter fraud data analytics activities to a high quality standard⁸³. The types of resources required will vary between organisations but broadly there are three types: analytical skill sets and expertise, technological infrastructure and capability, and data.

- **analytical skill sets and expertise** - organisations should ensure that individuals working in counter fraud data analytics undertake regular learning and development to keep their knowledge and skills up to date⁸⁴
- **technological infrastructure and capability** - organisations should ensure that their technological infrastructure and capability can handle the requirements of the organisation's need for counter fraud data analytics

Technological infrastructure and capability includes, but is not limited to:

- the technology needed to manage and undertake counter fraud data analytics activities. This may include, for example, data processing and the subsequent analysis of this data
- the technology needed to store, maintain and manage large amounts of data securely
- training to use technology appropriately and as required by legislation and organisational policy

Data organisations should ensure that, when processing personal data, the provisions of the Data Protection Act 2018 are complied with in full. They should also ensure that any data processing, storage and analytics for counter fraud purposes is consistent with their registration with the Information Commissioner's Office and has the consent of the nominated data owner and data controller.

Organisations should ensure that, when undertaking data analytics for counter fraud purposes, they fully comply with the six principles for law enforcement data processing, laid down by the General Data Protection Regulation (GDPR)⁸⁵.

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

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

83 Resources could be internal or external. Not every organisation will have an in-house capability, but should have access to an external resource for counter fraud data analytics.

84 See Government Functional Standard GovS 005 Digital (HTML) - <https://www.gov.uk/government/publications/government-functional-standard-govs-005-digital/government-functional-standard-govs-005-digital-html>

85 About the Guide to Law Enforcement Processing - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/?template=pdf&patch=6#3>

The law enforcement purposes are defined under section 31 of the Data Protection Act 2018 as:

‘The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’

These are such that data processing must be:

- lawful and fair
- be specified, explicit and legitimate
- adequate, relevant and not excessive
- accurately processed and kept up to date
- kept no longer than is necessary
- processed in a secure manner

The organisation should nominate an information assurance manager, who will be accountable for the acquisition, storage, processing, analysis, dissemination, use, disclosure and disposal, of all information and data collected and applied for counter fraud purposes. Organisations should also establish and maintain data sharing arrangements in support of fraud prevention. Organisations should make full use of the statutory information sharing powers available to them⁸⁶.



86 In the UK, this includes sections 68-72 of the Serious Crime Act 2007, section 56 and schedule 8 of the Digital Economy Act 2017 and schedule 2, paragraphs 2 and 5 of the Data Protection Act 2018 - <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

Glossary

Competency command word ⁸⁷	Definition
Know	Provide evidence of factual information or awareness gained through experience or education.
Understand or interpret	Provide the intended meaning or cause of something.
Describe	Give a report on how something is done or what something is like.
Explain	Make something easier to understand by giving information about it or giving a reason for an action.
Apply	Make use of a skill or knowledge.
Evaluate or assess	Judge or calculate the quality, importance, amount, or value of something.
Design	Make or draw plans for something.
Demonstrate	Show something and explain how it works.
Identify	Recognise a problem, need, fact, or other item and show that it exists.
Discuss	Consider and offer an interpretation or evaluation of something or give a judgement on the value of arguments for and against something.

87 From the GCFP Standard Development Principles.

Frequently used terms	Definition
Bribery	Offering, promising or giving a financial or other advantage to induce or reward improper performance or the request or receipt of such an advantage. It includes the corporate offence of failing to prevent bribery.
Corruption	Corruption is the abuse of entrusted power for private benefit that usually breaches laws, regulations, standards of integrity and/or standards of professional behaviour.
Error	Is a similar occurrence to fraud, but where the elements of dishonesty or intent (see definition of fraud) are missing or cannot be proved. However, error also results in losses to public funds and for the purposes of this standard, is considered alongside fraud.
Fraud	Defined in the Fraud Act 2006 ⁸⁸ . The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position.
Fraud deterrence	The act of discouraging fraud by being clear of consequences. Sending out the message that committing fraud has adverse consequences for fraudsters, victims and society.
Fraud prevention	To stop the likelihood and reduce the impact of fraud. To create an anti-fraud culture in which people and processes work together to minimise fraud risk.
Fraud risk assessment	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.
Horizon scanning	Exploring what the future might look like to understand uncertainties better. Horizon scanning helps organisations analyse whether it is adequately prepared for potential opportunities and threats. This helps ensure that policies are resilient to different future environments.
Inherent risk	Also defined as gross risk, is the risk to an organisation assuming there are no controls in place.
National Audit Office (NAO)	The UK's independent public spending watchdog. The NAO supports Parliament in holding the government to account and in helping improve public services through high-quality audits.

88 See Fraud Act 2006 - <https://www.legislation.gov.uk/ukpga/2006/35/contents>

Frequently used terms	Definition
Residual risk	Also defined as net risk, or fraud risk exposure, it is the risk remaining once the risk response has been successfully applied.
Risk	The possibility of an adverse event occurring or a beneficial opportunity being missed. If realised, it may have an effect on the achievement of objectives and can be measured in terms of likelihood and impact.
Risk appetite	The amount of risk the organisation is willing to accept at the enterprise level, which manifests itself in the type and number of activities and associated risks that the organisation is willing to undertake.
Risk tolerance	The threshold levels of risk exposure and target levels of incidences and losses that, with appropriate approvals, can be exceeded; but which, when exceeded, will trigger some form of response - for example, reporting the situation to senior management.
Threat	<p>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.</p> <p>* “can be described as” is used throughout this standard, where multiple definitions are available</p>



Public Sector
Fraud Authority

