Government
Counter Fraud
Profession

Operated by the Public Sector Fraud Authority

Government Counter Fraud Profession

Standard for Fraud Intelligence Practitioner

July 2024

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 2024

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

Version Control

Version 1	Issued February 2018
Version 2	Issued July 2024

Contents

Contents

"We know that fraudsters are a capable and committed adversary and the way they commit fraud is diverse and evolving. Enhancing fraud intelligence capabilities is essential. The more capable we are in sharing and using intelligence to its best effect, the better we can find and take action on fraud and those who attack our public services."

Mark Cheeseman OBE,
Chief Executive, Public Sector Fraud Authority

A. Professional Standard and Competencies for the Fraud Intelligence Practitioner

A1. Purpose

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

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

- To describe the knowledge, skills and experience (professional standards and competencies) needed for an individual to 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 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 **Fraud Intelligence Practitioner**. To be acknowledged as a Counter Fraud Professional, these standards will have to be met.

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.

The term fraud includes all fraud within economic crime i.e. bribery, corruption, for the purpose of this standard. This document focuses on an individuals' intelligence skills.

> The GCFP Standards and Guidance are designed to present a consistent cross government approach to countering fraud

A2. Introduction

A Fraud Intelligence Practitioner should be able to recognise the importance of intelligence in assessing the organisation threat and response to fraud. A Fraud Intelligence Practitioner must understand what intelligence is, what work can be done to develop intelligence, how this supports decision making and how it can assist in fraud investigations, both criminal and civil.

A3. How this Document is Structured

This document contains the following:

- The **Competency Framework** outlining the knowledge, skills and experience required by those undertaking work in fraud intelligence to operate effectively, and how these develop through the competency framework levels of Trainee, Foundation to Practitioner.
- **Guidance for Professionals includes:**
  - **Process guidance** describing the recommended processes for fraud intelligence.
  - **Product guidance** setting out the recommended guidance on developing good quality outputs in relation to fraud intelligence.
  - **Organisation guidance** agreed as best practice and should be followed by all counter fraud professionals and their organisations.

> A Fraud Intelligence Practitioner must understand what intelligence is and how it supports decision making

The standards have been created, reviewed and agreed by the Government Counter Fraud Profession (GCFP) Board, the body with oversight of the Profession, and the responsibility for the development and maintenance of the Counter Fraud Professional Standards and Guidance. The board is assisted by an expert Cross Sector Advisory Group[1] (CSAG).

A4. 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] 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.

A5. Government Functions (UK)

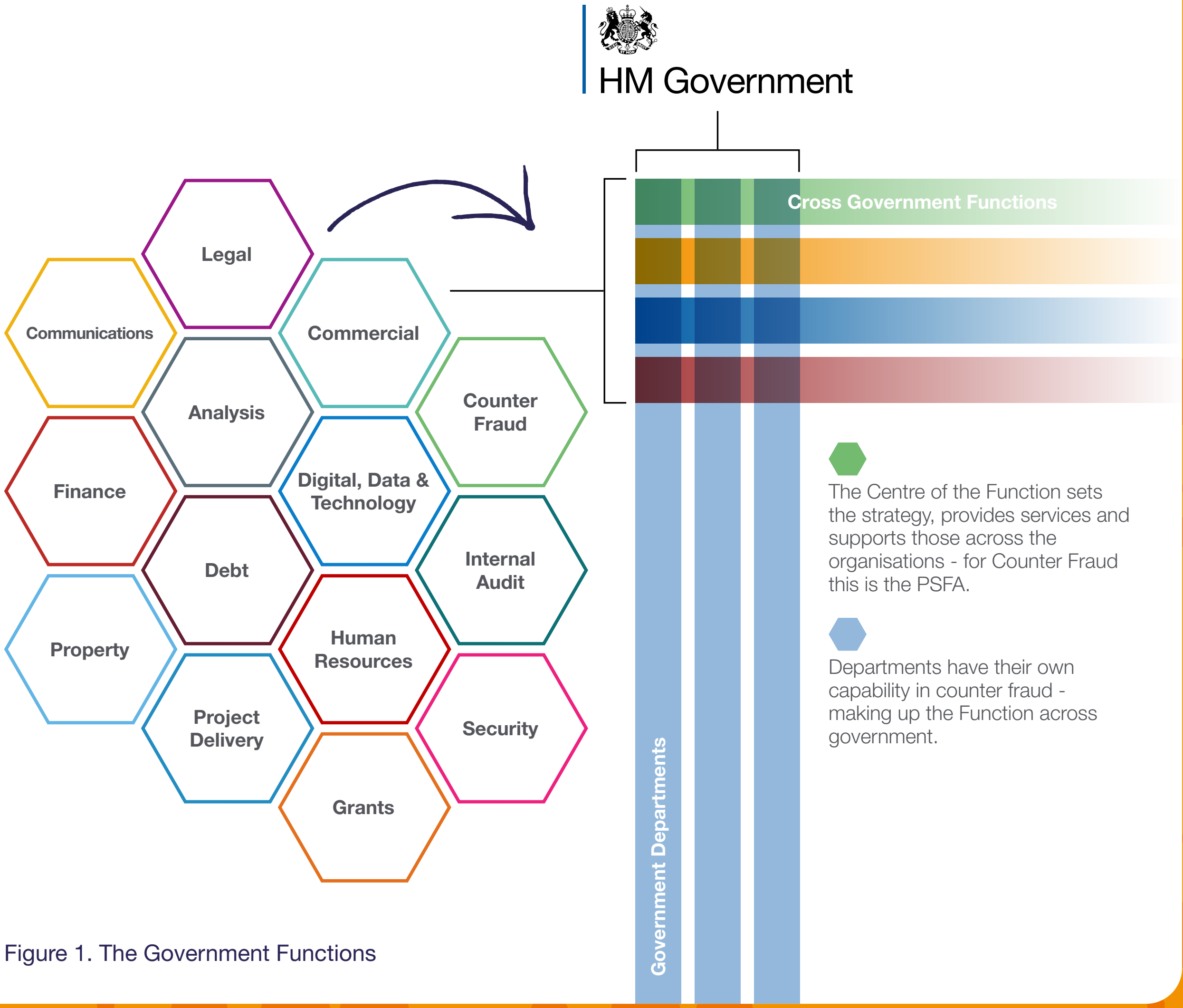
In the United Kingdom, the Central Government operates under a functional model.

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

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

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

The Government Functions



The Centre of the Function sets the strategy, provides services and supports those across the organisations - for Counter Fraud this is the PSFA.

Departments have their own capability in counter fraud - making up the Function across government.

Figure 1. The Government Functions

A6. Public Sector Fraud Authority

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

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

It brings:

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

The PSFA is changing the way that government manages fraud.

Its mission is to:

- ✓ 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). The PSC works with a number of public bodies, via an oversight board, to agree the strategy, focus and products of the Profession. The PSFA is also the home of the Centre of Learning for Counter Fraud, which is responsible for building a vibrant learning community, improving counter fraud capability and providing fraud leaders with industry-leading skills.

A7. Government Counter Fraud Profession

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

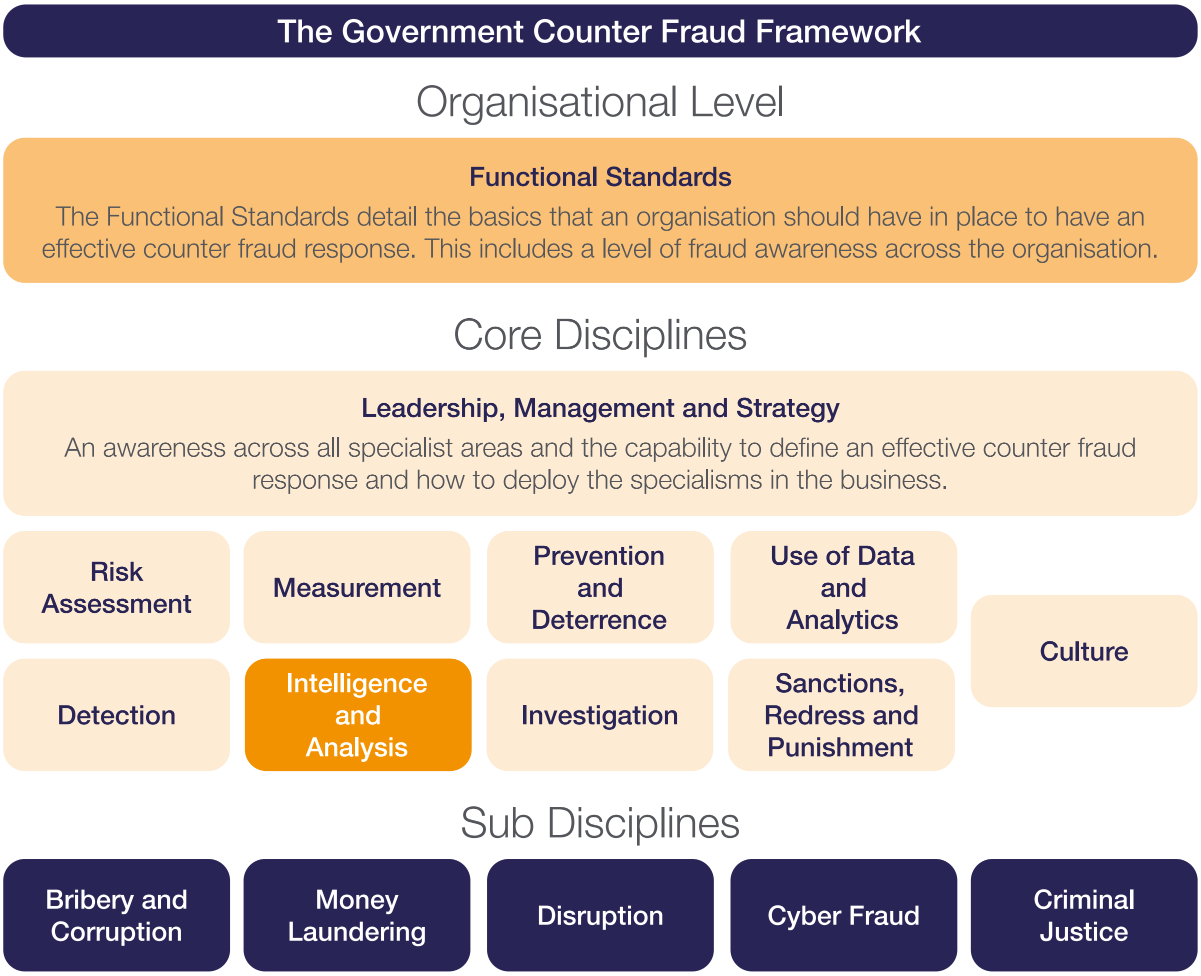
The GCFP board is supported by a Cross Sector Advisory Group (CSAG). This is made up of experts in counter fraud from a range of sectors, including academic, financial, legal and regulatory. The advisory group acts as a critical friend to the decisions made by the board.

> The GCFP Cross Government Board leads oversight of the Profession

A8. Government Counter Fraud Framework

The framework covers all of the core disciplines and sub-disciplines that a public sector organisation needs to deal 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 sub-disciplines are areas of additional knowledge, skills and experience that enhance capability across a number of core disciplines.



The Government Counter Fraud Framework

Organisational Level

Functional Standards

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

Core Disciplines

Leadership, Management and Strategy

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

Risk Assessment

Measurement

Prevention and Deterrence

Use of Data and Analytics

Culture

Detection

Intelligence and Analysis

Investigation

Sanctions, Redress and Punishment

Sub Disciplines

Bribery and Corruption

Money Laundering

Disruption

Cyber Fraud

Criminal Justice

Figure 2. The Government Counter Fraud Framework

Membership Categories

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

Investigation

Intelligence

Fraud Control

Data and Analytics

Leadership, Management and Strategy

Figure 3. The Government Counter Fraud Framework Membership Categories

The Fraud Control Cluster

The Fraud Control Cluster incorporates Fraud Risk Assessment, Fraud Loss Measurement, Fraud Prevention, Counter Fraud Culture and Fraud Detection 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.

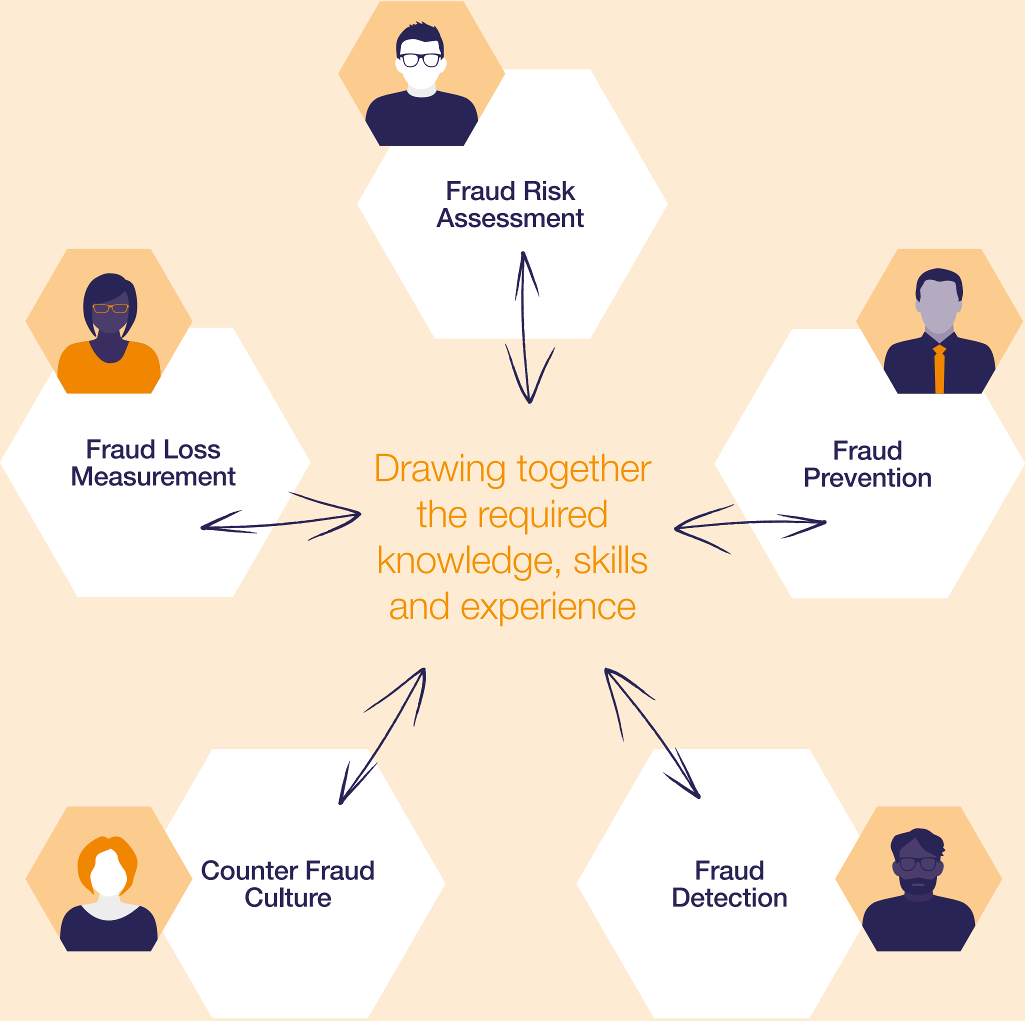


Figure 4. The Fraud Control Cluster

A9. Roles and Responsibilities

For the purposes of this standard a Practitioner will be undertaking work within fraud intelligence and will have the ability and opportunity to develop, manage and analyse intelligence.

A10. Key Components Explained

Components outline at a high level, the knowledge, skills and experience required for each core and sub-discipline. There are **13** key components for the **Intelligence Standard for Fraud Practitioner.** 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.

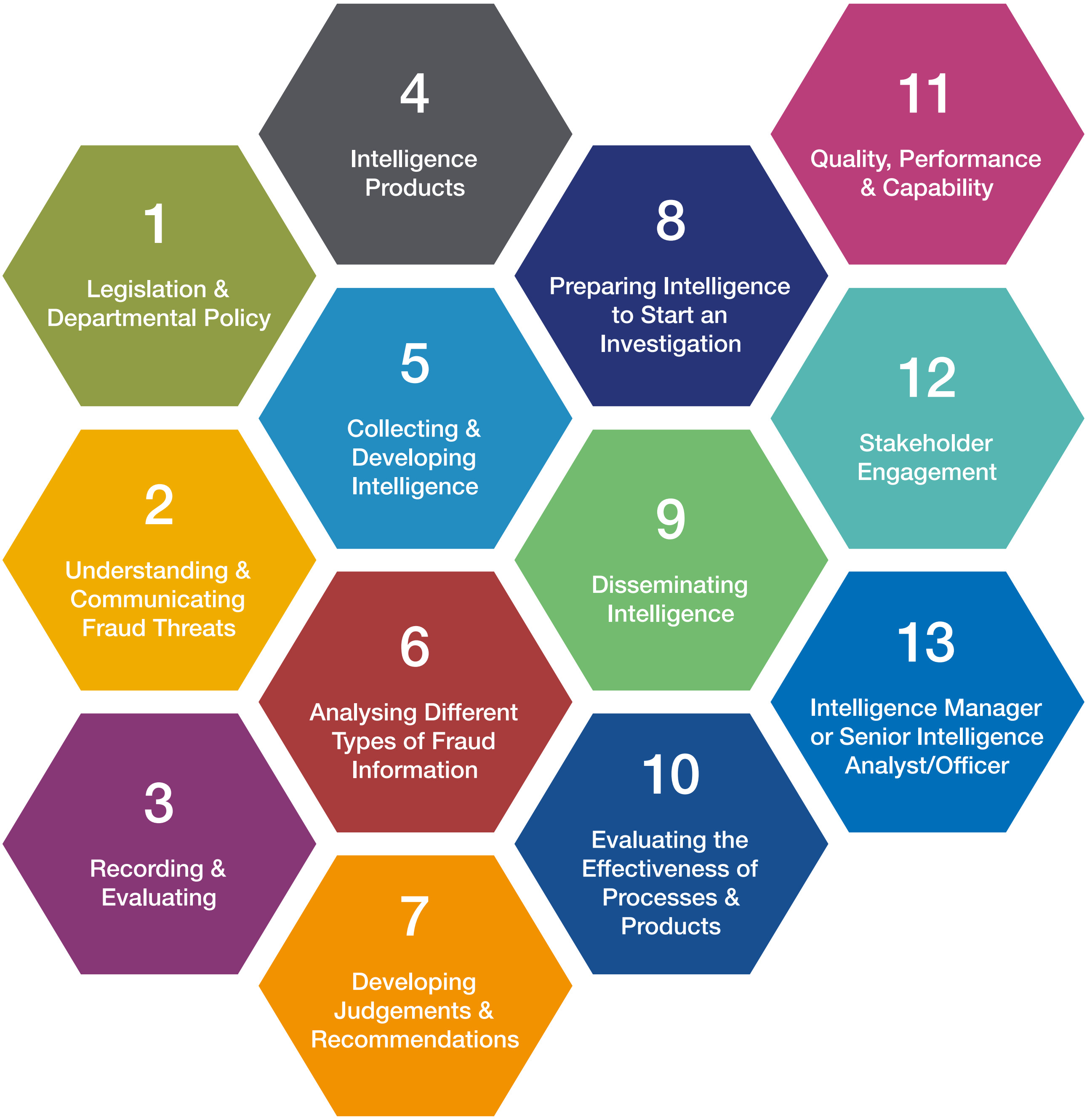

1
Legislation & Departmental Policy
2
Understanding & Communicating Fraud Threats
3
Recording & Evaluating
4
Intelligence Products
5
Collecting & Developing Intelligence
6
Analysing Different Types of Fraud Information
7
Developing Judgements & Recommendations
8
Preparing Intelligence to Start an Investigation
9
Disseminating Intelligence
10
Evaluating the Effectiveness of Processes & Products
11
Quality, Performance & Capability
12
Stakeholder Engagement
13
Intelligence Manager or Senior Intelligence Analyst/Officer

Figure 5. Fraud Prevention Standard Key Components

1 Legislation & Departmental Policy

Handling of intelligence in accordance with legislation and internal policies is essential.

2 Understanding & Communicating Fraud Threats

Using intelligence to understand the operational landscape and its fraud risks and effectively communicate fraud threats to stakeholders.

3 Recording & Evaluating

Evaluating and recording new information received securely and accurately to support a conclusion about further action.

4 Intelligence Products

Producing intelligence reports and analysis of products.

5 Collecting & Developing Intelligence

Awareness of a wide range of sources and ability to develop intelligence in a meaningful way.

6 Analysing Different Types of Fraud Information

Using various techniques to present and analyse information.

7 Developing Judgements & Recommendations

Developing a range of hypotheses, judgements and recommendations from intelligence analysis.

8 Preparing Intelligence to Start an Investigation

Evaluating a complex intelligence case and making a decision about whether it should be investigated.

9 Disseminating Intelligence

Understanding risks associated with sharing intelligence and presenting intelligence findings.

10 Evaluating the Effectiveness of Processes & Products

Continuous assessment of intelligence processes and products.

11 Quality, Performance & Capability

Identify own training and development opportunities to increase knowledge & capability and have a good understanding of performance and productivity management, and the skills to perform quality control.

12 Stakeholder Engagement

Building a network of counter fraud stakeholders both internally and externally to the organisation.

13 Intelligence Manager or Senior Intelligence Analyst/Officer

Oversight and management of team resources, adhering to organisational objectives, decision making on dissemination of intelligence, managing critical incidents, and stakeholder management.

Within the competency framework are competency levels. 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.

A11. Competency Levels

General rules about the competency levels are set out below:

- **Trainee (T)** – is about developing introductory knowledge.
- **Foundation (F)** – is about having the knowledge.
- **Practitioner (P)** – is about demonstrating the application of the knowledge.
- **Advanced Practitioner (AP)** – is about having a more expansive, specialist knowledge and being able to use this to evaluate and improve what is being done.

A12. Understanding Categories

Categories are defined combinations of elements, which show the knowledge, skills and experience expected for each core discipline. Categories are not people or grade specific and the title or description used by organisations may be different to those below. By considering the intelligence activity you undertake, you will be able to determine which **Category**, **A**, **B** or **C**, is relevant.

For Intelligence there are 3 core categories:

- **A** – **Researcher** accurately records information, complete initial enquiries and searches.
- **B** – **Analyst (Tactical/Strategic)** analyses information, feeding the results into wider fraud activity.
- **C** – **Intelligence Officer/Handler** gather intelligence, develop packages and identify emerging frauds and risks.

For each category there are a specific group of elements from the Competency Framework that should be demonstrated. Recognition will be available at Foundation level and as a Practitioner. Trainee level will not be formally recognised, but the elements in this level set out how you can begin your journey to develop knowledge and skills in intelligence. So, for example, you will be classified as a Category A Intelligence Foundation. This structure allows progression within categories, across to other categories and then wider to demonstrate skill in other core or sub-disciplines.

We recognise that intelligence activity may be undertaken in a tactical or strategic context and have incorporated this into the structure. The elements are designed to be applicable to both contexts, to allow flexibility of use. We have identified that some elements are not applicable for strategic roles and this is clear in the Category Matrix for tactical analysts. The Category Matrix tools have been developed to offer a guide on which elements relate to which category. For example, you may be a Category B Tactical Intelligence Foundation.

We have incorporated hybrid roles into the structure as we recognise that in some organisations investigation roles may require a level of technical competence in intelligence to support their combined role. This is often where there is no separate intelligence function in-house.

To be recognised as a Practitioner Hybrid, investigators must demonstrate Practitioner level investigation competency in the category they operate in (A, B or C) before accessing the elements in intelligence identified in the Hybrid Category Matrix for their category A, B or C in Intelligence.

For Intelligence there are two Categories for Managers:

- **Intelligence Manager (IM)** – Strategic oversight of operations, resource and intelligence activity.
- **Senior Intelligence Officer/Analyst (SIO/SIA)** – As above for IM, but with the addition of being actively involved in intelligence, and developing intelligence packages alongside managerial duties.

The prerequisite knowledge to access the Manager Categories is as follows:

- **Intelligence Manager (IM)** – must demonstrate Foundation level in the category of Intelligence standards they manage staff in, then the Manager elements.
- **Senior Intelligence Officer/Analyst (SIO/SIA)** – must demonstrate Practitioner level in the category of Intelligence standards they manage staff in, then the Manager elements.

There is also a Category for **Hybrid Managers**, with a prerequisite model following the similar approach above, but the skills required must be demonstrated in both Investigation and Intelligence to achieve Hybrid Manager or Hybrid SIO/A status.

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 of particular interest or focus in, to demonstrate their knowledge, skills and experience. How we will recognise the Advanced Practitioner level will be determined at a later stage, but for now members may use those elements in the framework for self-assessment of their knowledge, skills and experience to help map their development.

Categories will enable a common assessment of skills and draw a distinction of those with a level of skill and those without.

> “Categories will enable a common assessment of skills and draw a distinction of those with a level of skill and those without

B. Fraud Intelligence Professional – Competency Framework

1. Legislation and Departmental Policy

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
1.1 Legislation and Departmental Policy[2]	Identify main areas of legislation and policies that affect intelligence work.	Explain key legislation & policies that affect intelligence work.	Demonstrate application of relevant legislation and policy that affect intelligence work.	Analyse the application of relevant legislation and policy that affect intelligence work.

[2] Guidance can be found in Section C1.

2. Understanding & Communicating Fraud Threats

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
2.1 Understanding and Communicating Fraud Threats – Types of Fraud	Identify different types of fraud that could affect their organisation and others.	Explain how different types of fraud could affect their organisation and others and the role of intelligence in stopping this.	Demonstrate a wide knowledge of fraud types that could affect their organisation and others.	Evaluate how a wide range of fraud types could affect their organisation and others. Interpret strategic risk and threat assessments considering the impact of current or new legislation and policies.
2.2 Understanding and Communicating Fraud Threats – Fraud Risk	Identify specific fraud risks arising from intelligence referrals.	Explain emerging areas of fraud risk within their organisation and for key partners.	Demonstrate application of strategic intelligence to inform the organisations risk, detection and prevention functions.	Evaluate the application of strategic intelligence to inform the organisations risk detection and prevention functions.
2.3 Understanding and Communicating Fraud Threats – Research & Network	Identify who needs to be made aware of specific intelligence referrals inside and outside of the organisation, and identify relevant secure gateways.	Explain who needs to be made aware of specific intelligence referrals inside and outside of the organisation and able to identify relevant secure gateways.	Demonstrate establishment of a network of contacts inside & with other organisations to alert to potential frauds and emerging areas of fraud risk using a relevant secure gateway.	Evaluate how to work with other organisations to produce joint fraud risk and threat assessments for their sector or sub-sector.
2.4 Understanding and Communicating Fraud Threats – Technology	Identify technology available to address key and emerging threats.	Explain how to deploy technology to address key and emerging threats.	Demonstrate the use of technology to address key and emerging threats.	Evaluate how to access or deploy technology to address key and emerging threats.

3. Recording & Evaluating

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
3.1 Recording & Evaluating – Intelligence Cycle	Identify the key elements of the Intelligence Cycle and National Intelligence Model (NIM).	Explain the key elements of the Intelligence Cycle and National Intelligence Model (NIM).	Demonstrate application of the key elements of the Intelligence Cycle and National Intelligence Model (NIM).	Evaluate the application of the key elements of the Intelligence Cycle and National Intelligence Model (NIM).
3.2 Recording & Evaluating – Recording	Identify how to record intelligence securely, accurately and in a manner that enables analysis across multiple intelligence items.	Explain how to record intelligence securely, accurately and in a manner that enables analysis across multiple intelligence items.	Demonstrate how to record intelligence securely, accurately and in a manner that enables analysis across multiple intelligence items.	Analyse the recording of intelligence across multiple intelligence items using knowledge of statistics and other analytic tools and routines.
3.3 Recording & Evaluating – Source Evaluation	Identify how intelligence referrals are assessed using handling codes.	Explain how to assess the reliability of information and its source using relevant handling codes.	Demonstrate using evaluation and handling codes how to assess the reliability of information and its source.	Evaluate the use of source evaluation and handling codes to ensure consistency.
3.4 Recording & Evaluating – Source Protection	Identify the criteria where a source may be under threat, the need for risk assessment and how to escalate.	Explain the need for risk assessment and where a source may be under threat and how to escalate.	Demonstrate the use of risk assessment and identification of where a source may be under threat and escalate.	Evaluate the identification of criteria where a source may be under threat, the application of risk assessment and the use of escalation strategies.
3.5 Recording & Evaluating – Bulk Data Volumes	Recognise the need to manage bulk volumes of new information and make decisions about what to evaluate and input as intelligence.	Explain how to manage bulk volumes of new information and make decisions about what to evaluate and input as intelligence.	Demonstrate ability to manage bulk volumes of new information and make decisions about what to evaluate and input as intelligence.	Evaluate the management of bulk volumes of new information and make decisions about what to evaluate and input as intelligence.
3.6 Recording & Evaluating – Collating Data Sources for Launching Investigations	Recognise the need to review and develop intelligence held through cross checking and collating a number of different sources, resulting in the provision of an accurate and reliable base from which to launch investigations.	Explain how to review and develop intelligence held through cross checking and collating a number of different sources, resulting in the provision of an accurate and reliable base from which to launch complex and sensitive investigations.	Demonstrate the ability to review and develop intelligence held through cross checking and collating a number of different sources, resulting in the provision of an accurate and reliable base from which to launch complex and sensitive investigations.	Evaluate the review and development of intelligence held through the assessment of the cross checking and collation of a number of different sources, resulting in the provision of an accurate and reliable base from which to launch complex and sensitive investigations.

4. Intelligence Products

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
4.1 Intelligence Products – Summarise and Report	Identify how to produce intelligence summaries of specific fraud cases and threats.	Explain how to produce intelligence summaries of specific fraud cases and threats.	Demonstrate production of intelligence summaries of specific fraud cases and threats.	Evaluate the production of intelligence summaries of specific fraud cases and threats and the ability to produce reports on complex matters including emerging or sensitive threats quickly, based on relevant reliable information.
4.2 Intelligence Products – Intel Packages	Identify the elements to be included in intelligence packages.	Explain how to develop intelligence packages.	Demonstrate the ability to develop intelligence packages.	Evaluate the development and quality of intelligence packages.
4.3 Intelligence Products – Typology	Identify the difference between tactical (operational) and strategic intelligence.	Explain the difference between tactical (operational) and strategic intelligence.	Demonstrate the ability to differentiate between tactical (operational) and strategic intelligence.	Evaluate the assessment of tactical (operational) and strategic intelligence to produce strategic risk and threat assessments & translate these into programmes of work for other teams and parts of the counter fraud team.
4.4 Intelligence Products – Terms of Reference	Recognise the need to produce a terms of reference for use with stakeholders.	Explain how to produce terms of reference and the process of outlining strengths and limitations with stakeholders.	Demonstrate the production of terms of reference and the ability to discuss the strengths and limitations of this with stakeholders.	Evaluate the review and development of intelligence held through the assessment of the cross checking and collation of a number of different sources, resulting in the provision of an accurate and reliable base from which to launch complex and sensitive investigations.

5. Collecting & Developing Intelligence

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
5.1 Collecting & Developing Intelligence – Developing	Recognise the need to develop intelligence using a range of qualitative and quantitative information to answer a set of intelligence questions.	Explain how to develop intelligence using a range of qualitative and quantitative information to answer a set of intelligence questions.	Demonstrate the ability to develop intelligence using a range of qualitative and quantitative information to answer a set of intelligence questions, and demonstrate awareness of new threats and trends.	Evaluate the development of intelligence aligned to new threats and trends and adapt intelligence operations to deal with these.
5.2 Collecting & Developing Intelligence – Classify and Protect	Identify the Government Security Classifications and which types of intelligence require special handling.	Explain the Government Security Classifications and which types of intelligence require special handling.	Demonstrate how to protect information in accordance with the Government Security Classifications.	Evaluate the protection of information in accordance with government security classifications.
5.3 Collecting & Developing Intelligence – Specialists	Identify when and how to utilise specialist intelligence collection teams to develop intelligence.	Explain the tasking of specialist intelligence collection team to develop an intelligence objective.	Demonstrate tasking specialist intelligence collection teams to develop an intelligence objective.	Evaluate the tasking of specialist intelligence collection teams to develop an intelligence objective.
5.4 Collecting & Developing Intelligence – Planning	Identify the key elements of a collection plan for gathering fraud intelligence.	Explain how to create a collection plan for gathering fraud intelligence.	Demonstrate the ability to create a collection plan for gathering fraud intelligence.	Evaluate collection plans used for gathering fraud intelligence.
5.5 Collecting & Developing Intelligence – Gap analysis	Recognise there is a process for identifying intelligence gaps and the need to address them.	Explain how to identify intelligence gaps and action taken to address them.	Demonstrate the identification of intelligence gaps and action taken to address them.	Evaluate the identification of intelligence gaps and action taken to address them.
5.6 Collecting & Developing Intelligence – Sources	Identify the different sources available to gather information about fraud and suspected fraudsters.	Explain the different sources available to gather information about fraud and suspected fraudsters.	Demonstrate the use of an extensive range of fraud intelligence sources and understand the strengths and weaknesses of each.	Evaluate and identify new sources of information on emerging, sensitive and complex threats and be aware of the risks of doing so.

5. Collecting & Developing Intelligence

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
5.7 Collecting & Developing Intelligence – Intelligence Collection Contingency	Identify when current intelligence arrangements may not be able to cope with emerging, sensitive or complex threats and recognise action is required to proceed.	Explain how to recognise when current intelligence arrangements are not able to cope with emerging, sensitive or complex threats and what action is required to proceed.	Demonstrate the recognition of when current intelligence arrangements are not able to cope with emerging, sensitive or complex threats and be able to produce robust and persuasive arguments as to how to proceed.	Evaluate the recognition of when current intelligence arrangements are not able to cope with emerging, sensitive or complex threats and be able to produce robust and persuasive arguments as to how to proceed.
5.8 Collecting & Developing Intelligence – Collection Means and Authority	Recognise the difference between covert and overt intelligence, and the legislation that governs these methods.	Explain the difference between covert and overt intelligence, and the legislation that governs these methods.	Demonstrate the ability to manage covert and overt intelligence; apply the legislation that governs these methods.	Evaluate the management of covert and overt intelligence; apply the legislation that governs these methods.
5.9 Collecting & Developing Intelligence – CHIS	Identify the key criteria that identify a person as a covert human intelligence source (CHIS).	Explain when a person becomes a covert human intelligence source (CHIS) and when to report the situation.	Demonstrate the maintenance and the security of covert sources of fraud intelligence.	Evaluate the use of covert information gathering and advise others on the consideration and development of applications under relevant legislation.
5.10 Collecting & Developing Intelligence – Pseudonyms	Identify that legislation governs the use of a pseudonym covertly.	Explain how to use a pseudonym to acquire information covertly, in line with legislation and, when necessary, seek advice from the appropriate officer when considering this action.	Demonstrate the ability to identify which information requires authorisation to use/ collect, and the ability to apply for this authorisation in accordance with legal requirements.	Evaluate the identification of information requiring authorisation to use/ collect, and support others to apply for authorisation in accordance with legal requirements.
5.11 Collecting & Developing Intelligence – Covert Evidence Applications	Recognise applications for use of covert intelligence gathering is governed by RIPA/ IPA regulations.	Explain how applications for the use of covert intelligence gathering are governed by RIPA / IPA regulations.	Can effectively develop applications to use covert intelligence gathering, such as those governed by RIPA / IPA corporate regulations either using their own organisations powers or by informing applications with other enforcement bodies.	Evaluate the consideration of applications to use covert intelligence gathering, such as those governed by RIPA / IPA corporate regulations either using their own organisations powers or by informing applications with other enforcement bodies.

6. Analysing Different Types of Fraud Information

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
6.1 Analysing Different Types of Fraud Information – Characteristics	Identify indicators of fraud and analysis techniques.	Explain the indicators of fraud and analysis techniques used to establish details about a fraud or fraudster.	Demonstrate the application of fraud indicators and analysis techniques to establish details about a fraud or fraudster.	Evaluate the application of fraud indicators and analysis techniques to establish details about a fraud or fraudster.
6.2 Analysing Different Types of Fraud Information – Presentation, Visualisation and Analysis	Identify a range of techniques to present, visualise and analyse information.	Explain the application of a wide range of advanced techniques to present, visualise and analyse information.	Demonstrate the application of a wide range of advanced techniques to present, visualise and analyse information.	Evaluate the application (and any limitations) of a wide range of advanced techniques to present, visualise and analyse information.
6.3 Analysing Different Types of Fraud Information – Inconsistency Identification	Identify the potential for inconsistencies when analysing different types of fraud information.	Explain the potential for inconsistencies with similar intelligence analysis products from inside and outside their organisation, and the importance of objectivity.	Demonstrate the ability to address any inconsistencies with similar intelligence analysis products from inside and outside their organisation. Resist the temptation to agree with the existing analysis if their assessment is different.	Evaluate the ability to address any inconsistencies with similar intelligence analysis products from inside and outside their organisation. Resist the temptation to agree with the existing analysis if their assessment is different.
6.4 Analysing Different Types of Fraud Information – Intelligence Relationship	Recognise there is a process to identify relationships between pieces of information, including trends, anomalies, gaps and changes.	Explain the process to identify relationships between pieces of information, including trends, anomalies, gaps and changes.	Demonstrate the application of a process to identify relationships between pieces of information, including trends, anomalies, gaps and changes.	Evaluate the application of a process to identify relationships between pieces of information, including trends, anomalies, gaps and changes.
6.5 Analysing Different Types of Fraud Information – Evidence, Assumptions, Interpretations and Judgements.	Identify there is a need to distinguish between evidence, assumptions, interpretations and judgements.	Explain how to distinguish between evidence and analysts' assumptions, interpretations and judgements, explicitly stating the latter when used.	Demonstrate the ability to distinguish between evidence and analysts' assumptions, interpretations and judgements, explicitly stating the latter when used.	Evaluate the analysis of evidence, assumptions interpretations and judgements for different types of fraud information.

6. Analysing Different Types of Fraud Information

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
6.6 Analysing Different Types of Fraud Information – Inference Development	Identify the need to draw inferences from intelligence in order to make logical and relevant recommendations.	Explain how to draw inferences from intelligence in order to make logical and relevant recommendations.	Demonstrate the ability to draw inferences from intelligence in order to make logical and relevant recommendations.	Evaluate the development of inferences from intelligence in order to make logical and relevant recommendations.
6.7 Analysing Different Types of Fraud Information – Influence / Bias	Recognise the existence of cognitive bias.	Explain the impact of cognitive bias and the consideration of alternative perspectives.	Demonstrates steps taken to combat the possibility of cognitive bias that may disproportionately influence the analysis.	Evaluate the steps taken to combat the possibility of cognitive bias that may disproportionately influence the analysis.

7. Developing Judgements & Recommendations

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
7.1 Developing Judgements & Recommendations – Hypotheses	Recognise the result of intelligence analysis should be the formation of judgements, hypotheses and recommendations.	Explain how the result of intelligence analysis should be the formation of judgements, hypotheses and recommendations.	Demonstrate the ability to develop and test hypotheses, using judgement in response to intelligence problems, resulting in recommendations.	Evaluate the formation of judgements, hypothesis and recommendations for a range of specific referrals.
7.2 Developing Judgements & Recommendations – Confidence levels	Identify there is a process to evaluate the level of confidence that can be placed in the intelligence analysis and judgements.	Explain how to evaluate the level of confidence that can be placed in the intelligence analysis and judgements.	Demonstrate the ability to recommend the level of confidence that can be placed in the intelligence analysis and judgements.	Evaluate the recommendation of confidence levels placed in the intelligence analysis and judgements.
7.3 Developing Judgements & Recommendations – Opportunity / Risk	Identify the possible opportunities and risk associated with specific recommendations.	Explain how to analyse the possible opportunities and risks associated with specific recommendations.	Demonstrate the ability to analyse possible opportunities and risks associated with specific recommendations.	Evaluate the assessment of possible opportunities and risks associated with a variety of different recommendations.
7.4 Developing Judgements & Recommendations – Connections and Response	Recognise the need to make connections within intelligence involving engagement with internal and external stakeholders.	Explain how to make connections within intelligence involving engagement with internal and external stakeholders.	Demonstrate the identification of connections within intelligence and recognise the need for a strategic rather than tactical response to key threats, working with internal and external stakeholders.	Evaluate the identification of connections within intelligence and the recognition of the need for a strategic rather than tactical response to key threats, working with internal and external stakeholders.
7.5 Developing Judgements & Recommendations – Future Impact	Identify the need to assess the likely consequences, potential impact and future development of findings.	Explain how to assess the likely consequences, potential impact and future developments of findings.	Demonstrate the assessment of the likely consequences, potential impact and future developments of findings, resulting in the production of judgements proportionate to the business drivers and risks faced.	Evaluate the assessment of the likely consequences, potential impact and future developments of findings, resulting in the production of judgements proportionate to the business drivers and risks faced.
7.6 Developing Judgements & Recommendations – Influence	Identify the need to inform and influence senior managers of the need for change and investment.	Explain the need to inform and influence senior managers of the need for change and investment.	Demonstrate informing and influencing senior managers of the need for change and investment.	Evaluate the need to inform and influence senior managers of the need for action, change and investment.

8. Preparing Intelligence to Start an Investigation

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
8.1 Preparing Intelligence to Start an Investigation – Evaluation	Recognise the key purpose of intelligence development is to establish whether there is enough intelligence to start an investigation.	Explain the process of assessing whether there is sufficient and accurate intelligence to start an investigation.	Demonstrate the assessment of intelligence to establish whether it should be investigated and present it in a simple manner through the agreed process.	Evaluate the assessment of intelligence to establish whether it should be investigated and present it in a simple manner through the agreed process.
8.2 Preparing Intelligence to Start an Investigation – Process and Products	Identify the relevant investigative procedures and processes and ensure that intelligence products meet the needs of investigation teams, and offer relevant advice as to where and how to locate additional material, from both overt and covert sources where appropriate.	Explain the relevant investigative procedures and processes and ensure that intelligence products meet the needs of investigation teams, and offer relevant advice as to where and how to locate additional material, from both overt and covert sources where appropriate.	Apply relevant investigative procedures and processes and ensure that intelligence products meet the needs of investigation teams, and offer relevant advice as to where and how to locate additional material, from both overt and covert sources where appropriate.	Evaluate relevant investigative procedures and processes and ensure that intelligence products meet the needs of investigation teams, and offer relevant advice as to where and how to locate additional material, from both overt and covert sources where appropriate.
8.3 Preparing Intelligence to Start an Investigation – Limitations	Identify how to determine the limitations of the intelligence picture.	Explain the limitations of the intelligence picture and where further intelligence work could support investigation.	Demonstrate the identification of limitations of the intelligence picture and where the production of further intelligence work could support investigation.	Evaluate the identification of limitations of the intelligence picture, and analyse the recommendations for further intelligence work to support investigation.
8.4 Preparing Intelligence to Start an Investigation – Initial Enquiries and Test	Identify the need to conduct initial enquiries to test whether allegations made or suspicions held should be referred for investigation.	Explain how to conduct initial enquiries to test whether allegations made or suspicions held should be referred for investigation.	Demonstrate the development of intelligence to the next stage through the conduct of initial enquires to test whether allegations made, or suspicions held, should be referred for investigation.	Evaluate the development of intelligence to the next stage through the conduct of initial enquiries to test whether allegations made, or suspicions held, should be referred for investigation.

9. Disseminating Intelligence				
	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
9.1 Disseminating Intelligence – Process	Identify the difference between intelligence and evidence, in accordance with relevant legislation.	Explain the difference between intelligence and evidence in accordance with relevant legislation.	Demonstrate the difference between intelligence and evidence (in accordance with relevant legislation) through the presentation of findings in a structured way to others, including seniors.	Evaluate and quality assure the outcome of intelligence findings and briefings, and ensure alignment to relevant legislation.
9.2 Disseminating Intelligence – Protecting Source	Identify the need to sanitise intelligence and protect the source during dissemination, aligned to legal requirements and aligned to NIM.	Explain how to sanitise intelligence and protect the source during dissemination, aligned to legal requirements including to those outside the organisation and aligned to NIM.	Demonstrate sanitising and protecting the source during dissemination, aligned to legal requirements including to those outside the organisation and aligned to NIM.	Evaluate the handling and disseminating of intelligence with reference to legal requirements. Develop procedures for agreeing proportionate arrangements for the protection of sources and data, aligned to NIM.
9.3 Disseminating intelligence – Gateways	Identify the legal gateways for sharing information and that dissemination may be restricted in some scenarios.	Explain how to apply legal gateways for sharing information and when dissemination may be restricted in some scenarios.	Demonstrate disseminating intelligence via legal gateways to those outside the organisation, including deciding when further dissemination should be restricted.	Evaluate the dissemination of intelligence via legal gateways to those outside the organisation, and analyse the decision to restrict further dissemination.
9.4 Disseminating Intelligence – External to the Organisation	Identify legislation that governs the dissemination of intelligence to others inside and outside the organisation.	Explain how to disseminate intelligence to others who need to be informed, applying relevant legislation.	Demonstrate how to disseminate and risk assess the sharing of intelligence with partners, applying relevant legislation.	Evaluate the risk assessment of sharing intelligence with partners, using the relevant legislation.
9.5 Disseminating Intelligence – Pre-investigation Briefings	Recognise the need to conduct pre-investigation briefings to investigators using an appropriate briefing model.	Explain how to conduct pre-investigation briefings to investigators using an appropriate briefing model.	Lead pre-investigation briefings to investigators using an appropriate briefing model.	Evaluate pre-investigation briefings delivered to investigators using an appropriate briefing model.
9.6 Disseminating Intelligence – Restrictions	Recognise there are restrictions to dissemination attached to intelligence received from another organisation.	Explain the identification of restrictions to dissemination attached to intelligence received from another organisation.	Demonstrate the identification of restrictions to dissemination attached to intelligence received from another organisation.	Evaluate the identification of restrictions to dissemination attached to intelligence received from another organisation.

10. Evaluating the Effectiveness of Processes & Products

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
10.1 Evaluating the Effectiveness of Processes & Products – Evaluate	Identify the need to assess the effectiveness of intelligence processes and products to meet the HMG standard and achieve their purpose.	Explain the assessment of the effectiveness of intelligence processes and products to meet the HMG standard and achieve their purpose.	Demonstrate the assessment of the effectiveness of intelligence processes and products to meet the HMG standard and achieve their purpose.	Evaluate the assessment of the effectiveness of intelligence processes and products to meet the HMG standard and achieve their purpose.
10.2 Evaluating the Effectiveness of Processes & Products – Change and Improve	Identify the need to change and improve intelligence processes.	Explain best practice within their sector and the need to change and improve intelligence processes.	Demonstrate developing and implementing improvements to the intelligence processes.	Evaluate the development and implementation of change to intelligence operations. Develop and present business cases where change is needed.
10.3 Evaluating the Effectiveness of Processes & Products – Data Analytics	Identify the role of analytics in developing the intelligence picture.	Explain the use of data analytics to increase the effectiveness of the intelligence picture.	Demonstrate the use of data analytics to increase the effectiveness of the intelligence picture.	Evaluate, design and initiate change to intelligence products and processes using a range of data analytics available.

11. Quality, Performance & Capability

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
11.1 Quality, Performance & Capability – Learning & Development		Recognise their level of training and experience and can list their training and development needs.	Review their level of training and experience. Able to identify and plan training and development opportunities for themselves.	Review and evaluate changes in practice, policy and law concerning fraud intelligence. Contribute to the development of intelligence training for self and others.
11.2 Quality, Performance & Capability – Performance Management		Explain the performance measures in place and expectations of them in their role.	Review performance management data and proactively report their success against set criteria.	Evaluate performance management data to identify and develop high and poor performers in the context of intelligence assignments.
11.3 Quality, Performance & Capability – Productivity		Explain the measures in place to monitor productivity and their expected contribution.	Review their productivity and outcomes in intelligence assignments and report upwards.	Evaluate the productivity of intelligence assignments, utilising a range of outcome-based metrics.
11.4 Quality, Performance & Capability – Quality assurance		Explain the quality controls in place.	Apply the quality controls to intelligence assignments.	Evaluate the quality controls for a complex range of intelligence assignments including recommendations / lessons learnt. Interpret the results to suggest process improvements.

12. Stakeholder Engagement

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
12.1 Stakeholder Engagement – Building Partnerships	Identify possible stakeholders when working in intelligence roles including the agencies who work in fraud intelligence.	Explain the need to build and maintain new partner/ stakeholder relationships with those involved in intelligence to achieve progress on objectives, key initiatives and shared interests.	Demonstrate the ability to actively build and maintain new partner/ stakeholder relationships to achieve progress on objectives, key initiatives and shared interests.	Evaluate the building and maintaining of new partner/stakeholder relationships. Demonstrate effective engagement with senior stakeholders to achieve required risk mitigation measures, offering technical insight.
12.2 Stakeholder Engagement – Risk Mitigation	Identify the need to engage senior stakeholders to achieve risk mitigation measures.	Explain the need to engage senior stakeholders to achieve risk mitigation measures.	Demonstrate the ability to inform the engagement with senior stakeholders to achieve risk mitigation measures.	Evaluate the engagement of senior stakeholders to achieve the required risk mitigation measures.
12.3 Stakeholder Engagement – Improve / VFM	Identify the need to work with stakeholders to define and improve service delivery, and value for money outcomes.	Explain how to work with stakeholders to define and improve service delivery, and value for money outcomes.	Demonstrate the ability to work with stakeholders to define and improve service delivery, and value for money outcomes.	Evaluate service improvements and value for money outcomes by working with stakeholders at all levels, using technical expertise to identify key stakeholders.
12.4 Stakeholder Engagement – Intelligence Partners	Identify the agencies that work in fraud intelligence.	Explain who are the partners in the government fraud intelligence community and law enforcement sector.	Demonstrate networking with partner organisations in the government fraud intelligence community and law enforcement sector organisations and develop beneficial working relationships.	Evaluate networking with partner organisations in the government fraud intelligence community and law enforcement sector and develop beneficial working relationships. Demonstrate a well-developed network of contacts within the government fraud intelligence community and law enforcement sector and act as a primary conduit to facilitate the progression of complex intelligence assignments.

13. Intelligence Manager or Senior Intelligence Analyst/Officer

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
13.1 Intelligence Manager or Senior Intelligence Analyst/Officer – Management of Team Resources and Activity	Identify the requirement for prioritising team resources and activity.	Explain how to prioritise team resources and activity.	Demonstrate practical application of how to prioritise team resources and activity.	N/A
13.2 Intelligence Manager or Senior Intelligence Analyst/Officer – Departmental/ Strategic Objectives	Identify the organisations departmental and strategic objectives.	Explain the organisations departmental and strategic objectives and how these align to their work.	Apply the organisations departmental and strategic objectives in managing the work of the team.	N/A
13.3 Intelligence Manager or Senior Intelligence Analyst/Officer – Authority and Financial Approval	Identify how to recognise expenditure outside of intelligence costs.	Recognise how to identify expenditure outside of intelligence costs.	Demonstrate practical application of monitoring and approving expenditure outside of routine intelligence costs.	N/A
13.4 Intelligence Manager or Senior Intelligence Analyst/Officer – Decision Making – Dissemination	Identify decisions regarding dissemination that require management approval, internally and externally to the Organisation.	Explain when dissemination requires management approval internally and externally to the Organisation.	Demonstrate approval and decision making in regards to regarding dissemination internally and externally to the Organisation.	N/A
13.5 Intelligence Manager or Senior Intelligence Analyst/Officer – Critical Incidents	Identify a critical incident and when management intervention is required.	Explain the process for dealing with a critical incident and the types of interventions that may be required.	Demonstrate the ability to handle critical incidents, which require management intervention.	N/A
13.6 Intelligence Manager or Senior Intelligence Analyst/Officer – Legislative Authority	Identify situations where authority is required to carry out legislative governed activity.	Explain the process for the granting of authority, when required to carry out legislative governed activity.	Demonstrate the application of the process for granting authority when required, to carry out legislative governed activity.	N/A
13.7 Intelligence Manager or Senior Intelligence Analyst/Officer – Case Progression and Review	Identify the need to conduct intelligence product reviews, monitor progression and identify the relevant departmental guidance, legislation and aims.	Explain how to conduct intelligence product reviews, monitor progression and identify the relevant departmental guidance, legislation and aims.	Demonstrate how to conduct intelligence product reviews, monitor progression and identify the relevant departmental guidance, legislation and aims.	N/A

13. Intelligence Manager or Senior Intelligence Analyst/Officer

	Trainee (T)	Foundation (F)	Practitioner (P)	Advanced Practitioner (AP)
13.8 Intelligence Manager or Senior Intelligence Analyst/Officer – Quality Control & Performance	Recognise there is a process for quality control relevant to intelligence.	Explain the process for quality control relevant to intelligence.	Demonstrate application of existing quality control processes for intelligence.	N/A
13.9 Intelligence Manager or Senior Intelligence Analyst/Officer – Productivity & Management Information	Identify the need to review productivity using relevant management information.	Explain how to review productivity using relevant management information.	Demonstrate the ability to review productivity using relevant management information.	N/A
13.10 Intelligence Manager or Senior Intelligence Analyst/Officer – Information Management	Identify relevant information management policies complying with relevant legislation including DPA and information commissioner guidelines.	Explain relevant information management policies complying with relevant legislation including DPA and information commissioner guidelines.	Demonstrate the application of relevant information management policies complying with relevant legislation including DPA and information commissioner guidelines.	N/A
13.11 Intelligence Manager or Senior Intelligence Analyst/Officer – Stakeholder engagement	Identify the need to actively build and maintain new and existing stakeholder relationships to benefit the team and organisational aims and objectives.	Explain the need to actively build and maintain new and existing stakeholder relationships to benefit the team and organisational aims and objectives.	Demonstrate the ability to actively build and maintain new and existing stakeholder relationships to benefit the team and organisational aims and objectives.	N/A
13.12 Intelligence Manager or Senior Intelligence Analyst/Officer – Critical Risk Management	Identify the process for identification and management of critical risks and possible steps available to mitigate or escalate.	Explain the process for identification and management of critical risks and possible steps available to mitigate or escalate.	Demonstrate the ability to identify and manage critical risks and take steps to mitigate or escalate.	N/A

C. Guidance on Intelligence Processes

C1. Introduction

This guidance covers effective intelligence processes. Intelligence staff must be able to assess what matters are appropriate to the intelligence development, how these will be applied and the process by which this will be managed.

The creation of standard operating procedures should be considered for intelligence processes. All processes and procedures should be regularly reviewed and evaluated to ensure they are of the required standard and remain current.

> Intelligence staff must be able to assess what matters are appropriate to the intelligence development

Those working in Counter Fraud should have knowledge of the following legislation and policy and understand how it impacts upon their role:

- **Fraud Act 2006**
- **Theft Act 1968**
- **Bribery Act 2010**
- **Proceeds of Crime Act 2002**
- **Human Rights Act 1998**
- **Data Protection Act 2018**
- **Computer Misuse Act 1990**
- **Criminal Procedure & Investigations Act 1996**
- **Police and Criminal Evidence Act 1984**
- **Criminal Justice Act 2003**
- **Regulation of Investigatory Powers Act 2000**
- **Investigatory Powers Act 2016**
- **Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
- **Freedom of Information Act 2000**
- **Public Interest Disclosure Act 1998**
- **Government Security Classifications**
- **Civil Service Code**

C2. Intelligence Cycle

The Intelligence Cycle provides a framework for the collection, analysis and dissemination of intelligence and supports decision-making. The model highlights the need for intelligence products and using intelligence for effective tasking and coordination to reduce fraud crime and offending.

The Intelligence Cycle is structured around the following steps:

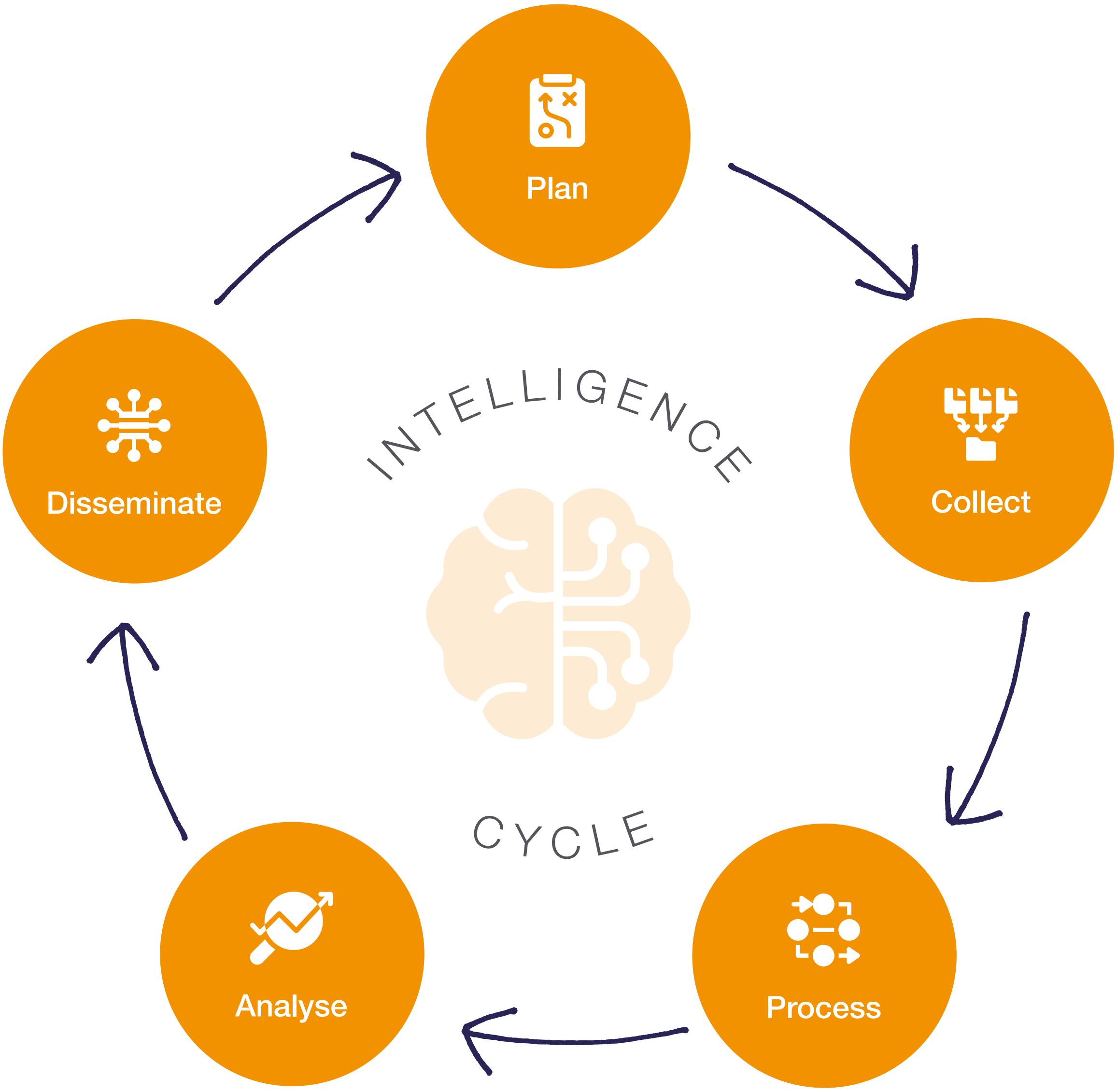


Figure 6. The Intelligence Cycle

Plan

This is where the objectives and direction are set and the intelligence needs are identified. There are three types of Intelligence requirement

- **Strategic** – Broad trends, anticipate future challenges long term planning and objectives.
- **Tactical** – shorter term plans specific objective within a defined timeframe.
- **Operational** – day to day to support frontline operations and resources allocated.

Collect

Information should be gathered (collected) from various sources (closed and open) with consideration given to opportunities to parallel source or turn information/intelligence to evidence and the means of acquiring it.

Process

Intelligence is information that has been through some type of process. The information should be assessed in line with the original objectives in the plan phase and then recorded with appropriate handling codes and dissemination instructions. Consideration should be given to any necessary sanitisation of sensitive information.

Analyse

Analysis is where you use analytical techniques to identify patterns, trends, potential threats and intelligence gaps.

Disseminate

This is to communicate the intelligence to relevant stakeholders. Sharing intelligence informs the decision-making process, helps to review plans and how to address any intelligence gaps. This should be done in line with any restrictions in dissemination instructions.

Benefits of the Intelligence Cycle

The Intelligence Cycle gives a structured approach to the collection, analysing and dissemination of fraud intelligence. It allows a thorough understanding of fraudulent activities by gathering information from various sources, identifying patterns and trends and enabling organisations to make informed decisions.

By continuously cycling through the process of collect, analyse, disseminate, organisations can respond promptly to emerging threats and adapt strategy accordingly, acting on intelligence that comes to light. Potential risks and vulnerabilities can be identified and measures put in place to mitigate them. The Intelligence Cycle promotes informed decision making by providing timely and accurate intelligence to decision makers to address threats, exploit opportunities, mitigate risks and allocate resources efficiently and effectively.

C3. Collection of Fraud Information

- The intelligence function should work closely with the organisation's risk, detection, prevention and investigation functions to collect and manage information on potential frauds and fraud risks.
- Collection of intelligence should be in line with a strategic intelligence requirement or a specific case of potential fraud.
- When handling referrals of potential fraud e.g. through a whistleblower, the following information should be sought, name of the individual accused, time(s) and date(s) of incident(s), location, method, any potential evidence (consider 5WH - who, what, where, when, how).
- Thought should be given as to whether it would be valuable to alert the rest of the organisation and/or partners to the fraud or fraud risk in order to improve vigilance, sanitising information if necessary. It is important to consider the most suitable medium for sharing this alert to reduce undue panic.
- Reporting known frauds to Action Fraud should be considered.
- Compliance with legal and ethical requirements of collecting information must always be followed and monitored.

C4. Recording of Fraud Information

All information received regarding potential frauds and fraud risks should be recorded on a register. The details recorded should include:

- Time and date the information was received.
- The method of reporting.
- A new unique reference number for the intelligence that matches that on the intelligence database.
- Details of the person or organisation providing the information including name, address, phone number, accessibility and security for making contact.
- Description of the potential fraud.
- Details of the staff member recording the information.
- Details of the initial action taken with the information.
- Only authorised staff members according to the organisation's policy should be able to access this register.
- The original information should be stored in a secure part of the network.
- A sanitised version should be recorded on an intelligence database as sanitised intelligence reports, following the same conventions (see Products).
- Each report on the intelligence database should be given a unique reference number.
- In certain circumstances checks should be made to see whether the information is already held in order to establish links, avoid duplication and direct resources efficiently.
- It is not necessarily practical for organisations that receive a large volume of information to upload the entirety as structured intelligence reports. In this case, there should be a method to establish which information should be uploaded according to potential harm and which should be stored in its original form on the network.
- Frauds may be grouped according to their type in order to compile data on the type of fraud the organisation is most vulnerable to.
- The provisions of the Data Protection Act 2018 and the Public Interest Disclosure Act 1998 must be adhered to.

C5. Evaluation of Fraud Information

- New information regarding potential fraud should be evaluated at a speed, and to the level of threat/risk posed by the information, proportionate to the nature of the incidents the organisation deals with.
- An evaluation of how accurate and reliable the source and information is should be made, using the codes in the new intelligence report if these are appropriate.
- Risk to the source and subject must be assessed and immediately escalated if appropriate.
- Checks should be made to assess whether entities within the information are already known to and/or being investigated by the organisation or other organisations, for example by checking the Joint Asset Recovery Database and by utilising intelligence sharing networks.
- Each report should result in one of the following actions:
  - Initiating a response. This will depend on the nature and capability of the organisation but could involve immediately initiating a civil or criminal investigation, if it meets the organisation's case acceptance criteria for an investigation, or sharing the report with other partners.
  - Conducting further research and development before assessing whether to investigate.
  - Making a decision to not do anything, but to record and review the information at a future date.
  - Deciding to take no action.

C6. Intelligence Grading – 3x5x2

Intelligence is information that has been collected, undergone a process of evaluation and assessment and recorded in a way that is searchable and retrievable.

A way to evaluate and assess the information is the 3x5x2 process. The process seeks to understand where the information is from (source), what the information is telling us (evaluation) and how the information can be shared (handling). A consistent approach to the evaluation and assessment increases confidence in the sharing of intelligence across agencies and organisations.

The 3x5x2 consists of the following sections:

Source evaluation – this is the assessment of where the information has originated.

- 1 – **Reliable** – used when the source is believed to be competent and information received is generally reliable. The source will have provided information previously which was verified. Reliable sources can include information from people, technical (e.g. CCTV), scientific and forensic sources. If it cannot be ascertained if the source is both competent and reliable then the assessment should be given as unreliable.
- 2 – **Untested** – used when the source has not previously provided information to the person receiving it. The source may not necessarily be unreliable, but the information provided should be treated with caution until it can be corroborated. Untested sources can include reporting hotlines such as Crimestoppers and open source information.
- 3 – **Unreliable** – used where there is reason to doubt the reliability of the source. Any reason to doubt the source of the information should be outlined in an attached risk assessment and corroboration of the information should be made.

Information Evaluation

This assesses what is being reported in the body of the intelligence report.

- **A – Known directly** – this is information obtained first-hand, e.g. witnessing it. It is important to differentiate between what is first-hand and what may have been told/ over heard from a third party (that would be evaluated as known indirectly)
- **B – Known indirectly** – information that the source has not witnessed themselves, but the information can be corroborated by separate information that is evaluated as A (known directly). Care should be taken when obtaining corroboration to ensure that the information that is presented as corroboration is independent and not from the same original source.
- **C – Known indirectly** – this is information that the source has been told by someone else (third party).
- **D – Not known** – when the source of the information is not known for example information received via an anonymous reporting line.
- **E – Suspected to be false** – when there is reason to believe that the information provided is false. The reason for suspecting the information to be false should be recorded on a risk assessment.

> Intelligence is information that has been collected, undergone a process of evaluation and assessment and recorded in a way that is searchable and retrievable

Handling/Sharing

This outlines any conditions which must be adhered to when sharing the intelligence.

- **P** – There is a lawful basis to share the information and there are no sensitivities around the sharing. The sharing will assist to protect life or property, assist to preserve order, prevent the commission of offences or bring offenders to justice. Consideration should be given to who is asking for the information, why they want it and what do they intend to do with it.
- **C** – Sharing is permitted but certain conditions must be observed. A risk assessment should be completed and an application for public interest immunity (PII) should be considered if the intelligence is subsequently used in court.

The body of the information within a 3x5x2 report should answer the who, what, where, when, why, how of the information and must not mention source of information.

Intelligence Confidence Assessment

The below table can be used in conjunction with the 3x5x2 to indicate the confidence of an intelligence report and inform decision making.

	Reliable	Untested	Unreliable
Known Indirectly but Corroborated	High	High	Medium
Known Directly	High	Medium	Low
Known Indirectly	Medium	Low	Low
Not Known	Low	Low	Low
Suspected to be false	Low	Low	Low

Figure 7. Intelligence Confidence Assessment Table

C7. Intelligence Development

- Intelligence should be developed with a clear purpose and customer in mind (for example to support an investigation, examine a report of potential fraud or to build a picture of a certain fraud type).
- There should be a system in place to record all current intelligence cases and their progress.
- For each new development of an intelligence case a record of events should be established, recording research completed, decisions made and their rationale to create a clearly auditable process.
- Research into individuals e.g. through the checking of databases, organisation systems or communications data, should be in accordance with relevant legislation and remain proportionate to the incident. Certain kinds of information should not be accessed without the appropriate authorisation and handling procedures, for example covert material may need to be accessed through a confidential unit.
- All relevant research, sanitised if necessary, should be entered onto the intelligence database following the same conventions as those used for an intelligence report.
- Intelligence development should result in an intelligence package of the information discovered, collated and analysed (see Skills) which can be disseminated to the customer or considered for acceptance as an investigation.

C8. Creating an Intelligence Analysis Product

An intelligence analysis product could address both strategic and tactical questions.

Examples include:

- A threat assessment of the organisation's fraud risk.
- An analysis of data e.g. from bank accounts or communication devices to answer a set of questions.
- A profile of a certain type of fraud and how it affects the organisation.
- Terms of reference should be agreed between those commissioning and those delivering the product.
- A collection plan should be formed to identify what intelligence is needed and whether it has been gathered.
- Once collected, intelligence should be analysed. Documents to aid this could also be produced e.g. an association chart, depending on the type of end product that is being created.
- Any hypotheses derived from the process should be tested, or if this would be a resource-intensive piece of work, a recommendation be made to test them.
- Conclusions, judgements, recommendations and/or predictions should be clearly stated, accompanied by rationale and evidence.
- If applicable, the intelligence product should be submitted to relevant parties for quality review and redraft if necessary.
- The product should be communicated to those who commissioned it and any other relevant parties and feedback requested.

C9. Sharing/Disseminating Fraud Intelligence

- When intelligence has potential significance to a partner, it should be shared unless there are overriding legal reasons not to.
- Sharing intelligence with partners should be risk assessed on a case-by-case basis.
- Dissemination should only take place when it is legal and does not breach laws on confidentiality.
- Due consideration must be given to achieving a balance between the protection of an individual's rights and the public interest. It must be assured that sharing the information under consideration is proportionate, necessary and meets a legitimate need under Article 8 of the European Convention of Human Rights.
- Before sharing intelligence, consideration must be given towards whether certain details should be sanitised before disseminating further or restrictions should be put in place on further dissemination.
- Likewise, if the intelligence has been received from a partner with restrictions attached, due consideration must be given to these before sharing further.
- A dissemination register of all intelligence shared inside e.g. to other areas of the organisation, audit committees or an investigation team, and outside the organisation should be created, including the following information:
  - Time and date the report was disseminated.
  - Destination of the report i.e. the individual, team and organisation.
  - Name of the staff member responsible for dissemination.
  - Name of the owner of the report.
  - Unique reference number of the report.
  - Evaluation and handling code.
  - Details of any restrictions in further dissemination.

C10. Accepting an Intelligence Case for Investigation

The organisation should have case acceptance criteria to decide which intelligence cases to investigate and assign resources to. This will vary depending on the organisation's function.

Staff dealing with the initial information will consider the status of the source, in particular considering whether the source could be vulnerable. Any concerns that the source may be vulnerable should be escalated to a manager for consideration of action.

The assessment of each case should consider the organisation's strategic priorities, resources available, quality of the intelligence case, the chance of the investigation being successful and the potential impact of the fraudulent activity.

In larger organisations, intelligence cases should be put before a tasking group who assess each case according to the criteria. Decisions and rationale should be fully recorded.

C11. Briefing Tools

Fraud intelligence helps to support the organisation by providing insights into risks, emerging issues and aiding decision making and policy development, ultimately helping to achieve the strategic aims and objectives. Being able to brief intelligence in a clear, concise and structured way provides the decision makers with the necessary and relevant information to make those decisions.

Intelligence briefings should be a concise summary of the information which has been established through the intelligence development process. This should include a threat/risk assessment along with consequences and impacts of not investigating further. The criminality identified should be outlined and lines of enquiry highlighted including parallel sourcing opportunities. This helps to maintain a firewall/sterile corridor between intelligence and investigations.

IIMARCH[3] is a briefing model used in operational settings for the briefing of intelligence. IIMARCH stands for:

- I **Information and Intelligence**
- I **Intention**
- M **Method**
- A **Administration**
- R **Risk**
- C **Communication**
- H **Human Rights**

> Fraud intelligence helps to support the organisation by providing insights into risk, emerging issues and aiding decision making

- **Information and Intelligence** – a summary of what information/intelligence is currently known, what is the background to the briefing.
- **Intention** – the briefing should have a purpose/intention. This could be to brief investigators of intelligence development where criminality needs to be investigated, or emerging trends in fraud intelligence.
- **Method** – what methods have been used to gather/develop the intelligence and what investigation methods are now open. Parallel sourcing can be highlighted.
- **Administration** – covering what resources are required/investigation or intelligence techniques to be deployed in order to achieve the aims as well as the relevant legislation/legal basis.
- **Risk** – the risks involved should not only cover the risks presented by the intelligence and what has been identified but what the risks are in taking further steps or not taking further steps.
- **Communication** – consideration should be given to methods of communication to ensure that everyone who needs to know about the intelligence is made aware and that intelligence is shared in agreed ways.
- **Human Rights** – any intelligence gathering or investigation should consider Human Rights and particularly article 6 right to a fair trial and article 8 respect of private and family life.

[3] https://www.college.police.uk/app/operations/briefing-and-debriefing

D. Guidance on Intelligence Products

D1. Introduction

This guidance covers what good quality products should include. An intelligence report can be accompanied by a package of relevant information and analysis products.

D2. Intelligence Collection Plans

Intelligence collection plans are used to coordinate and manage the collection of intelligence in support of a specific issue/task.

Intelligence collection plans should include:

- **What the problem is** – why are we planning to collect intelligence and what is the problem/risk that needs addressing? This should include a reference to source intelligence and assessment of the confidence of the intelligence. The proportionality and necessity of the activities that will be used for collecting the information/intelligence need to be justified.
- **What the objective is** – why do we need to collect intelligence? Once the problem is identified then the purpose and aim for collecting intelligence should be outlined, showing how the collection is going to achieve the aim and address the problem (anticipated outcome).
- **What we know and what do we need to know** – identifying where intelligence can be used to corroborate information and highlight intelligence gaps contain the necessary information requirements in order to inform a comprehensive and accurate intelligence picture.
- **How we going to answer the questions/ fill the gaps** – outline the methods of intelligence collection that will be utilised (open source/info share requests/covert taskings), where information could be found to address the intelligence gaps and what resources are needed with consideration of IPA/RIPA/data protection requirements.
- **How the intelligence going to be handled** – where will the intelligence be recorded and is further dissemination needed, who needs to be kept informed and is a briefing cycle required?
- **Review process** – the intelligence collection plan should be monitored and updated regularly to assess when intelligence gaps have been met, assess the intelligence picture being presented and identify further intelligence gaps. This review process should also identify any limitations to the intelligence collection.

D3. Intelligence Report

An intelligence report should be used to submit, evaluate and disseminate intelligence. Standardisation of the intelligence report is crucial to sharing intelligence with partners.

An intelligence report must contain the following features:

- Government security classification.
- A unique reference number to provide an audit trail of received information.
- Reporting member of staff. Organisational policy may be to omit this to remove those working in an intelligence environment from the chain of evidence.
- The date/time of report.
- Who the report is being disseminated to, if applicable.

- Source evaluation.
- Handling code and content.
- Information should be clear and without abbreviations.
- It should be understood without the need to refer to other information sources.
- It must give no indication of the existence or nature of the source or the proximity of the source to the information; and where possible, information should be corroborated, potentially through information already held in other databases. Where this has been done, this should be recorded within the initial intelligence report.
- Common entities within intelligence e.g. names, addresses, date of births, should be recorded in a consistent way defined by the organisation.
- There should be no mention of the source in any part of the intelligence report. Organisations must have measures in place to ensure that the identity is not revealed.
- A means of cross-referencing intelligence reports to the original source material should be created by the organisation. A policy should be created to determine who in the organisation has access to source material.
- Items of information from the same source but concerning different matters should be recorded on separate intelligence reports. If a single source of information provides several items of intelligence relevant to the same issue that could compromise the source, separate intelligence reports can be considered.

D4. Intelligence Analysis Products

- Intelligence analysis products should make the most accurate and clear judgements possible, based on the intelligence available and known information gaps.
- Products should be independent of political consideration.
- The quality and credibility of underlying sources, data and methodologies should be taken into account in the analysis and described where appropriate.
- The certainty of a judgement should be expressed using the yardstick of uncertainty (see below) in order to develop a consistent understanding of certainty.

Qualitative Statement	Associated Probability Range
Remote/Highly Unlikely	<10%
Improbable/Unlikely	15% - 20%
Realistic Possibility	25% - 50%
Probable/Likely	55% - 70%
Highly/Very Probable/ Likely	75% - 85%
Almost Certain	>90%

- The product must distinguish between evidence and analysts' assumptions, interpretations and judgements, explicitly stating the latter when used.
- Alternative hypotheses/judgements to those favoured in the product should be considered and included where useful.
- Examples of types of analytical products include – Pattern Analysis, Network Analysis, Comparative Case Analysis and Red Teaming.

D5. Threat Assessment

A Fraud intelligence threat assessment is used to identify, analyse and evaluate potential fraud threats. Based on intelligence from various sources it can highlight emerging trends within the fraud landscape which may impact the organisation. This horizon scanning allows decision makers to put into place steps to mitigate these threats.

A threat assessment should include:

- Summary of the intelligence, any corroborating factors or indicators that fraud threat is already impacting.
- Identify any gaps in the intelligence.
- The possible impacts of the fraud threat indicated by intelligence – what does it mean to the organisation?
- Recommendations.

D6. Subject Profile

A subject profile is a detailed report of an individual who forms part of an ongoing investigation (including intelligence development). A subject profile helps to identify intelligence gaps, identify prosecution opportunities and provide justification for an individual to form part of an investigation. A subject profile should have an assigned owner and be a living document which is updated and reviewed during the span of the investigation. The document should also be stored centrally so the information may be retrieved if necessary.

A subject profile should contain:

- Date and version control.
- Reasons or justification for the subject profile being commissioned (source intelligence reference).
- Name (including nicknames and aliases), date of birth, addresses, linked vehicles.
- Family and relationships.
- Lifestyle and habits.
- Employment details.
- Criminal record details.
- Financial profile.
- Risk assessment.
- Highlight potential new sources of information.

D7. Problem Profile

A problem profile is used to provide a better understanding of an established or emerging issue. A problem profile can be used to raise and prioritise an issue. A problem profile should be a current document and kept updated until such time that the problem is resolved.

A problem profile should:

- Be based on the research and analysis of a wide range of information sources.
- Have date and version control and reasons or justification for the problem profile being commissioned (source intelligence reference).
- Be formed around the 5WH (who what where when why and how).
- Through analysis of information provide recommendations, predictions, highlight intelligence gaps and new intelligence sources and provide a risk assessment of the problem.

> A problem profile can be used to raise and prioritise an issue

E. Guidance for Organisations

E1. Introduction

The guidance set out below is for public sector organisations to present a consistent cross-government approach to counter fraud intelligence and analysis and raise the quality of organisations' counter fraud work and the skills of their individuals. The aim is twofold; to outline what individuals working in counter fraud should aim to have in place in their organisation; and for organisations to gain an understanding of what should be in place in Counter Fraud areas.

They are designed to help organisations identify the research, training and resources needed to develop their capability further. Individuals should use this guidance and competency framework to measure and develop their skills.

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

This document focuses on an organisation's capability to apply the use of intelligence associated with their counter fraud activities.

E2. Structure

- The organisation should put in place a structure for the management and configuration of the intelligence function. The head of the function should ensure the implementation and development of standards.
- Where possible, the structure and job roles should be consistent with those in other established organisations by following the National Intelligence Model (NIM).
- All staff should be trained to an appropriate level for their job role, ensuring they can carry out tasks legally and competently. The organisation should conduct a skills audit to ensure its needs are met by staff and resolve gaps through training or recruitment.
- Staff managing an intelligence function should consider the correct application of NIM to their organisation and its information assets.

E3. National Intelligence Model – NIM

The National Intelligence Model (NIM) was introduced into law enforcement in 2000. The NIM structure is illustrated below. It was the result of work by the then National Criminal Intelligence Service (NCIS) and the Association of Chief Police Officers (ACPO)[4]. The model promotes an intelligence led response, guiding intelligence activity and decision making and offering a framework to resource, collect and disseminate intelligence.

Benefits of the National Intelligence Model

- Gives a structured approach to intelligence activity, ensuring consistency and coherence in decision making.
- Allows activity to be risk focused, maximising the allocation of resources.
- Facilitates collaboration and information sharing across agencies and departments enhancing overall intelligence capabilities.
- Promotes accountability and oversight by defining roles and responsibilities.
- Allows for flexibility to adapt to evolving threats and changing priorities over time.

[4] Section 3 of National Intelligence Model Code of Practice - https://library.college.police.uk/docs/npia/NIM-Code-of-Practice.pdf

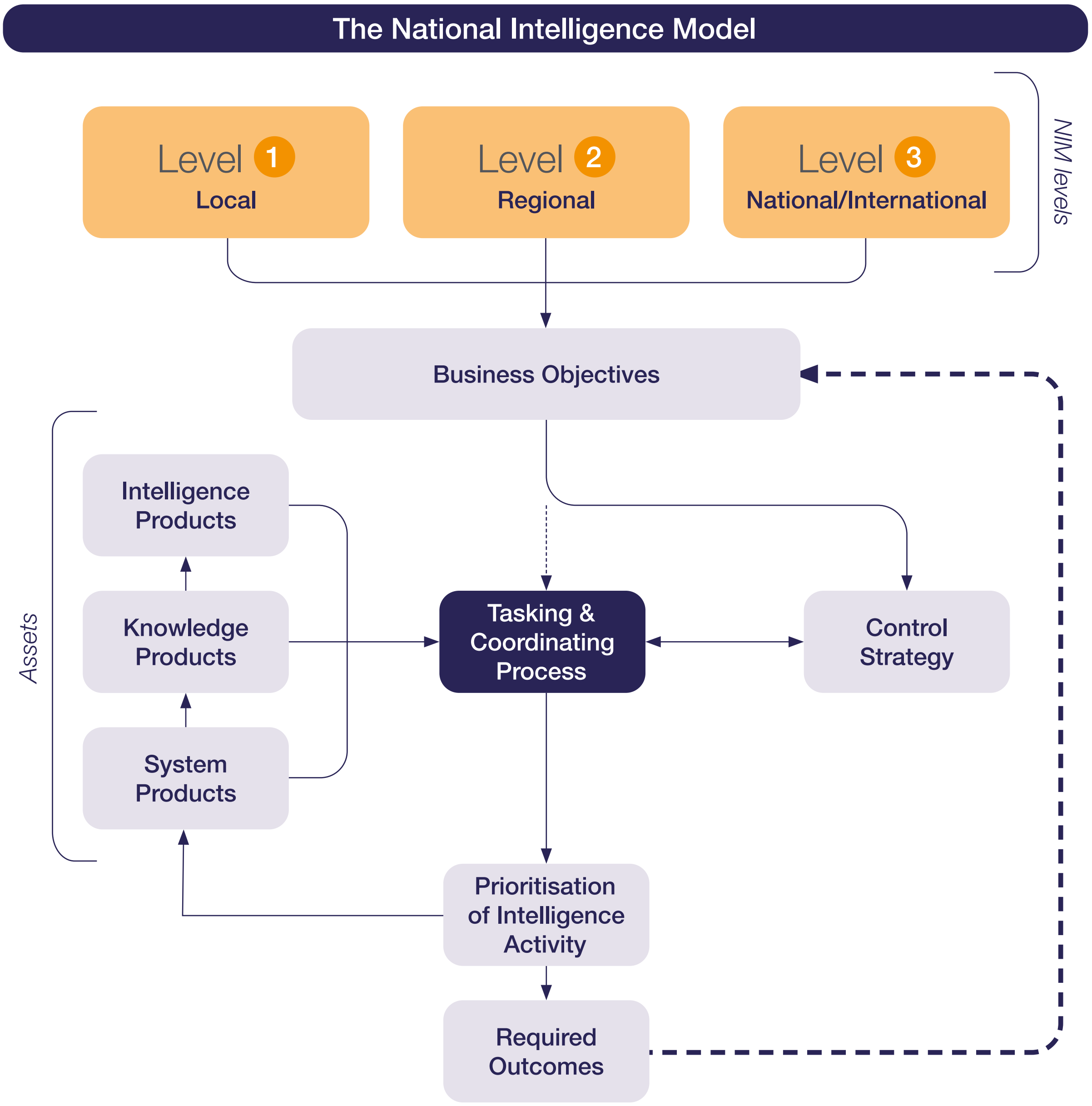


Figure 8. The key elements of the National Intelligence Model

Central to NIM is the Tasking and Coordinating process. This process is linked to the Business Objectives and fed by Intelligence Assets (Intelligence Products, Knowledge Products and System Products) which are then reviewed against the Control Strategy and Required Outcomes. The NIM can operate effectively at any of the three levels - Local, Regional (cross boarders) and National. The Tasking and Coordination element ensures that Intelligence Activity is correctly directed and efficiently executed to support informed decision making and enhance the Counter Fraud environment.

NIM levels

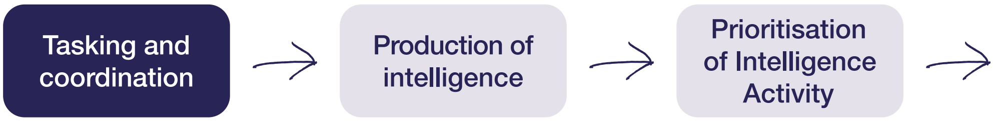
The NIM levels are described here, which clarify the range and differences for consideration when evaluating intelligence.

Level	Descriptor	Description
1	Local	Local issues impacting on a force area often linked to volume crime offending
2	Cross Border	Cross border impacting on several forces and/or agencies
3	National/International	Serious and organised crime often requiring a national proactive response

NIM control strategy

The NIM control strategy details the organisational priorities to counter fraud and may relate to detection, prevention and enforcement. It provides a framework for those attending the Tasking and Coordinating meetings to prioritise resources and inform the decision-making process. The control strategy should be developed in a collaborative manner engaging with a wide range of stakeholders. The control strategy can be amended by those attending the strategic tasking group.

Tasking and coordination group meetings



Tasking and coordination → Production of intelligence → Prioritisation of Intelligence Activity →

Taking and coordination meetings are ‘driven’ by four key intelligence products, the Strategic Assessment, Tactical Assessment, Target Profiles and Problem Profiles. Two meeting types may take place:

- **Strategic** – this meets 3 - 6 monthly and considers the control strategy, setting the priorities for the intelligence, prevention, disruption, and enforcement priorities and resource control.
- **Tactical** – meets weekly to review the tactical assessment and reviews how the current plans are fulfilling their objectives. It uses a tactical menu to respond to emerging issues. The frequency of the tactical meetings can change depending upon the threats being managed at the time.

E4. Strategic Intelligence

- Organisations may have a strategic intelligence function at the heart of their intelligence function; the size of it should depend on the organisation's resources. This is crucial for proactive fraud defence, rather than just the reactive investigation of reported frauds.
- The strategic fraud intelligence function should produce assessments that identify, evaluate and monitor the organisation's fraud risks in order to decide priorities. It should identify areas in which its knowledge is incomplete and commission research into these, including potential future trends.
- This should work in tandem with the organisation's risk, detection, and prevention functions. Strategic intelligence can be found proactively in the collection of this wider information and the identification of anomalies, e.g. in audit reports, security reviews and payroll information, not just through the reports of fraud it receives. Conclusions from strategic documents should contribute to the organisation's fraud risk assessment and guide the implementation of its prevention controls.
- It may be the case that the intelligence function produces a strategic assessment of the organisation's overall fraud risk, a summary of its priorities and a list of intelligence requirements that outlines the information required to fill gaps in knowledge.
- A process should be in place to approve these documents. The organisation should also have a means of agreeing actions and aligning resources to address the problem trends identified.
- The strategic assessments should be communicated to senior members in the organisation's governance structure, such as its audit committee.
- The organisation must decide how often to update these documents to ensure they remain current and relevant. As a guide they should be revised annually.

Strategic Intelligence Assessment

- **Purpose** – A strategic intelligence assessment (SIA) is used by senior leaders to give an overview of the current and long-term issues affecting or likely to affect the fraud landscape. It should be used to draw inferences and make recommendations for measurement, prevention and future fraud strategy. The SIA helps to define an intelligence requirement and aid decision making. The strategic intelligence assessment is a living document and should be maintained to ensure it is current and relevant. Information collection and analysis in support of the SIA must also be ongoing and can include problem profiles, trends analysis and horizon scanning.
- **Content** – The strategic assessment should be based on the research and analysis of a wide range of internal and external information sources. It should contain:
  - The information sources used and methods (the date/age of information should be taken into account as the assessment should be made on current/recent intelligence).
  - Overview of the current fraud intelligence taking into account national/international trends and emerging threats.
  - Analysis of Fraud levels based on the intelligence.
  - Public perception of the issues.
  - Recommendations.
  - Prioritisation of the identified issue/outcome.

E5. Tactical Intelligence

- Understanding sources of information, their legal gateways and effective use of that information is the core service provided by tactical intelligence staff.
- Staff within the tactical intelligence function will be called upon to advise and inform lines of enquiry developed by the investigating officer and officer in charge of a fraud enquiry, in particular covert means of acquiring information.
- Although a considerable amount of work may be undertaken to commence an investigation into possible fraud at the start, the themes identified in the offending will be continually revisited throughout the subsequent investigation. Considerations such as new suspects and witnesses in investigations, methods for laundering the proceeds and modus operandi will be identified, requiring research and analysis. This work is key to an effective tactical intelligence function.

Tactical assessment

- **Purpose** – A tactical assessment is used to define a short-term/specific issue which needs to be actioned. It should be used to draw inferences and make recommendations for prevention, measurement, detection or further intelligence gathering. A tactical assessment can also identify emerging patterns and trends which are then fed into the Strategic assessment. The tactical intelligence assessment is a living document and should be maintained to ensure it is current and relevant.
- **Content** – The tactical assessment should be based on research and analysis of a wide range of information sources. It should contain:
  - Detail on the information sources and method used in compiling the report.
  - Overview of the issue/problem and any updates since previous reviews.
  - Trends and emerging issues for the reporting period.
  - Progress and performance against set priorities.
  - Key dates for completion of actions.
  - Recommendations as a result of the research and analysis.

E6. Technical Infrastructure

A secure technical infrastructure should be in place on which to run an intelligence database that records, stores and shares intelligence. The system must support permission-based access. Information held needs to be protected.

The organisation must have a secure email address for the exchange of intelligence.

E7. Security

- All staff members in the intelligence function must be security cleared to the level of the material they are accessing. If the organisation has access to covert intelligence, extra legal requirements may need to be met.
- Intelligence material must be protected in accordance with the Government Security Classifications.
- The physical environment must be appropriate for the security classification of the intelligence being handled.
- Access to the intelligence function should be balanced to ensure access to it by the rest of the organisation ensuring there is a healthy level of engagement whilst still maintaining appropriate security of assets.

E8. Access to Information

- The intelligence function should provide for the centralised collection and collation of all information of intelligence value pertaining to fraud available from within the organisation.
- A decision must be made about whether intelligence on fraud involving individuals inside the organisation is stored separately to that held on external fraud. If it is stored separately it must be made clear who is authorised to handle it and safeguards put in place to ensure only these staff members can access it.
- The intelligence function must be able to access information and data in the organisation e.g. invoices to contractors, in order to identify information that indicates potential frauds and fraud risks.
- Arrangements should be in place, and followed, for other functions in the organisation to feed information into the intelligence function.
- There must also be policies and permissions in place to enable designated members of the function to access employee records in cases of insider fraud, if the intelligence function is responsible for this area.

E9. Relationships with Other Organisations

- Depending on its size and resource, in addition to its own intelligence database, an organisation should have access to other relevant systems. This could either be through direct access or via an agreement that enables indirect access. This includes other organisations' intelligence databases.
- Organisations with a smaller intelligence function should establish agreements with other organisations to access services e.g. access to communications data or bulk data analysis, which would be impractical to provide within the organisation.
- The organisation should put in place an information sharing agreement/ memorandum of understanding for sharing intelligence via a legal gateway with its partners. This should set out the statutory obligations of the organisations involved, together with the procedures to ensure effective, timely and consistent disclosure.
- The organisation should have a means of engaging with other organisations to assess joint threats and consider joint working opportunities.
- Organisations with no powers under the Regulation of Investigatory Powers Act 2000 or Investigatory Powers Act 2016 should have protocols in place with other organisations who have the capability to develop and manage human intelligence, obtain communications data and other work governed by the legislation where it is lawful, proportionate and necessary to do so.

E10. Policies

- Organisations must understand what specific capabilities they have under legislation.
- Organisations should have policies to support their counter fraud intelligence function covering:
  - Access rights to data held on the intelligence database.
  - Who is able to authorise access to and dissemination of certain types of intelligence.
  - The protection of sources and whistleblowers.
  - An information management strategy covering storage, retention, review and disposal of intelligence.
  - Security of information in accordance with the Government Security Classifications.
  - General information handling rules e.g. observing a clear desk policy and security of the physical environment.
- The organisation must have a policy on whether it develops some or all of its cases to the criminal standard. If it chooses to, these developments must comply with the Criminal Procedure and Investigations Act 1996, Police and Criminal Evidence Act 1984 and requirements under Public Interest Immunity, so that its intelligence can be used as evidence in court and disclosed.
- Organisations should ensure that there are clear policies in place governing intrusive methods of intelligence gathering. These methods will include the use of surveillance, the acquisition and monitoring of digital data and the management of sources of human intelligence. These policies should reflect the responsibility of all staff to understand the legal framework when dealing with these sources and the management and oversight of staff operating in this environment.

E11. Process

The extent and capability of the organisation’s intelligence function will, by necessity, depend on its resources and fraud risk profile. It should have the capability to generate, receive, record, collate, evaluate, develop, analyse and share intelligence and have established processes for these made available to staff.

Organisations should have a group who discuss whether to accept an intelligence case for investigation, and case acceptance criteria that supports this decision making.

Organisations should have a considered approach to how their intelligence and investigation functions interact.

> Organisations should have the capability to generate, receive, record, collate, evaluate, develop, analyse and share intelligence

F. Further Guidance

F1. Further Information

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

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

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

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

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

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

GCFP@cabinetoffice.gov.uk

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

Correspondence@giaa.gov.uk

Information on the Intelligence Categories and the breakdown of the categories can be obtained by emailing:

GCFP@cabinetoffice.gov.uk

Glossary

Competency command word	Definition
Core Disciplines	Areas of expertise, knowledge skills and experience that are needed to be called upon for an effective counter fraud response. They are not people role or category specific.
Sub Disciplines	Areas of additional knowledge skills and experience that enhance capability in those areas across a number of core disciplines.
Core Components	Behind each core and sub discipline there are high level components outline knowledge skills and experience required.
Elements	Specific descriptors of the skills knowledge and experience required within a core or sub discipline These are grouped into competency framework document.
Subject Matter Expertise	We will recognise not only technical specialism but also where individuals have deep knowledge in a particular subject for example Tax, Legal Aid or Grant Fraud.
Competency Framework	Group of elements found in core or sub disciplines. Grouped together with carrying levels of knowledge skills and experience required.
Competency Levels	Used to identify progression within the standards and competencies from Trainee to Foundation.
Categories	Defined combinations of elements which show the knowledge skills and experience expected from each core discipline. These enable a commons sense assessment of skills and draw distinction of those with a level of skill and those without.
Technical Specialism	Specific focused areas, usually build off or enhance core disciplines often the specialism and will be the primary focus of their role.

Public Sector
Fraud Authority