Government
Counter Fraud
Profession

Government Counter Fraud Professional Standards and Guidance

Fraud Risk Assessment Core Discipline

March 2022

Crown copyright disclaimer

Contents

A. Introduction to the Fraud Risk Assessment Discipline

A1. Purpose

This document contains the agreed professional standards and guidance for those persons and organisations undertaking Fraud Risk Assessments (FRA) within central government. These form part of the wider government Counter Fraud Standards covering all of the disciplines and sub-disciplines set out in the government Counter Fraud Framework.

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

The professional standards and guidance's aim is threefold:

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

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

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

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

These standards will form the basis of the FRA part of the Counter Fraud Profession that is being established within government. To be acknowledged as a counter fraud professional in fraud risk assessment, these standards must be met.

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

A2. Contents

This document contains the following:

- The Competency Framework outlining the knowledge, skills and experience required by those operating effectively and how these develop through the competency framework levels: Trainee, Foundation and Practitioner.

- Guidance for Professionals includes:
  -Product guidance setting out what good quality FRA products look like;

  -Process guidance describing the recommended processes for organisations to correctly implement an effective FRA approach; and

  -Organisation guidance outlining the key considerations for an organisation in relation to Fraud Risk Assessment.

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

A3. Government Counter Fraud Function

The Counter Fraud Function is one of government's fifteen functions. The aim of the Functions is to develop the Civil Service to evolve and be even more efficient. The Counter Fraud Function brings together over 15,000 public servants who work to find and fight fraud across the public sector, including those who focus on understanding and mitigating fraud risks. The Counter Fraud Function has published a Functional Standard[1] which applies to all government departments and their arms-length bodies and covers the planning, delivery and management of the measures to counter fraud, bribery and corruption. Part of the Strategy of the Counter Fraud Function has been to develop the first Counter Fraud Profession to provide discipline specific standards for individuals operating in counter fraud across the UK government and wider public sector.

The vision of the Counter Fraud Function is:

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

[1] See GOVS013 for information on www.gov.uk

Functions are embedded in government departments and arm's length bodies, and these teams make up the wider government function, supported by expertise in other public bodies and the functional centre. The Counter Fraud Centre of Expertise (CoEx) at the Cabinet Office is responsible for overall leadership of the function, including overseeing the strategy, defining standards and monitoring performance. Within the Functional Standards for Counter Fraud, there is a clear ask of Organisations in relation to Fraud Risk Assessment.[2]

A4. Governance of the Government Counter Fraud Profession

The Government Counter Fraud Profession has a clear governance structure, established in 2015. The Government Counter Fraud Profession Board leads oversight of the Profession, with senior members selected from public sector organisations with a mature response to counter fraud and economic crime. Member organisations vary in size and the number of staff they have working in the Counter fraud, but all have an equal vote on the Board. The key principles when developing the Profession, as agreed by the Board are Collaboration, Choice, Empowerment and Pace.

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

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

A5. Government Counter Fraud Framework

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

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

- **Core Disciplines:** The core disciplines include a functional leadership level (Leadership, Management Strategy) for those that are responsible for

[2] See GOVS013 for information on www.gov.uk

coordinating an organisation's overall response to fraud and economic crime. The main area is in the functional delivery level. This details the core disciplines that an organisation may use in an effective counter fraud response. Within these core disciplines are details of the knowledge, skills and experience needed to undertake these disciplines effectively.

- **Sub Disciplines:** The sub disciplines are areas of additional knowledge, skills and expertise that enhance capability across a number of core disciplines. For instance, knowledge, skills and experience in Bribery and Corruption will help counter fraud professionals undertake more effective risk assessments and investigations (depending on their role).

This document is intended to reflect the position in England and Wales

Government Counter Fraud Profession Standards

A6. Definitions

For many years there was no commonly agreed definition for risk or threat within the fraud and economic crime communities. Therefore, experts across the public sector and beyond have collaborated to now agree these definitions. Below are the agreed HMG definitions, which are formally approved by the Government Counter Fraud Profession Board. These are applicable for use when conducting a Fraud Risk Assessment.

A risk is defined as the possibility of an adverse event occurring or a beneficial opportunity being missed. If realised it may have an effect on the achievement of objectives and can be measured in terms of likelihood and impact.

A risk arises out of threats. **A threat** is defined as a person or group, object or activity, which has the potential to cause harm to the achievement of the organisation's objectives. To understand the risk, it is important to take into account and assess the capability and intent of those posing the threat.

Fraud is defined as set out in the Fraud Act 2006. The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. In HMG we use this definition but for reporting instances of fraud we apply the standard from civil law, the balance of probabilities test.
In all three classes of fraud, it requires for an offence to have occurred, the person must have acted dishonestly and that they acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or risk of loss) on another. Whilst intent is a key factor in determining fraud, it may not always be apparent and so for the purposes of protecting the UK public purse we incorporate the risk of **Error** alongside the risk of Fraud when undertaking Fraud Risk Assessments. Therefore all references to fraud risk within this document should be taken to also include the risk of error, which represent losses where there is insufficient evidence to prove intent.

A7. Scope

Fraud Risk Assessment (FRA)
Fraud Risk Assessment covers how to effectively identify, describe and assess individual fraud risks and develop these into a comprehensive fraud risk assessment for the entire organisation. It covers how to identify and evaluate mitigating controls, including understanding their limitations.

Fraud Risk Assessment vs Fraud Threat Assessment
Risk and threat assessments are often linked. Although there is no set definition, threat assessments in this context focus on 'the capabilities and intent of a person or group with the potential to cause harm to the organisation's objectives'. This can include an analysis of past frauds; the skills needed for a fraudster to launch a successful fraud, and the opportunities to commit a fraud on the organisation.

Some threats, for example the use of emerging technologies by third parties to commit new and unforeseen types of fraud, might be beyond the organisation's control to mitigate at the time the scheme is launched. In these circumstances organisations should use threat-related knowledge/strategic intelligence to aid risk prioritisation and review of control measures whilst the scheme is live. A threat assessment should be used to inform the likelihood section of the fraud risk assessment.

Fraud Risk Assessment vs Fraud Risk Management
FRA is a fundamental part of any Fraud Risk Management programme. It helps management understand the fraud risks that are relevant to the business; identify gaps or weaknesses in controls and mitigate those risks: It helps management to develop a practical plan for targeting resources to reduce the risks, which forms an integral part of any counter fraud response. Fraud Risk Management is the total process of how you use knowledge of the risks to manage fraud in the business. The Fraud Risk Assessment part of this cycle is explored in section C.

The 'evaluating controls and reviewing and reporting' parts of the Fraud Risk Management Cycle (steps in grey, see C.1 for diagram) sit outside the scope of this document. The responsibility for managing the whole cycle effectively rests with the

government counter fraud functional lead and as such details can be found in the Leadership, Management and Strategy Standards. It is accepted that in some organisations the functional lead may also be the person undertaking the FRA, and so that person will need to prove capability in relation to both standards.

B. Professional Standards and Competencies for Fraud Risk Assessment

B1. Introduction

The professional standards and competencies for Fraud Risk Assessment identify the knowledge, skills and experience required in this discipline. Individuals can use the standards to measure and develop their skills, not only within this discipline but also in others. This information is then helpful to target learning and development, and assist career planning.

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

The Professional Standards and Competencies are not intended to cover every eventuality or every specific issue that might arise and should be adapted to the organisation's resources and fraud risk profile. They are living documents, owned by the Profession Board and will be maintained and updated as applicable.

This document focuses on individuals' capability to complete a fraud risk assessment. A risk is defined as 'the possibility of an adverse event occurring or a beneficial opportunity being missed.'

This discipline is therefore focused on the practical assessment of fraud risk. It includes many factors, such as:

· An understanding of counter fraud, motivators of fraudsters and types of fraud;

· The process and techniques for effective communication and facilitation required for fraud risk assessment.

It also covers in detail the process of fraud risk assessment using knowledge of the business and engagement with the business to understand, articulate, log and evaluate fraud risks

B2. General Guidance

These professional standards and competencies specify the skills that are required by those involved in counter fraud risk assessment.

The skill competence levels required are at an increasing level of expertise; from Trainee to Foundation, and then Practitioner. These levels of expertise are not necessarily held by different roles within an organisation (see B4 for further explanation of the competency levels).

B3. General Principles

A Fraud Risk Assessment (FRA) is a process aimed at proactively identifying and understanding an organisation's vulnerabilities to both internal and external fraud. It is an essential element of an effective counter fraud response and, whilst it should be integrated into the organisation's overall risk management approach, requires specific skills, knowledge, processes and products. A proactive approach to understanding the organisation's fraud risks should be a priority when dealing with the issue of fraud. These risks can then be managed through effective mitigations such as control changes, policy changes, and compliance and audit activity.

Those undertaking an FRA must have a firm understanding of how to gather information held by those working in other disciplines, e.g. Intelligence, Detection, Investigation and Leadership, Management and Strategy.

Fraud Risk Assessors must be able to conduct professional and competent reviews to a standard that informs a robust process and decision for the business. They must also be able to talk confidently about how the organisation could be defrauded.

Fraud Risk Assessors will be skilled at understanding core business processes. They will support others by being able to recommend appropriate improvements in controls, ensuring that these are reported to those charged with governance, such as audit and risk committees.

They should recognise that other Counter Fraud specialists have different knowledge, skills and experience, both generally and covering specific areas; a community arrangement should be in place so that Fraud Risk Assessors can call upon advice from the Counter Fraud community when required. This community also serves to help individuals maintain their skills, keep them up to date, and access peer review and challenge to enhance ability. It also helps to build a wider picture of risk – which is vital in the role of a Fraud Risk Assessor.

B4. Competency Framework (Fraud Risk Assessment)

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

B4.1 Key Components Explained

Components outline, at a high level, the knowledge, skills and experience required for each core & sub discipline. There are 5 key components for Fraud Risk Assessment. These elements are then grouped into a Competency Framework.

B4.2 Competency Levels

Within the Competency Framework are three **Competency Levels**. These range from **Trainee, Foundation to Practitioner**. These can be used to identify progression within the Fraud Risk Assessment standard. The Framework helps to establish where your competency level is and where you have areas you might wish to develop.

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

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

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

B4.3 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 might be different to those below.

By considering the Fraud Risk Assessment activity you undertake, you will be able to determine which Category, A or B, is relevant.

For Fraud Risk Assessment there are 2 core categories:

A – Facilitator (Fraud Risk Assessment)

The facilitator focused on working with the business to help them draw out relevant fraud information to define and assess the fraud risks. They do this via engagement with key stakeholders in the business, through workshops and interviews. They present the information they gather back to the business.

B – Fraud Risk Assessor

The fraud risk assessor both facilitates drawing information out of the business (from activity such as workshops) and uses their experience to conduct research to provide additional insight and in order to further understand and assess fraud risks and communicate them effectively.

For each Category there is a specific group of elements from the Competency Framework that should be demonstrated.

There will be an option to be recognised formally at Foundation or Practitioner level, at both Category A and B. Category A and B requirements to achieve Foundation are the same, with demonstration of 47 elements in total. However, individuals who wish to progress to a practitioner must demonstrate occupational competency against specific elements relevant to each role, to reach Practitioner[3] level at facilitator or fraud risk assessor level. The specific requirements for this are outlined in a separate document, entitled the GCFP FRA Category Matrix.

Competency Framework

Overleaf you will find a detailed competency framework outlining the knowledge skills and experience required for Fraud Risk Assessment. Within each of the five key components (see diagram below) you will find descriptors of the elements required at each level, from trainee to practitioner level.

[3] Category matrix for Facilitator and Fraud Risk Assessor available from GCFP@cabinetoffice.gov.uk on request

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
1.1 Counter Fraud Knowledge – Statutory Frameworks	Identify the statutory framework as being an important consideration in assessing fraud risks and their prioritisation.	Explain the various aspects of the statutory framework in the discussion of fraud risks to help bring these to life for those engaging in the process.	Demonstrate the application of the statutory framework in the discussion of fraud risks to help bring these to life for those engaging in the process.
1.2 Counter Fraud Knowledge – Professional Standards	Identify that there are several relevant professional standards, associated guidance materials, including the GCFP Code of Ethics and Civil Service Code, and regulatory requirements.	Explain the relevant professional standards, associated guidance materials, including the GCFP Code of Ethics and Civil Service Code, and regulatory requirements.	Demonstrate the application of the relevant professional standards, associated guidance materials, including the GCFP Code of Ethics and Civil Service Code, and regulatory requirements.
1.3 Counter Fraud Knowledge – Define Fraud	Identify the principle fraud offences within the Fraud Act 2006, Bribery Act 2010, Theft Acts 1968, Proceeds of Crime Act 2002 and other relevant legislation.	Explain the principle fraud offences within the Fraud Act 2006, Bribery Act 2010, Theft Acts 1968, Proceeds of Crime Act 2002 and other relevant legislation.	Demonstrate and apply knowledge of the principal fraud offences within the Fraud Act 2006, Bribery Act 2010, Theft Acts 1968, Proceeds of Crime Act 2002 and other relevant legislation.
1.4 Counter Fraud Knowledge – Motivation of Fraudsters	Identify the theories regarding the motivation of fraudsters and the elements of fraud such as the Fraud Triangle/Diamond, Rational Choice, Routine Activity Theory, Differential Association and the Fraud Scales Model.	Explain the theories regarding the motivation of fraudsters and the elements of fraud such as the Fraud Triangle/Diamond, Rational Choice, Routine Activity Theory, Differential Association and the Fraud Scales Model.	Demonstrate the application of the knowledge of theories regarding what motivates fraudsters and the elements of fraud such as the Fraud Triangle/Diamond, Rational Choice, Routine Activity Theory, Differential Association and the Fraud Scales Model.

1.5 **Counter Fraud Knowledge - People who commit fraud**	Identify that there are a variety of types of people who commit fraud from inside the organisation and/or externally with different motivators.	Explain who fraudsters are, the range of people who commit fraud from inside the organisation and/or externally and the different motivators, including organised crime and terrorist financing.	Demonstrate and apply knowledge of the range of people who commit fraud from inside the organisation and/or externally and motivators, including organised crime and terrorist financing, as well as the relationship between different fraudsters and organisations.
1.6 **Counter Fraud Knowledge – Victims of Fraud**	Identify that there are a range of people and organisations that may be victims of fraud and name a number of victim organisations and demographic groups.	Explain who the victim of fraud is in a range of scenarios (e.g. governmental organisation, financial services institute, other organisations, individuals) and explain the potential impacts on the victims e.g. - financial, physical, environmental, social, reputational and potential national security issues.	Demonstrate and apply knowledge of who the victim of fraud may be in a range of scenarios (e.g. governmental organisation, financial services institute, other organisations, and individual) and the impacts on the victims e.g. - financial, physical, environmental, social, reputational and potential national security issues.
1.7 **Counter Fraud Knowledge – Fraud Typologies**	Identify the various ways to categorise fraud into types e.g. by modus operandi (misappropriation of assets, financial statement fraud, and bribery) or by victim.	Explain the various fraud types that exist in the counter fraud world (by modus operandi and victim).	Demonstrate and apply knowledge of the various fraud types whilst categorising fraud risks and demonstrate an understanding of the increasing role of technology as an enabler in this process.
1.8 **Counter Fraud Knowledge – Fraud Controls and Prevention Tools**	Identify that there are a variety of different controls used to deter, prevent, detect and disrupt fraudsters and name a few key concepts e.g. segregation of duties, policy frameworks and freezing assets.	Explain how organisations, including your own, use key fraud controls and mitigations to prevent, detect, deter and disrupt fraud and that technology has a huge impact in this area.	Demonstrate and apply an understanding of a range of fraud controls and mitigations used to deter, prevent and detect fraud and how current trends and technology impact this area.

1.9 **Counter Fraud Knowledge – Fraud in Public Sector**	Identify a few types of fraud across different sectors and those within public sector including, procurement fraud, corruption, and grant fraud.	Explain the types of fraud seen across the public sector including, procurement fraud, corruption, and grant fraud.	Demonstrate and apply an understanding of the different types of fraud across the public sector including, procurement fraud, corruption, and grant fraud.
1.10 **Counter Fraud Knowledge – FRA v Threat Assessment**	Identify the similarities and differences between an FRA and a threat assessment; intelligence; detected fraud; and fraud risk management.	Explain the similarities and differences between an FRA and a threat assessment; intelligence; detected fraud; and fraud risk management.	Demonstrate an ability to manage the similarities and differences between an FRA and a threat assessment; intelligence; detected fraud; and fraud risk management.
1.11 **Counter Fraud Knowledge – Business Units**	Identify all the business units with responsibility for different aspects of fraud risk management.	Explain the role of the business units in managing fraud risk e.g., Finance, Legal, HR, Risk Management, Internal and External Audit (NAO) and other relevant business units.	Demonstrate and apply an understanding of how different organisations manage the risk of, and the response to, fraud. Also apply an understanding of the roles of various BUs in this process e.g. such as Finance, Legal, HR, Risk Management, Internal and External Audit (NAO) and other relevant business units.
1.12 **Counter Fraud Knowledge – Bribery and Corruption**	Identify that there are differences in how bribery and corruption are defined and how it is carried out.	Explain the modus operandi of bribery and corruption and provide examples for each, together with the potential impact i.e. financial, physical and reputational.	Demonstrate and apply knowledge of the various elements of bribery and corruption relating to the assessment of the fraud risks an organisation faces, together with the potential impact i.e. financial, physical and reputational.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)

2.1 **Business Knowledge & Skills – Research Methods**	Identify various research methods used to obtain information from an organisation and its key stakeholders in order to gain an understanding of the organisation, its strategy, structure, key objectives, delivery targets, key financial systems, policies and processes. This could include, but is not limited to, desk-based research, interviews, surveys, process walkthroughs, workshops, meetings, focus groups and document review.	Explain the various research methods used to obtain information from an organisation and its key stakeholders in order to gain an understanding of the organisation and the fraud risks it faces from all aspects of its operations including its strategy, structure, key objectives, delivery targets and mechanisms, key financial systems, policies and processes.	Demonstrate the effective use of the different qualitative and quantitative research methods used to obtain and analyse information from the organisation and its key stakeholders in order to gain an understanding of the organisation and the fraud risks it faces from all aspects of its operations, including its strategy, structure, key objectives, delivery targets and mechanisms.
2.2 **Business Knowledge & Skills - Qualitative and Quantitative Techniques**	Identify, in general terms, the employees, stakeholders, business processes and documentation that are essential to the development of a successful FRA.	Explain how and where in the business key information may be obtained from. These could include intelligence, investigation reports, risk registers, threat assessments, process manuals, policies, procedures and people (from board members through to administrators). Explain the qualitative and quantitative techniques that may be applied to this data to produce an effective FRA.	Demonstrate the ability to use the appropriate qualitative and quantitative techniques to effectively obtain and analyse all the information needed to identify, categorise and classify those fraud risks to which the organisation is, or may be vulnerable.
2.3 **Business Knowledge & Skills – Management Information**	Identify that management information (MI) has a key role	Explain the role of MI in supporting fraud risk management and how recent, current and future changes in	Demonstrate the use of quality MI to assess and report fraud risks to a range of stakeholders whilst successfully

	to play in the assessment and monitoring of fraud risks.	processes or systems within an organisation might impact on the quality of the MI.	influencing other parts of the organisation to provide more effective MI to identify and manage fraud risks.
2.4 **Business Knowledge & Skills - Review of Relevant Information**	Review and précis relevant information as directed by senior assessors / management to aid the FRA process.	Explain the need to review and précis relevant information to the person leading the assessment and management will aid the FRA process.	Demonstrate and systematically assimilate complex information to extract that which is relevant for the FRA process, including, but not limited to, governance arrangements (structures and accountabilities), deliverable products and services, available technologies, organisational culture, risk management processes and procedures, control frameworks and how responsibilities for receipts, payments, grants processes and services are delegated.
2.5 **Business Knowledge & Skills - Contractual Points**	Identify the parties to a contract and the key contractual points of relevance in relation to an FRA. These could include; accountability rests throughout the supply chain, quantity and quality of goods or services, the nature of contractual relationships and the capability of the team to manage the contract to hold the supplier to account with appropriate checks and balances.	Explain the importance of understanding how an organisation's services are delivered to identifying fraud risks. These could include; accountability rests throughout the supply chain, quantity and quality of goods or services, the nature of contractual relationships and the capability of the team to manage the contract to hold the supplier to account with appropriate checks and balances.	Demonstrate the application and understanding of how an organisation's services are delivered. These could include accountability rests throughout the supply chain, the nature of contractual relationships and the capability of the team managing the contract to hold the supplier to account/put in place appropriate checks and balances.

2.6 **Business Knowledge & Skills - Tactical and Strategic Intelligence**	Identify the difference between tactical and strategic intelligence in the fraud risk assessment process.	Explain the difference between tactical and strategic intelligence in the fraud risk assessment process.	Demonstrate the use of tactical and strategic intelligence in the fraud risk assessment process.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
3.1 **Communication and Facilitation Skills - Engagement**	Identify the importance of communicating confidently to all levels of an organisation the need for an FRA.	Explain the process of engaging with a range of people in an organisation when undertaking the FRA process.	Demonstrate effective engagement with people at all levels of an organisation to influence the decision makers when communicating fraud risk, especially when seeking a sponsor for each individual FRA.
3.2 **Communication and Facilitation Skills - Working with Stakeholders**	Identify the relevant stakeholders who should be able to contribute to the FRA and suggest methods to engage them i.e. meetings, interviews, walkthroughs and/or workshops.	Explain how to identify and engage relevant stakeholders in the fraud risk assessment process using a range of mechanisms including facilitation meetings, interviews, walkthroughs and / or workshops.	Demonstrate an ability to engage relevant stakeholders in the fraud risk assessment process using a range of mechanisms including facilitation of meetings, interviews, walkthroughs and / or workshops.
3.3 **Communication and Facilitation Skills - FRA Process**	Identify the importance of clearly communicating the fraud risk assessment process and products.	Explain how to guide stakeholders through; the identification of inherent and residual fraud risks, the identification and assessment of controls/mitigation, benefits to the business and the approach to challenge any assumptions regarding control effectiveness.	Demonstrate the ability to; guide stakeholders through the identification of inherent and residual fraud risks, the identification and assessment of controls/mitigation, benefits to the business and where appropriate challenge any assumptions regarding control effectiveness.

3.4 Communication and Facilitation Skills – Creating Risk Ownership	Identify the importance of having fraud risk owned by the business and how communication and facilitation can be a key factor in realising this objective.	Explain the importance of having fraud risk owned by the business as part of general risk management and how to communicate and facilitate this.	Demonstrate the ability to engage and communicate with key stakeholders to create ownership of fraud risks and fraud risk products. Ensure that fraud risk owners are at a senior level that is sufficient to make decisions and take action on fraud risk vulnerabilities.
3.5 Communication and Facilitation Skills - Feedback	Identify the importance of having effective feedback loops in the identification and assessment of fraud risks.	Explain how to create effective feedback loops with stakeholders, including suppliers and areas of the business and explain the use of feedback loops to amend or create an FRA.	Demonstrate the implementation of effective feedback loops with stakeholders, including suppliers and areas of the business, which will support the FRA remaining up to date and relevant to current business needs.
3.6 Communication and Facilitation Skills – Reporting Findings and Results	Identify the importance of having strong written and verbal communication skills in order to clearly articulate the fraud risk assessment process.	Explain the importance of strong written and verbal communication skills in order to be able to clearly articulate, via written or online products, the findings of any part of an FRA e.g. interview, document review, workshop discussion.	Demonstrate the ability to clearly articulate the findings of an FRA e.g. risk register, report, workshop discussion and present these to a range of audiences.
3.7 Communication and Facilitation Skills – Heat maps & other visual aids	Identify the role of heat maps and/or other visual aids in articulating to stakeholders the findings of the fraud risk assessment process.	Explain how to create and utilise heat maps and/or other visual aids in articulating to stakeholders the findings of the fraud risk assessment process.	Demonstrate the effective use of heat maps and/or other visual aids in articulating to stakeholders the findings of the fraud risk assessment process.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
4.1 **Fraud Risk Assessment- Planning**	Identify the importance of effective planning in fraud risk assessment activity and how it should take into consideration the organisation's maturity in fraud risk assessment.	Explain the principle steps involved in the effective planning of fraud risk assessment activity and how it should take into consideration the organisation's maturity in fraud risk assessment.	Develop a plan for an effective fraud risk assessment activity across one or more organisations taking into consideration the organisation's maturity in fraud risk assessment.
4.2 **Fraud Risk Assessment- Levels of Fraud Risk Assessment (Organisational (Enterprise), Thematic (Grouped) / & Full)**	Identify the differences between the four different levels of fraud risk assessment • Organisational (Enterprise) • Thematic (Grouped) • Initial Fraud Impact Assessment • Full Fraud Risk Assessment	Explain the differences between and appropriate use of the four different levels of fraud risk assessment • Organisational (Enterprise) • Thematic (Grouped) • Initial Fraud Impact Assessment • Full Fraud Risk Assessment	Demonstrate the appropriate use of fraud risk assessments at the four different levels: • Organisational (Enterprise) • Thematic (Grouped) • Initial Fraud Impact Assessment • Full Fraud Risk Assessment
4.3 **Fraud Risk Assessment- Translation and Integration of Fraud Risks**	Identify the requirement to translate and integrate fraud risks into the organisation's broader risk management and governance framework.	Explain the process for effectively translating and integration of fraud risks into the organisation's broader risk management and governance framework.	Demonstrate the process for effectively translating and integration of fraud risks into the organisation's broader risk management and governance framework.
4.4 **Fraud Risk Assessment- Fraud Risk Logs/Registers**	Identify the need for fraud risk logs/registers that categorise and prioritise fraud risks in a way that is clearly communicated and understood by the organisation.	Explain the process to create a fraud risk log/register that categorises and prioritises fraud risks in a way that is clearly communicated and understood by the organisation. Explain the function and structure of	Demonstrate the ability to create fraud risk logs/registers that categorises and prioritises fraud risks in a way that is clearly communicated and understood by the organisation.

		a fraud risk log/register and how it differs from a fraud risk assessment.	
4.5 Fraud Risk Assessment- Defining Risks	Identify the need for accurately describing and recording risks using the Action, Actor & Outcome Model or other similar structure in a fraud context.	Explain how to accurately describe and record risks using the Action, Actor & Outcome Model or other similar structure in a fraud context.	Demonstrate the accurate description and recording of risks using the Action, Actor & Outcome Model or other similar structure in a fraud context.
4.6 Fraud Risk Assessment- Use of causes, sub causes & consequences	Identify that there is a difference between causes, sub-causes & consequences when framing or describing risk.	Explain the differences between causes, sub causes & consequences when framing or describing risk and how they would be used.	Demonstrate the effective and appropriate use of causes, sub-causes & consequences when framing or describing risk.
4.7 Fraud Risk Assessment- Inherent Risk	Identify the strengths and weaknesses of assessment of inherent risk in a fraud context, including scoring methods assessing likelihood and impact, as well as considering duration.	Explain the strengths and weaknesses of assessment of inherent risk in a fraud context including scoring methods assessing likelihood and impact, as well as considering duration.	Demonstrate the ability to appropriately use inherent risk including scoring methods assessing likelihood and impact, as well as considering duration.
4.8 Fraud Risk Assessment- Identification of Controls	Recognise the need to identify and record relevant prevention and detection controls to mitigate risk, including evaluating their effectiveness and articulating their impact.	Explain how to identify and record controls relevant to each fraud risk; and to classify by type, specifically: directive, deterrent, preventative, detective, and corrective controls. Show understanding that only prevention and detection controls can mitigate risk by stopping or finding fraud and the need to evaluate their effectiveness and articulate their	Demonstrate the identification, correct classification and recording of relevant controls to mitigate each fraud risk and evaluating their effectiveness and articulating their impact by highlighting any limitations and weaknesses.

		impact in respect of the risk being assessed.	
4.9 Fraud Risk Assessment- Evaluation of effectiveness of Controls	Identify the need to effectively assess controls including their ability to prevent and detect instances of fraud.	Explain how to assess the effectiveness of controls including their ability to prevent and detect instances of fraud and their weaknesses.	Demonstrate the ability to evaluate the effectiveness of controls including their ability to prevent and detect instances of fraud and their weaknesses.
4.10 Fraud Risk Assessment- Assessment of Residual Risk	Identify the need to assess, describe and prioritise residual risk in a fraud context, including scoring methods assessing likelihood and impact, as well as considering duration.	Explain the assessment, description and prioritisation of residual risk in a fraud context, including scoring methods assessing likelihood and impact, as well as considering duration. Articulate the importance of this being a narrative assessment of how fraud could still happen despite controls in place, and how a fraudster could circumvent controls.	Demonstrate the assessment, description and prioritisation of residual risk in a fraud context, including scoring methods assessing likelihood and impact, as well as considering duration. Show how fraud could still happen despite controls in place, and how a fraudster could circumvent controls.
[New] Fraud Risk Assessment - Scoring residual risk and providing a rationale for the scores provided	Identify the need to score the residual risk identified in terms of likelihood and impact and to provide an explanation for each score given.	Explain how the scores for likelihood should differentiate between the likelihood of occurrence and frequency of the risk materialising; and the scores for Impact should differentiate between the impact of the possible duration of a fraud and its recurrence and its materiality. Explain how materiality should include all types of impact, not just financial. Explain the need to provide an explanation for each score given to	Demonstrate appropriate scoring for residual risk covering likelihood and impact which is consistent with the evidence gathered in the assessment. Likelihood should differentiate between the likelihood of occurrence and frequency of the risk materialising; and the scores for Impact should differentiate between the impact of the possible duration of a fraud and its recurrence and its materiality. Materiality must consider all types of impact, not just financial. Provide a

		provide visibility to the thinking of the assessor.	narrative rationale to explain the reason for each score given.
4.11 **Fraud Risk Assessment- Risk Owners**	Identify the need to identify appropriate fraud risk owners.	Explain the process required to identify appropriate fraud risk owners who have authority that is sufficient to make decisions and take action on residual risk.	Demonstrate the process required to identify appropriate fraud risk owners who have authority that is sufficient to make decisions and take action on residual risk..
4.12 **Fraud Risk Assessment- Risk Tolerance**	Identify the need to apply the concept of tolerance in a risk and fraud risk assessment context.	Explain the different ways of applying the concept of tolerance in a risk and fraud risk assessment context and its use to develop target risk.	Demonstrate the application of the concept of tolerance in a risk and fraud risk assessment context and its use to develop target risk.
[New] Fraud Risk Assessment - Initial Fraud Impact Assessments	Identify the need for an early, upfront, assessment of fraud risk and potential impacts for new spend activity.	Explain the process of building an Initial Fraud Impact Assessment, including the need to Identify types of fraud risk that might be encountered, the different types of impact, and specific factors that might increase the likelihood of fraud occurring.	Demonstrate the ability to build an Initial Fraud Impact Assessment for new spend activities. Identifying types of fraud risk that might be encountered, the different types of impact, and specific factors that might increase the likelihood of fraud occurring.
4.13 **Fraud Risk Assessment- Thematic (Grouped) Risk Assessment**	Identify the use of Thematic (Grouped) risk assessments.	Explain the process of building an Thematic (Grouped) level fraud risk assessment through full fraud risk assessments or in other situations where these are absent.	Demonstrate the ability to build an Thematic (Grouped) level fraud risk assessment through full fraud risk assessments or in other situations where these are absent.
4.14 **Fraud Risk Assessment- Organisational (Enterprise) Fraud Risk Assessment**	Identify the use of high-level fraud risk assessments.	Explain the process of building a high-level fraud risk assessment through full fraud risk assessment or in other situations where these are absent.	Demonstrate the ability to build an Organisational (Enterprise) fraud risk assessment through full fraud risk assessment or in other situations where these are absent.

Competency	Trainee (T)	Foundation (F)	Practitioner (P)
5.1 **Risk Management Skills – Risk Management Cycle**	Identify the various elements of the HMG Fraud Risk Management Cycle.	Explain the various elements of the HMG Fraud Risk Management Cycle in simple terms.	Demonstrate knowledge and application of the HMG Fraud Risk Management Cycle. Champion the HMG Fraud Risk Management Cycle to all stakeholders.
5.2 **Risk Management Skills – Risk Management Frameworks**	Identify a range of risk management frameworks.	Explain various risk management frameworks and how these may be applied within an organisation when undertaking an FRA.	Demonstrate an understanding of relevant risk management frameworks and processes and how these may be applied within an organisation when undertaking an FRA.
5.3 **Risk Management Skills - Risk Management**	Identify that risk management is the identification, prioritisation and monitoring of fraud risks (strategic, operational, and financial) that threaten an organisation's services and the security of its finances and assets.	Explain what risk management is e.g. the identification, prioritisation and monitoring of fraud risks (strategic, operational, and financial) that threaten an organisation's ability to deliver services and the security of its finances and assets.	Demonstrate the ability to secure senior management acceptance of the FRA and demonstrate the ability to manage conflict, when fraud risks arising from the FRA are challenged.
5.4 **Risk Management Skills - Risk Ownership**	Identify that risks are owned by the business and not the second and third lines of defence (risk management and internal audit).	Explain why and how risks are owned by the business and explain the role of the second and third lines of defence (risk management and internal audit).	Demonstrate the ability to work with second and third lines of defence (risk management and internal audit) to obtain a consensus on the ownership of each risk within the FRA process and support them to challenge the business when they are unclear on why they own fraud risk and how they manage them.

5.5 **Risk Management Skills - Controls**	Identify different types of control and the actions they have on fraud risk; specifically directive, deterrent, preventative, detective and corrective controls, and entity vs. process level control.	Explain the difference between directive, deterrent,preventative, detective and correctional controls, and entity vs. process level control.	Demonstrate the use of a range of controls to manage fraud (these can include, but are not limited to, preventative vs. detective controls, and entity-level vs. process or transactional controls.) Demonstrate that these controls are not necessarily mutually exclusive, have limitations and can fail and change over time.
5.6 **Risk Management Skills – Risk Management Options (4Ts)**	Identify how fraud risks can be managed by an organisation e.g. treated, tolerated, transferred or terminated.	Explain how fraud risks can be managed by an organisation e.g. treated, tolerated, transferred or terminated.	Demonstrate an ability to apply risk management options, e.g. treated, tolerated, transferred or terminated.
5.7 **Risk Management Skills – Fraud Risk Tolerance v Fraud Risk Appetite**	Identify there is a difference between risk appetite and risk tolerance.	Explain the difference between risk appetite and risk tolerance.	Demonstrate an ability to present to various audiences the difference between risk appetite and risk tolerance, as well as contributing to the development of your organisation's risk appetite.
5.8 **Risk Management Skills - Review and Monitoring**	Identify the importance of on-going review and monitoring of evolving fraud risk within the fraud risk assessment process, taking into account new and emerging risks, as well as changes in the control environment.	Explain the process of on-going reviewing and monitoring of changes in fraud risks as part of the fraud risk assessment process, taking into account new and emerging risks, as well as changes in the control environment.	Demonstrate on-going review and monitor changes in fraud risks as part of the fraud risk assessment process, taking into account new and emerging risks, as well as changes in the control environment.

Guidance for Professionals

C. Guidance on Processes
Fraud Risk Assessment

C1. Introduction

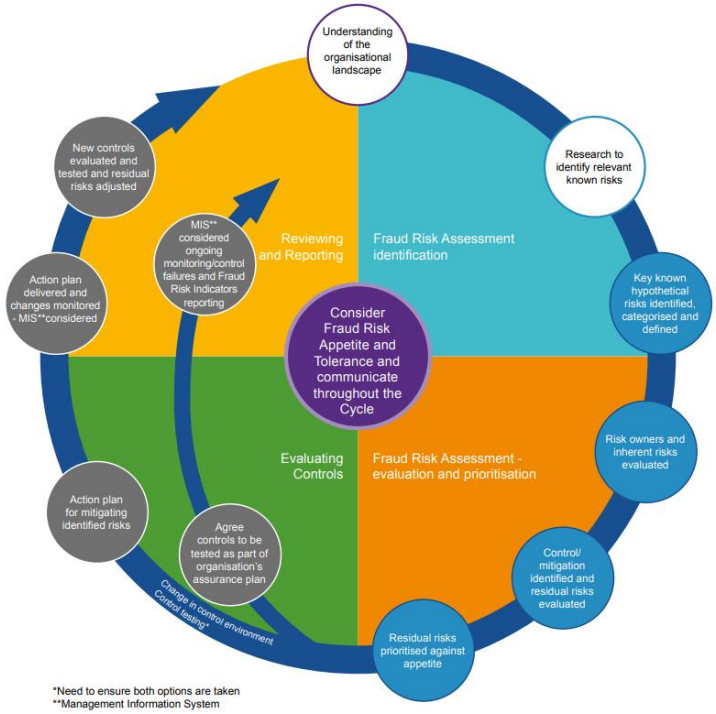
This document sets out guidance for the process of completing an effective Fraud Risk Assessment (FRA). A fraud risk assessor (the Assessor) must be able to identify fraud risks, evaluate controls and build a comprehensive picture of fraud risks that an organisation may be faced with. Set out below is the FRA process, designed as part of the HMG Counter Fraud Risk Management Cycle, included in the introduction to these standards.

The FRA process focuses exclusively on the assessment part of the Fraud Risk Management Cycle[4]. The Evaluating Controls and Reviewing and Reporting parts of the Fraud Risk Management Cycle sit outside the scope of this document. However, it is helpful to introduce the cycle as part of the introduction to FRA and how this fits together.

Fraud Risk Management Cycle

Below is the Fraud Management Cycle, part of which includes the Fraud Risk Assessment process. The cycle offers an illustration of the end-to-end process, from using research to identify known risks, completing a fraud risk assessment, and using this to actually manage and mitigate those risks by informing controls. There is a continual need for reporting and then reviewing and re-doing aspects of the cycle. Key to delivering an effective Fraud Risk Assessment, as part of the Fraud Management process, is a thorough understanding of the organisational landscape. The Fraud Risk Assessment part of this cycle is explored in section C.

[4] See Introduction to the Standards



The responsibility for managing fraud risks effectively rests with the organisation's accounting officer supported by the Board-level individual accountable for fraud and error risk, supported by the counter fraud functional lead as set out in the HMG Functional Standards. There is also guidance in the form of the Leadership, Management and Strategy standards within the Profession for functional leads.

It is accepted that in some organisations the functional lead can also be the person undertaking the FRA and so that person will need to prove capability in relation to both the FRA and also the Leadership, Management & Strategy Standards.

A one size-fits all approach to managing risks is unlikely to work across organisations of different sizes, structures and needs. A broad and high-level process will, however, help organisations ensure their arrangements for managing fraud risks are structured and comprehensive whilst building on what already exists and adding new concepts as necessary.

With this in mind, this document aims to complement the risk management principles and concepts that have come before, specifically:

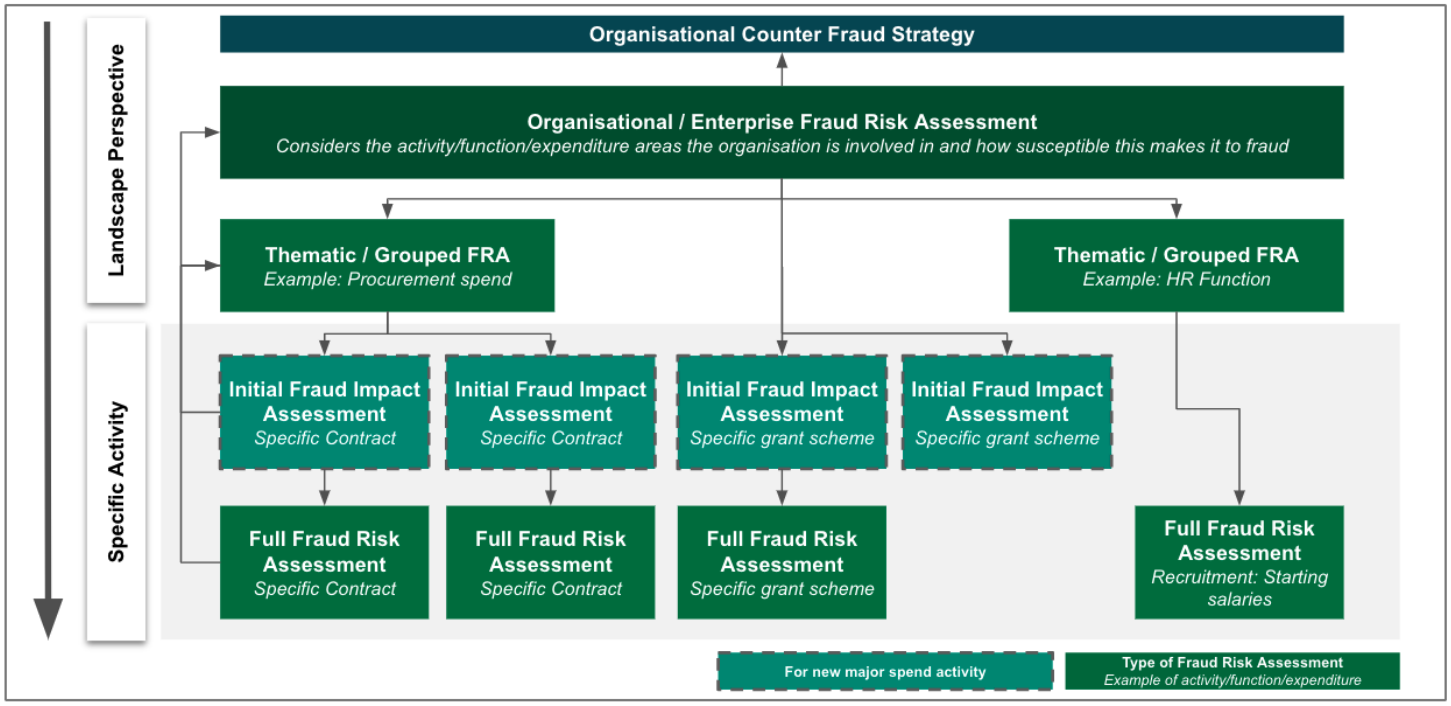
- HM Treasury's Orange Book;
- HM Treasury's Managing Public Money;
- HM Treasury's Green Book;
- NAO's Managing Risks in Government;
- the UK Corporate Governance Code; and
- FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting.

The rest of this document provides a simple yet structured process to implement the new concepts and principles with a pragmatic approach. This is further supported by the FRA Product guidance in Section D.

The four levels of Fraud Risk Assessment

There are four levels of Fraud Risk Assessment (FRA), Organisational (Enterprise), Thematic (Grouped), Initial Fraud Impact Assessment (IFIA) and Full (see D.6 for further explanation of the four levels and their purpose).

The FRA process described below can apply to various types of fraud risk assessment; Organisational (Enterprise), Thematic (Grouped), IFIA and Full FRA as illustrated below:



Departments should ensure that they have an Organisational (Enterprise) level FRA supported as appropriate by Thematic (Grouped) FRAs, IFIAs and Full FRAs.

The Assessor should have a structured approach to FRA and separate FRA into steps described below as far as possible. The Organisational (Enterprise) level gives an overview of the main fraud risks the organisation faces. The Thematic (Grouped) level focuses on areas of spend or various programmes across the organisation, depending on its operations and structure. An IFIA provides an initial upfront focus of the main fraud impacts and challenges facing a new spend activity. A Full FRA would focus on, and provide a detailed analysis of, specific fraud risks within an individual spend activity, business unit or programme.

C2. Fraud Risk Assessment Process

Steps 1&2 apply for all 4 levels of the Fraud Risk Assessment process, steps 3-4 apply for the full risk assessment and initial fraud impact assessment; whereas steps 5-6 apply to the full risk assessment only.

Depending on the complexity, breadth and granularity of the FRA, it can be covered in one workshop or a series of workshops/activities but Steps 1 and 2 (understanding of the organisational landscape and research) must be undertaken beforehand by the Assessor.

Step 1: Understanding of the organisational landscape

1. Assessors must gain an overview of an organisation's strategy, structure, key target operating models, priorities, policies[5] and guidelines before undertaking an FRA. This should result in all the organisation's activities being mapped and assessed for potential vulnerabilities to fraud and error.

2. Assessors should use their understanding of the organisation's structure to create a high level, methodical plan (the Plan) for their FRA(s)[6]. This can differ depending on the level of the FRA; Organisational (Enterprise) level, Thematic (Grouped), IFIA or full, see diagram above. At a minimum the Assessor will need to involve each operational business unit.

3. Assessors should understand the organisational structure and policies, including the Enterprise Risk Management Framework, and engage with the risk management function to support the FRA process. Where the organisation is undertaking a full FRA, Assessors should seek an operational business unit sponsor for each FRA undertaken in order to aid the process and give it traction. They should ask the sponsor to nominate a single point of contact from the business unit to make things easier logistically.

[5] Information includes but is not limited to: overarching departmental objectives, strategy and policies (at a high level), budget and key areas of spend/major projects planned or under way, history of current and past fraudulent incidents, counter fraud capacity/capability, role of Internal Audit and IA reports into areas subject to a FRA, risk management processes/procedure, supply-chain /relationship with third parties, information on structure and human capital (headcount, use of contractors, change programmes recent and planned).

[6] A description of an FRA plan can be found in the GCF Fraud Risk Assessment Product Standards.

Step 2: Research to identify relevant known risks and any factors likely to drive the likelihood of the risk occurring

4. Assessors should ensure that risks picked up via fraud investigations or mechanisms for raising concerns are considered in the FRA, as well as future risks from horizon scanning, as the FRA progresses.

5. Assessors should ensure that any relevant internal audit reports are reviewed in relation to the assessment of the control framework in the area being assessed.

6. Assessors must conduct research into the specifics of the business area(s) their FRA will focus on and collate information from internal and external sources. For instance, if the area under assessment is procurement, the Assessor should extend their research beyond their own organisation and consider other organisations' procurements, especially the ones that are buying similar services or similar approaches for procurement and contract management.

7. Assessors should identify specific factors that might make fraud or error more likely, such as the characteristics of the customer or supplier base, or the complexity of processes and transactions.

8. Assessors should ensure that there is a process in place whereby strategic and tactical intelligence feed into the fraud risk assessment by informing it of any new risks which should be assessed and/or revised in light of new information. If the organisation or part of the organisation has undertaken any fraud threat assessments, assessors should take their output into account to inform the FRA.

Step 3: Key known and hypothetical risks identified, categorised and defined

9. Assessors must identify and define the key inherent fraud risks faced by the organisation, using a variety of techniques, such as workshops, walkthroughs, structured questionnaires (to ensure consistency of response types) and structured interviews to assess the business environment. They should carry out appropriate qualitative and quantitative research (management information, detected fraud, intelligence) and collate information from relevant stakeholders.

10. Assessors must identify key risks and categorise them in a way that subdivides the fraud risk assessment into a format that is achievable, able to be effectively communicated and understandable by the organisation.

11. Assessors must consider the size and nature of transactions to ensure that impact is fully quantified e.g. multiple frauds in a category of high volume/low value transactions can still have a significant impact.

Step 4: Risk owner identified and inherent risks[7] evaluated

11. The assessment of inherent risk must be undertaken within an Initial Fraud Impact Assessment but is an optional step within the full fraud risk assessment. If included, assessors should engage with stakeholders who have an in-depth knowledge of the subject of the assessment, to help them assess the inherent risk of the identified risk.

12. Assessors must ensure that for each risk there is an owner identified with sufficient seniority to be able to introduce or re-design controls to effectively mitigate the risk within accepted levels of tolerance, taking into account the cost of mitigation versus the materiality of the risk exposure.

13. If this step is included, assessors should guide stakeholders through the evaluation of inherent risks using qualitative or quantitative assessments i.e. scales of a numeric or descriptive nature to determine probability and impact. These should be in line with the FRA Product Standards.

14. Assessors should look into different approaches to agreeing scores and consider which one is the most appropriate.

15. Assessors should design the key criteria used to establish risk impact in the FRA; the counter fraud functional lead should work with the organisation to agree them.

Step 5: Control/Mitigation identified and residual risk evaluated

16. Following the identification of the risks, Assessors must support stakeholders in the identification and assessment of current mitigation and controls. There are a

[7] also defined as gross risk, is the risk to an organisation assuming there are no controls in place

number of mechanisms that can be utilised here; workshops, walkthroughs, interviews and desk-based reviews of process documentation[8].

17. Once the control/mitigation has been identified, the Assessor must support stakeholders with the assessment of the difference made by controls/mitigation against the inherent risks, whilst highlighting any limitations or weaknesses.

18. Assessors should encourage stakeholders to actively partake in scenario hypothesis to anticipate the behaviour of a potential fraudster, by applying a sceptical mind-set to mitigation and controls and by asking questions such as, what are the limitations of the controls that could allow fraud to occur and how could a fraudster override or circumvent controls?[9] It is essential that the assessment of residual risk includes a clear description of how fraud could still occur despite the controls in place – and not just labels of 'low risk' or 'medium risk' or an associated numeric score.

19. Assessors should look into different approaches to agreeing scores for residual risk and consider which one is the most appropriate.

20. Assessors should support the communication of fraud risk throughout the organisation from top to bottom and bottom to top, allowing conscious decision-making in relation to residual risks.

Step 6: Residual risks prioritised against appetite

21. Assessors must ensure that residual risk is clearly defined, scored and prioritised against the organisation's fraud risk appetite to indicate which risks the organisation will take action on.

22. There should be a process for risks classified as acceptable to be periodically monitored and reassessed to understand if the risks have changed and for out of appetite risks to be considered seriously by senior management. Management should also ensure there is effective fraud measurement activity, including fraud loss measurement focused on key residual fraud risks, to provide assurance as to whether actual fraud and error losses remain within stated levels of tolerance.

[8] Tools and techniques are described in the FRA Product Standards.

[9] T.Jeffrey Wilks and M.F. Zimbelman 'Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud' Accounting Horizons, Volume 18, No.3 (September 2004)

D. Guidance for Professionals - Products

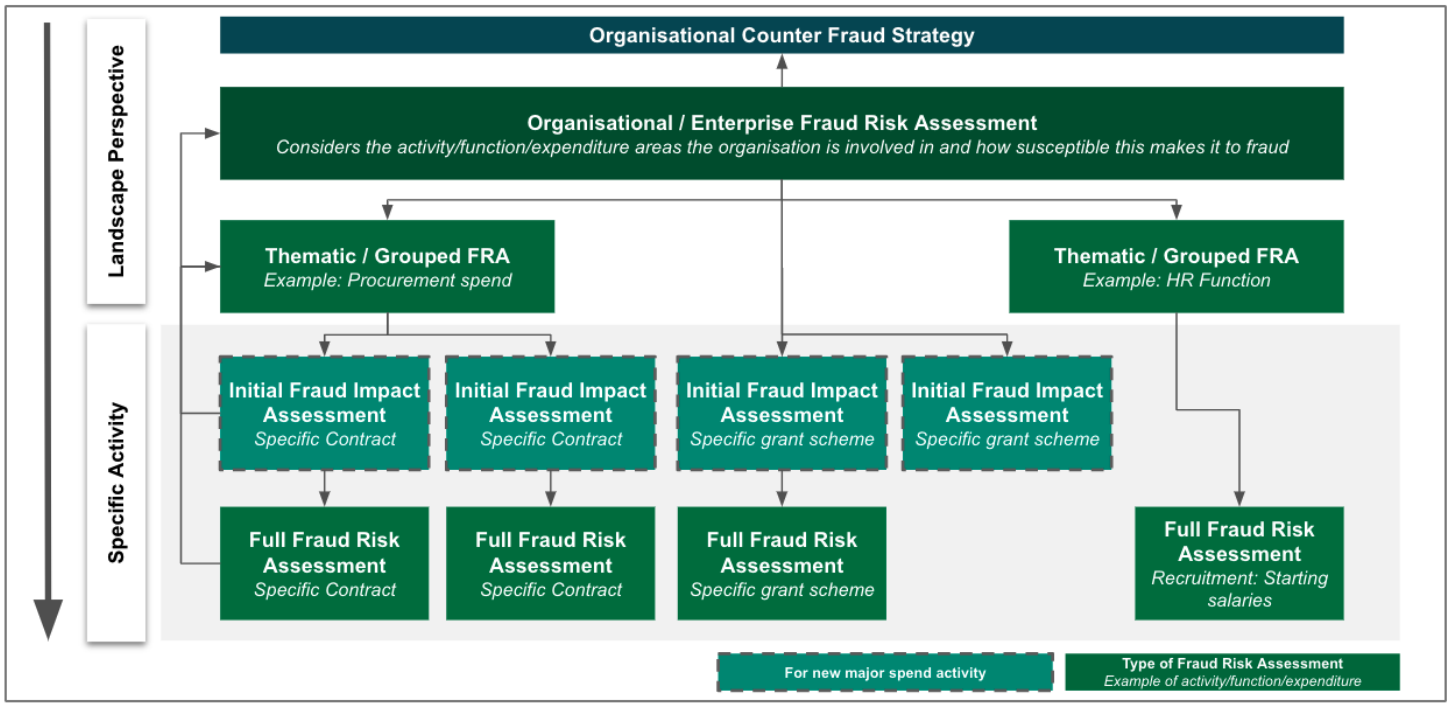
D1. Introduction

All U.K government and Public Sector organisations should have Fraud Risk Assessments (FRA) to show where the organisation is susceptible and vulnerable to fraud.

To be most effective, the fraud risk assessment process needs to be undertaken at four different levels in line with the Government Counter Fraud Functional Standard[10] [*provide footnote reference*].

There are four types or levels within the Fraud Risk Assessment (FRA) process which are explained in detail at section D6:

- Organisational (Enterprise) Fraud Risk Assessment
- Thematic (Grouped) Fraud Risk Assessments
- Initial Fraud Impact Assessments (IFIAs)
- Full Fraud Risk Assessments



These levels of FRA go from the general, providing a landscape view of areas susceptible to fraud within the organisation, to the specific, identifying particular instances of residual fraud risk where the organisation is most vulnerable to fraud happening. All levels of FRA are important but it is only through undertaking full FRAs that the organisation is able to identify and understand the particular instances and circumstances where it may be attacked by fraudsters.

Although the levels of FRA go from the general, to understand areas susceptible to fraud, to the detail of where specific vulnerabilities exist it is important that feedback

[10] See GCFF Functional Standards SO13

loops exist from the full FRA to the higher level assessments. This should map the vulnerabilities representing the highest risk back to the spend activities mapped within the Organisational and Thematic level FRAs. This allows senior managers and the Board to understand the top fraud risks faced by the organisation and also to see not only the activities most susceptible to fraud but the detail of the vulnerabilities that could allow instances of fraud to occur.

This document sets out the expected minimum standards to be applied to each type and tools and techniques to be utilised before, during and after the output of a FRA. For simplicity, we have referred to these tools and techniques as **products**. The final product of the FRA process must include a fully populated Fraud Risk Register (the Register) which identifies and highlights the specific areas where the organisation is vulnerable to fraud. The Register should then be integrated into the organisational and business unit risk registers, as deemed appropriate by the key stakeholders, e.g. the board and business unit's managers.

The products appear in the order in which an organisation or individual fraud risk assessor (the Assessor) may use them in the FRA process, as set out in the Fraud Risk Management Cycle. It is helpful to read this document in conjunction with the following standards and guidance:

- **FRA Process Guidance** describes the process to complete an effective FRA. A fraud risk assessor (the Assessor) must be able to identify fraud risks, assess controls and mitigations and build a comprehensive picture of fraud risks that an organisation may be faced with. Set out in these standards is the FRA process as designed as part of the HMG Counter Fraud Risk Management Cycle[11].
- **FRA Standards and Competencies** are designed to present a consistent cross-government skill level for delivering FRA, raise the quality of organisations' counter fraud work and the skills of their individuals.[12]
- **HMG Functional Standards** and **Leadership, Management and Strategy standards and guidance** cover the process of how to manage an effective counter fraud function. Functional leads must be able to understand and agree risk appetite/s and set an effective strategy and response in order to minimise the fraud risks and threats the organisation faces.

Threat[13]Assessment vs Risk Assessment

A threat assessment product differs from a risk assessment product in that the former should outline what is known, the likely threats and current response from the organisation. A threat assessment product should use the intelligence available to inform the organisation's risk function, as well as guiding its overall counter fraud priorities.

[11] See paragraphs 2,8,10,13 for references to Products

[12] See paragraphs 20 and 26-32 for reference to Products

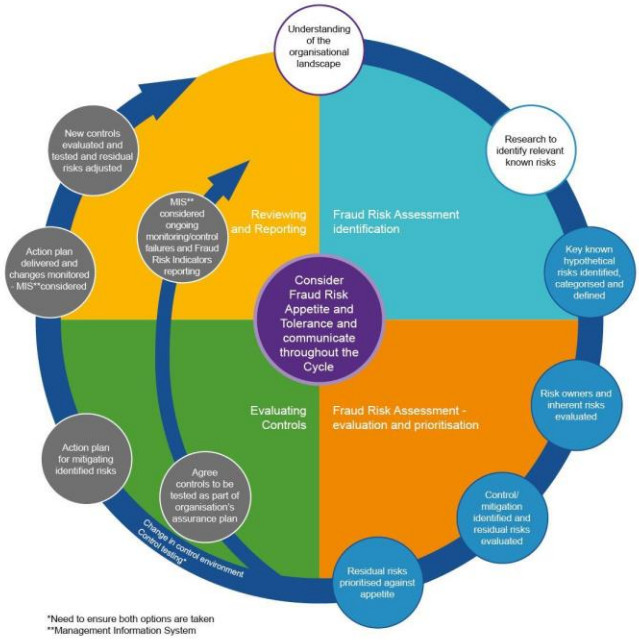
[13] See definition of Threat in the Introduction to the FRA Standards

Whereas an FRA assesses the likelihood and impact of an individual risk coming to pass, a threat assessment assesses the capability and intent of the potential threats.

A threat assessment product should consider the following:

- information and intelligence known, including data cost to the organisation;
- the type of fraud threat, whether it is capable of affecting the organisation, its objectives and the time needed to crystallise;
- the source of the threat;
- the potential impact and consequences of the threat, including which areas of the organisation it would affect; and
- a recommended response.

The Fraud Risk Management Cycle: The diagram below[14] depicts the FRM cycle, containing the FRA process. The remainder of this document focuses on the products and tools required in the FRA process shown in the blue circles.



D2. Planning

Fraud Risk Assessment Plan

There are two stages of planning. These are: general planning which includes annual planning of fraud risk assessment activities and individual assignment planning which includes individual fraud risk assessments.

A FRA Plan:

1. Will outline:

[14] Diagram 1: The Fraud Risk Management Cycle – extracted from the Leadership, Management and Strategy Standard (Crown Copyright 2016).

- the overall approach to FRA and which areas of the organisation will have an FRA applied to them;
- the extent and coverage of the four levels of fraud risk assessment[15];
- what the scope of each planned FRA will be;
- any high profile/notable fraud risks that will be reviewed;
- the rationale for the chosen areas;
- a clear, realistic and measurable timetable for the delivery of each FRA;
- the key stakeholders and overall sponsor for each FRA; and
- date for review (this is recommended to be yearly).

2. Should be linked to the Annual Counter Fraud Action Plan.[16]

3. Will vary depending on the organisation's maturity in FRA:
   - where no FRA exists, it should be focused on the areas of perceived highest risk from an initial view and structured by business units;
   - where an organisation is more mature i.e. has a variety of FRAs across multiple areas (potentially combined with other organisations) the structure of the FRA plan can be organised differently; for instance, by potential threats or processes that go across multiple business units e.g. internal fraud, grants.

4. Must have a structure that is meaningful to, and understood by, the organisation and is easy to communicate. It should outline accountability and responsibility for areas of fraud risk and individual fraud risks within these.

5. May include the review of areas of the business, or the review of the whole of the business, against a specific strategically important risk and often both of these. For instance, in one year an organisation may review the fraud risk of a specific delivery arm, whilst also assessing the whole of the organisation's resilience to a specific risk e.g. Mandate Fraud.

6. May include FRAs at multiple levels: Organisational (Enterprise), Thematic (Grouped), Initial Fraud Impact and Full.[17] For instance, in one part of the FRA plan a Full assessment will identify and assess specific fraud risk exposures (residual risk) where the organisation is vulnerable to fraud occurring. For example, within an individual procurement contract. However, the Thematic (Grouped) level FRA would look at the relative susceptibility to fraud across the organisation's procurement contract portfolio. The Organisational (Enterprise) level and Thematic (Grouped) level FRAs should be used to identify specific activities where a Full FRA would be the most beneficial to the organisation in identifying and understanding its key fraud vulnerabilities.

[15] Organisational (Enterprise), Thematic (Grouped), Initial Fraud Impact, Full FRA. See 4 level model for fraud risk assessment.

[16] See LMS Standards

[17] See the 4 level-model for fraud risk assessment in this FRA Standard

7. Governance for and oversight of the delivery of the Fraud Risk Assessment(s) should be determined.

8. Consideration should be given to emerging risks or trends. New spend activity which is novel is likely to carry a higher risk and be targeted by criminals because the activity is likely to have less maturity in addressing fraudulent activity.

9. Must be agreed with and communicated to the key stakeholders in the organisation who will be impacted by the FRA plan, and agreed by the counter fraud functional lead[18] and the Individual at Board Level accountable for fraud and error reduction.

10. This plan can be tailored to fit the organisation, based on the requirements of the Board, with advice from the audit and risk committee.

D3. Research

Prior to conducting any interviews, dependent on their experience of the organisation, the fraud risk assessor should consider what desk-based research they may need to conduct to cover some of the topics below at D4.

This may include, but not exclusively, understanding the activities and processes within scope of the FRA being undertaken; the governance and accountability structures; the types of generic fraud risk that are common to that area; types of fraud that have occurred in similar processes and business areas elsewhere; and the ways instances of fraud could have different impacts on the business area.

D4. Interviews

1. Any interviews of senior stakeholders should be consistent and ideally be in the form of a structured interview with a topic guide. Whilst interviews should ideally be structured, room should also be left for discussion and exploration of topics.

2. It should be made clear that all information will be kept in confidence and that quotes may be included but no names will be apportioned, except in relation to risk owners, as agreed with that person.

3. All interview responses should be collated in a systematic and logical format to enable qualitative analysis of risks raised.

4. As a minimum, consideration must be given to:
   - role/responsibilities/experience/time in role/financial accountabilities;
   - departmental structure and accountabilities;
   - budget;

[18] Or person with responsibility for counter fraud in the organisation.

- delegations of authority;
- complex processes or systems;
- key financial processes and systems;
- opinion on opportunities for fraud;
- opinion on internal pressures in the team including KPIs;
- previous incidents, including suspected and actual frauds;
- culture around mistakes;
- levels of challenge at peer level and within the team;
- awareness of departmental anti-fraud measures, including mechanisms for raising concerns i.e. whistleblowing;
- concerns they may have and anything else they want to raise;
- change in leadership/staff structure/mass redundancies/high staff turnover;
- other sources of assurance e.g. internal audit reviews/third party assurance; and
- performance of the team/business unit/organisation

D5. Pre-Workshop Packs / Questionnaire or Survey

Workshop participants may engage more effectively with the process if they receive a pre-workshop pack and have the opportunity to think about fraud risks in advance. The workshop pack should help the Assessor focus the attention of the participants and help them understand how a risk is defined ahead of the workshop, and as a result, ascertain the most common risks.

Questionnaires or surveys are a good starting point but ideally, they should not be conducted in isolation without a subsequent workshop.

Pre-Workshop Pack:

1. Any pre-workshop pack should clearly state the aims and objectives of the FRA, the methodology to be used by the Assessor and the expected outputs.

2. It should not be cumbersome, 5 to 10 minutes to complete/review, and take into account the audience's understanding of fraud risk.

3. It should set out the logistics of the workshop i.e. date, time, participants etc.

4. It should include a definition of fraud and examples of fraud risks.

5. It may include a non-disclosure agreement to be signed by participants, depending on the sensitivity of the discussions.

6. It should contain a one-page description of the FRA team and their contact details.

Questionnaires:

7. Questionnaires should be pre-populated with three to five risks that are relevant to the business unit, process or project as identified at the interview / research stage.

8. Questionnaires should remain confidential and no person should be attributed to raising a risk in the workshop or any subsequent reports.

9. Completed questionnaires should be communicated and stored using secure electronic tools.

10. Fraud risks should be clearly articulated and include a clear description of the inherent risk, with a distinction between its cause, sub-cause, event and consequence e.g. 'there is a risk that [include event that could happen] because [why and how it could happen] leading to [the consequence or outcome]'. A simple example would be that there is a risk that confidential information may be handed out to a third party because of social engineering of staff, leading to financial loss.

11. Questionnaires should be distributed, completed and analysed in good time as per the FRA Plan.

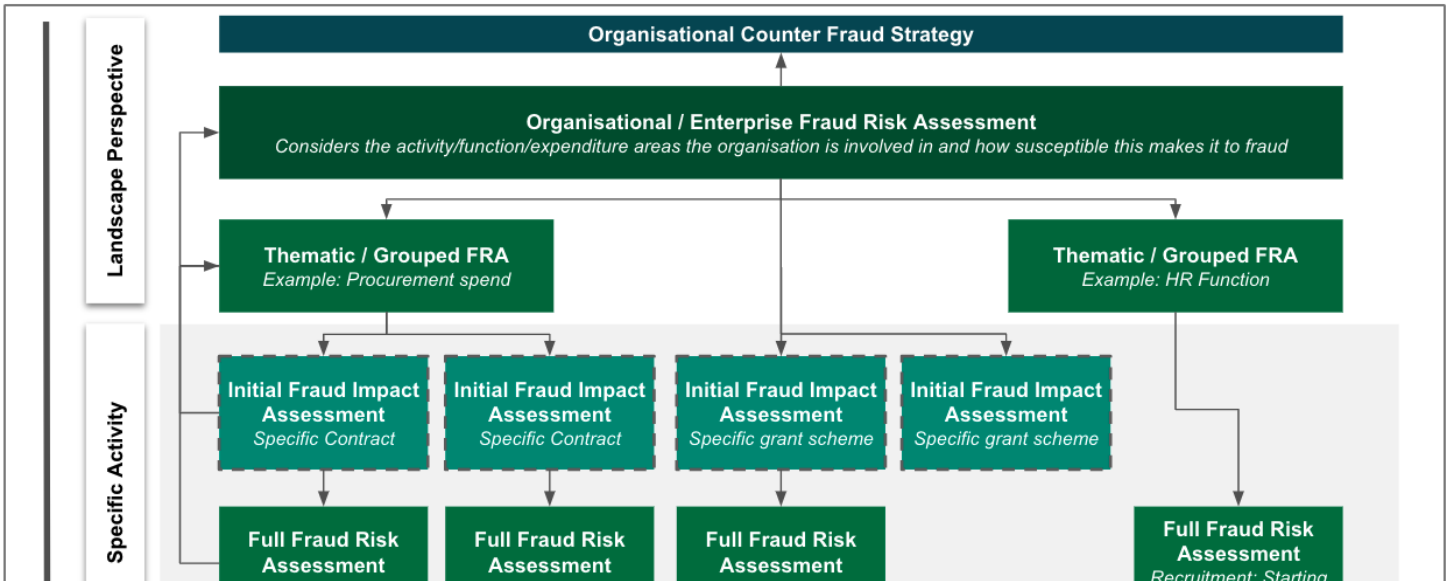
12. Questionnaire responses should be quantitatively analysed in any final report e.g. 'four out of nine questionnaires identified the risk that ambulance trusts have Key Performance Indicators on call response times that could cause department managers to fraudulently misrepresent the true response time, leading to inaccurate information and ultimately a skewed resourcing model'.

D6. Assessments

D6.1 General

1. There are four levels of Fraud Risk Assessment (FRA):
    - Organisational (Enterprise) Fraud Risk Assessment
    - Thematic (Grouped) Fraud Risk Assessments
    - Initial Fraud Impact Assessments (IFIAs)
    - Full Fraud Risk Assessments

The diagram below shows the scope and relationship of each level:



2. The Fraud Risk Assessment environment should operate as a two-way process between different levels of assessment. The Organisational (Enterprise) level and Thematic (Grouped) level should work as a two way process and inform each other. The Organisational (Enterprise) level and the Thematic (Grouped) level should also inform, and be informed by, the Initial Fraud Impact Assessments and Full FRAs.

3. The Organisational (Enterprise) level looks at the organisation as a whole and how susceptible to fraud it might be. This can be used to communicate fraud risk at a board level.

4. The Thematic (Grouped) FRA looks at the overall inherent risk faced within one of the specific activity/function/expenditure areas within or across organisations.

5. The Initial Fraud Impact Assessment looks at some of the inherent fraud risks and potential fraud impacts within specific processes and programmes.

6. The Full FRA is a thorough assessment of the risks within specific processes and programmes, how the controls in place reduce them and what the remaining vulnerabilities, or fraud risk exposures, are.

7. Fraud risk assessment is significantly underestimated, if considered at all. Fraud can be a hidden crime and can impact an organisation without it being apparent. Therefore, unlike some risks, fraud can be perpetrated without being detected or recognised as an issue.

8. Fraud Risk Assessment, at all levels, must be a living, iterative document. It must be clearly date stamped to show when it was last updated.

9. Fraud Risk Assessment, at all levels, should represent the cumulative knowledge that has been built up within the business.

10. A decision should be taken by the business on how openly shared and communicated the Fraud Risk Assessments and Initial Fraud Impact Assessments will be. The IFIAs and FRAs usually contain sensitive information as it details how a business can be defrauded. All FRAs should be open to be shared with other public sector fraud risk assessors and the centre of the counter fraud function in the Cabinet Office.

11. The author and owner/sponsor of all FRAs must be clearly recorded.

12. Consideration should be given to monitoring, assurance and quality review of all FRAs.

13. All FRAs should be signed off by the identified business owner. However, the fraud risk assessor should record any instances where they are required to make changes that are not in line with and cut across their professional opinion and judgement.

14. FRA activity should be integrated with the overall risk management process in the organisation. However, this does not necessarily mean that the scoring of risks should be aligned if the organisation's method for scoring risk is not meaningful in a fraud context.

15. Crossovers to other risk assessments should be acknowledged and discussed with other risk assessment owners and departments. For instance, a fraud risk assessment can have crossover with the following:
    - a security risk assessment, including information Technology security, Physical security and Data / Information security;
    - a health and safety risk assessment;
    - a bribery and corruption risk assessment; and
    - risk assessments for operational business units.

16. Fraud risk assessments should feed into other counter fraud activities and disciplines. The existence of key residual fraud risks might lead to further analysis of the potential fraud problem to inform fraud loss measurement exercises (as outlined in the Fraud Measurement Standard) or Data Pilots (outlined in the Data and Analytics Standard). These will quantify the extent to which the identified vulnerability has resulted in losses. This in turn can inform decisions on whether additional prevention or detection controls are appropriate.

D6.2 Organisational (Enterprise) level Fraud Risk Assessment

1. An Organisational (Enterprise) level FRA looks at the organisation as a whole and how susceptible to fraud it may be across all its business activities.

2. An Organisational (Enterprise) level FRA considers the activity / function / expenditure areas the organisation is involved in, its environment, and how susceptible this makes it to fraud. The areas identified should inform the Thematic (Grouped) level FRA and/or areas where a full FRA would be most beneficial. The Organisational (Enterprise)-level FRA is the most general level of fraud risk assessment.

3. When completing an Organisational (Enterprise) level FRA, organisations must be aware of the delivery chain through which they implement their services and policies and spend or collect their money. It should be acknowledged that the reputation risk from fraud cannot be avoided through outsourcing to a third-party organisation. For the financial risk to be transferred, for instance through

outsourcing, an effective fraud detection regime needs to be in place within the outsource provider.

4. An Organisational (Enterprise) level FRA must be time-limited. It should be updated at least annually, and take into account recent Initial Fraud Impact Assessments. For larger organisations, this should be more frequent. It should be shared with the Audit and Risk Committee and reviewed by them at least annually.

Mature Fraud Risk Assessment Environment

5. When effective Fraud Risk Assessment is established in an organisation, the Organisational (Enterprise) level Fraud Risk Assessment can be informed by the Thematic (Grouped) FRAs, which are ideally fed by the Initial Fraud Impact Assessments and Full Fraud Risk Assessments.

6. A mature Organisational (Enterprise) level FRA (built from Thematic (Grouped), IFIAs and Full FRAs) must be able to be reviewed at board level and should cover:
    - what the overall level of risk to the organisation is from fraud;
    - if it is possible to put an estimated financial value on the potential loss, either through measurement exercises, comparators or through other justifiable estimation methods;
    - what specific key risks/combinations of risks are to the organisation; and
    - what drivers around the organisation and its environment are currently affecting, or might affect in the future, either positively or negatively, the organisation's fraud risk. This might include how the motivators or enablers for risk are changing, or it might include any emerging risks that could affect the organisation in the future.

7. Organisational (Enterprise) Fraud Risk Assessments built from Thematic (Grouped) FRAs, IFIAs and Full FRAs may also include:
    - key identified threats;
    - a summary of key identified control weaknesses in the area;
    - a summary of the identified potential fraud impacts; and
    - any areas of uncertainty where information was not available at the time of assessment.

8. It is unlikely that an organisation would ever get to the extent that it has coverage of all of its spending and income areas in its Fraud Risk Assessment Environment. A mature environment has fraud risk assessments at all levels that drive the prioritisation of effort to both understand risk, and take action to reduce risk and loss.

Developing Fraud Risk Assessment Environment

9. Where a mature fraud risk assessment environment is not in place, it is possible to build an Enterprise / Organisational level FRA to give an organisation an indication of the overall importance of fraud risk whilst it develops its wider fraud risk assessment environment. This will deal with the strategic risk and risk drivers to the organisation, as opposed to the specific risks. It should be recognised that

this product is much less reliable than a risk assessment built up from the Thematic (Grouped)-level FRAs, IFIAs and Full FRAs.

10. An Organisational (Enterprise) level FRA, which is not built from the other assessments, should include coverage of:
    - what the organisation's key business purpose is;
    - how much money the organisation spends or is responsible for the spending of. This should also be compared to the proportion it spends on its own administration;
    - what the organisation spends its money on;
    - what the drivers of fraud risk are in the current context
    - where the organisation receives money from;
    - how many physical cash transactions are made;
    - how externally facing an organisation is i.e. what the general awareness of the existence of that organisation would be;
    - who the organisation does business with e.g. third-party suppliers, what their normal attributes are, and the variety and complexity of these interactions;
    - is the organisation operating overseas, if so include fraud indices of the relevant country/countries;
    - who the organisation's customers are and what their normal attributes are[19];
    - who the organisation's suppliers, financiers, regulators and other third parties are and the variety and complexity of their interactions;
    - how disparate the organisation is and how dependent the organisation is on delivery through others;
    - how specific the organisation's legislation/rules are on what it can spend money on and how;
    - how specific the organisation's legislation/rules are on what money the organisation should collect and how;
    - what the levels of awareness are in the organisation of the risk of fraud loss and how to report suspicions;
    - how mature the organisation is, or how new it is, and how established skills and ways of working to deliver the business are;
    - how mature the organisation's governance arrangements are, including reporting and assurance for financial management;
    - what new products/significant changes, including IT projects, are planned;
    - whether there are clear lines of responsibility and owners for financial loss and propriety in the key payment/service streams;
    - whether the organisation has a defined Fraud Risk Appetite; and
    - what previous audits and audit reports have indicated.

[19] Different customers may represent different levels of risk to an organisation. For instance, an organisation that interacts with a wide diversity of customers may inherently have a higher risk than one that interacts with a smaller, more tightly controlled customer base.

D6.3 Thematic (Grouped) Fraud Risk Assessments

1. A Thematic (Grouped) FRA looks at the overall risk faced within one of the specific activity / function / expenditure areas within the organisation or across organisations. These areas must be identified within the Organisational (Enterprise) level FRA, and should make sense to the business and how the organisation operates.

2. When effective Fraud Risk Assessment is established in the organisation, the Thematic (Grouped) FRA can be fed by IFIAs and Full FRAs within the activity / function / expenditure areas, but this is dependent upon having comprehensive coverage of the relevant area by the IFIAs and Full FRAs. These Thematic (Grouped) level FRAs then feed the Organisational (Enterprise) level FRA.

3. Where a Thematic (Grouped) level FRA is built from the IFIAs and full FRAs, it should:
    - show the scope of the area covered by the Thematic (Grouped) level FRA and the business activities within it and the extent to which they are covered by IFIAs and full FRAs;
    - give an overall assessment of the risk of fraud within that area in relation to the activities identified within the scope;
    - provide a description and a summary of the key known risks in the area; and
    - provide a summary of key identified control weaknesses in the area
    - explain any areas of uncertainty, for example where there is incomplete information at the time of the assessment
    - show the owners of the key risks and risk areas

4. Where there isn't comprehensive coverage of the area by IFIAs and Full FRAs, the Thematic (Grouped) level FRAs must include additional details to cover the limitations and gaps and should consider the following:
    - the spend level of the area, and the spend profile across the different elements / activities that make up the Thematic/Grouped area - which reflect the potential subjects for an IFIA and a Full FRA;
    - how high profile the area is and therefore the associated reputational risk of fraud issues;
    - how much is known about potential fraud in that area:
        - whether there are clearly identified and known fraud risks; and
        - whether there are reports of potential fraud or error within the spend activities;
        - whether there are similar/comparable spend areas which have had their risks assessed which can help in understanding risks relevant to this area
    - whether there is a detection and reporting process in place for fraud and error; and
    - to what extent there are controls in place to mitigate the known risks and whether there has been consideration of the effectiveness of these.

5. The Thematic (Grouped) level FRAs must be populated in clear language without unexplained abbreviations. It must be understood without the need to refer to other information sources and should have a key to aid understanding i.e. any colour codes or key definitions.

6. Where fraud risks are described they must be clearly defined in line with the definition of a fraud risk (using Actor, Action, Outcome). A fraud risk is an event that could happen that would result in a fraud attempt or actual loss.

D6.4 Initial Fraud Impact Assessments

What is an Initial Fraud Impact Assessment (IFIA)

1. An Initial Fraud Impact Assessment (IFIA) is a fraud, bribery and corruption impact assessment that gives an overview of some of the main fraud risks and challenges facing an individual business unit, project, programme or spending area.

The scope of an Initial Fraud Impact Assessment

2. An IFIA must be completed for any major new spend activity. Major spend activities, by definition, are large, complex or innovative, with many 'breaking new ground'.[20]

When an Initial Fraud Impact Assessment should be completed and how it will be used

3. An Initial Fraud Impact Assessment comes early in the life cycle of proposed new major spend activity. The purpose is to inform spend approval decisions and provide early assessment of the need to resource counter fraud activity, including mapping out counter fraud requirements throughout the spend area life cycle. It should also identify when the proposed design of a spend activity needs to be adapted or changed in relation to counter fraud concerns.

The impact if an Initial Fraud Impact Assessment is not completed

4. Failure to do this and to an appropriate standard could leave organisations exposed if the initial assessment under-represents the risk and impacts of fraud. A Counter Fraud Professional[21] must be closely involved with the development of the assessment.

Considerations before developing an Initial Fraud Impact Assessment

5. When developing an IFIA, the following areas should inform the potential ways that the spend could be defrauded:
    - lessons learned from other, comparative spend initiatives;
    - existing intelligence;

[20] Infrastructure and Projects Authority, Annual Report on Major Projects 2020-21, p. 13

[21] See Section D6.5 for Counter Fraud Professionals

- fraud risk logs;
- risk registers; and
- scenario planning.

6. The areas above can help to identify any known fraud risks as well as taking into account potential fraud risk drivers. Fraud risk drivers are referenced in paragraph section D6.5. If it is a new or novel spend activity, the likelihood of fraud risk is expected to be higher.

Timing of an Initial Fraud Impact Assessment

7. The IFIA should be time-limited to the planning and scoping phases of a spend activity. It is best practice for the IFIA to be completed before funding is approved. If it is after funding is approved, it should be completed as soon as possible.

What an Initial Fraud Impact Assessment must achieve

8. The Initial Fraud Impact Assessment must:
    - Understand the different types of fraud impacts that could affect the spend initiative arising from the types of fraud that could occur
    - Produce an initial indicative fraud risk rating and rationale based on the information provided, to determine the level of fraud risk that the spend activity could face relative to other spend
    - Enable the SRO and Accounting Officers to prioritise which of their spend activities they should put the greatest focus on for taking action to reduce and react to fraud risk. For the highest risk spend activities, counter fraud resourcing should be agreed up front.

The role of the Fraud Risk Assessor

9. The Fraud Risk Assessor could have one of three roles in relation to the IFIA. They are:
    - Completing an Initial Fraud Impact Assessment on behalf of the Senior Responsible Owner (SRO) of the spend activity
    - Facilitating the completion of an Initial Fraud Impact Assessment; and
    - Quality assuring an Initial Fraud Impact Assessment which has been completed by the business area/unit.

D6.5 Guidance on completing the IFIA

How an IFIA is completed

10. The IFIA should cover:
    - who and how many organisations are involved in the spend activity;
    - who the funding is available to and who the end beneficiary or recipient will be;
    - whether the funding has been divided across multiple initiatives or programmes;
    - the extent to which the spend is new, novel or contentious;
    - the anticipated speed of implementation or delivery of funding from the announced date;

- the operational environment, including the delivery or the supply chain
- the value of the spend initiative;
- what the counter fraud approach is across the lifecycle of the spend;
- which inherent fraud risks need to be monitored;
- what the potential fraud impacts could be to the spend initiative; and
- an initial assessment of fraud to enable prioritisation of further counter fraud activity.

Identifying fraud impacts

11. The Fraud Risk Assessor must consider which fraud impacts[22] could be relevant to the spend activity. The fraud impacts that should be considered are:
    - **Environmental** - Fraud can have an immediate and direct impact on the environment by; increasing levels of pollution; reducing biodiversity and disturbing ecological balance; resulting in significant clean up and maintenance costs due to environmental emergencies.
    - **Financial** - The amount of spending that is estimated to be lost as a result of fraud and error. It is estimated that public bodies lose 0.5 - 5% of their spending to fraud and error.
    - **National Security** - Fraud against public bodies can compromise national defence and security. It can; damage international standing; affect the ability of nations to get international support; be used to fund organised crime groups and terrorism, potentially leading to further crime and terrorist attacks.
    - **Physical** - Physical fraud impacts can; result in people having unnecessary or unsafe medical procedures; prevent people from receiving essential treatment or cause them to receive substandard treatment; expose people to hazardous substances or environments; lead to vehicles or aeroplanes crashing through faulty parts or maintenance; lead departments to rely on faulty or unsafe safety equipment or faulty infrastructure
    - **Policy Objectives** - Policy objective fraud impacts can happen in the following ways:
        i. Services are not delivered: finite money and resources are diverted away from the intended target, or services are not delivered to the standard required
        ii. Programme objectives are not met: the vision, objectives and goal of the policy or programme are compromised.
        iii. Programmes are shut down: in some circumstances, entite programmes are closed which can negatively impact those relying on that service
        iv. Opportunity cost: fraud can result in lost opportunities to a programme or service as they lose the opportunity to improve if shut down as a result of fraud.

[22] See International Public Sector Fraud Forum for further details on fraud impacts. Available here:https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance

- **Reputational** - Reputational fraud impacts include; erosion of trust in government; erosion of trust in industry; employee morale and confidence; damage to international and economic reputation
- **Societal** - Societal fraud impacts can often occur through; provision of sub-standard services or products; services or products being stolen or not being delivered; identity theft. Note: impacts are not limited to individuals, but can also extend to their families and communities.

How the IFIA should be assessed

12. The IFIA should have an initial indicative assessment score to understand the potential fraud risk that is posed to the spend activity as a whole.

13. The purpose of providing an initial indicative assessment is to determine the level of risk in comparison to other spend activity and to facilitate prioritisation of counter fraud resourcing.

14. Each IFIA should be made up of a series of assessments. These assessments are made using the knowledge and judgement of the SRO and policy/programme/project team, and should be considered in the light of the strategic context for the initiative. Note that the Full FRA focuses on assessing and scoring against individual inherent risks.

15. A scoring system of one to five (one being the lowest, five being the highest) should be used. Scoring definitions should be clearly articulated and explained.

16. When assessing the impact of fraud against the spend activity, the information supplied in the IFIA along with any existing research should inform the score. Assessors should ensure that the score is reflective of the impact that fraud could have on the spend activity as a whole.

17. It is important that each assessment has a short explanatory note of the reasoning for each mark (where appropriate) to provide an audit trail of the considerations.

Facilitating the completion of the IFIA

18. A Counter Fraud Professional might be asked to help facilitate the completion of an IFIA. In undertaking this role the facilitator might employ a number of techniques such as highlighting areas, and sources, for research, including the evidence base for fraud and its extent and impact within similar areas of spend; and bringing together relevant experts to form and run a meeting or workshop that will inform the details of the IFIA. It is vital that the facilitator enables consideration of the different ways fraud could happen that would result in harm arising out of the spend activity.

D6.6 Guidance on assuring the IFIA

Quality Assurance of the IFIA

19. If a Counter Fraud Professional[23] has been asked to complete a quality assurance review of a completed IFIA, the following steps must be taken:
    - Check that the IFIA has been completed in line with the FRA Standard; and
    - Provide a quality assurance comment based on the completeness of the IFIA as well as the level of counter fraud understanding that the IFIA demonstrates.

20. When assessing the IFIA, the Assessor should indicate whether a follow up is required to address any concerns that have arisen from:
    - the IFIA; and
    - the quality assurance assessment of the IFIA.

21. The explanation for a follow up should be provided in clear language without unexplained abbreviations.

Links to other Fraud Risk Assessments

22. An Initial Fraud Impact Assessment is not a Full Fraud Risk Assessment. It should drive prioritisation of a Full FRA, which must be undertaken once funding is approved and the scheme control frameworks are designed.

23. Initial Fraud Impact Assessments do not evaluate in detail the effects of the controls on the specific fraud risks and the extent to which residual risk remains. That is the role of the Full FRA.

24. The Full FRA will evaluate in detail the effects of the controls on specific fraud risks and the extent to which fraud risk exposures (residual risk) remain which could allow fraud, error, bribery or corruption to materialise.

25. A fraud risk log lists all frauds that an organisation might be subject to. The Initial Fraud Impact Assessment provides a broad assessment of inherent risks and potential fraud impacts to an individual business unit, project or programme.

26. An Initial Fraud Impact Assessment should also inform the Enterprise / Organisation Level FRA to capture the new areas of spend which pose a vulnerability of fraud to the organisation. This might also require similar updates to the Thematic (Grouped) Level FRA.

Outputs and Outcomes of the Initial Fraud Impact Assessment

27. A completed IFIA should be used to inform the department of the counter fraud resourcing requirements for the spend area over the lifetime of the scheme.

[23] This includes Professionals from department Counter Fraud teams, Government Internal Audit Agency or the wider Government Counter Fraud Function Centre of Expertise

28. The counter fraud resource requirements should be mapped across the lifecycle of the spend activity, highlighting specific counter fraud disciplines and expertise that will be needed at particular times. This corresponding Counter Fraud cycle should inform departments of the different counter fraud considerations and activities that are needed across the lifecycle of a spend activity. Examples, not exhaustive, include:
    - input to the design of the control framework to prevent and detect fraud, including the collection and the effective use of data and analytics employing data from both from internal and external sources;
    - the development and maintenance of full fraud risk assessments;
    - attending fraud risk governance panels to receive expert, independent counter fraud advice to strengthen fraud responses;
    - employing sanctions and penalties as part of a strategy of fraud deterrence;
    - linking with sources of intelligence and analysis; ensuring rights of access to inspect documents, individuals and premises;
    - the right to recovery funds in cases of irregularity; and
    - setting fraud tolerance levels and use of fraud measurement to estimate actual levels of fraud within the spend area.

D6.7 Full Fraud Risk Assessment

Fraud Risk Log

1. A Fraud Risk Log is a list of all of the fraud risks that an organisation might be subject to and that it is aware of. Fraud risk logs may be structured to suit the organisation. For example, they might be divided across different areas or products where there are cross-cutting risks on an area of spend.

2. In some organisations this will be held separate to the fraud risk register, as the log will be longer and more dynamic and the risks only incorporated into the register when they have been assessed. In other organisations the Fraud Risk Log might be part of the Fraud Risk Register.

3. An updated Fraud Risk Log is a key outcome of Step 3 of the Fraud Risk Assessment/Management Cycle. This step is: ‘Key known and hypothetical risks identified, categorised and defined’.

4. Fraud risks can be identified through:
    - tactical intelligence that the organisation receives, including whistleblowing;
    - outputs from strategic intelligence activity;
    - the results of completed investigations;
    - management information reports from fraud detection systems;
    - interviews with key staff;
    - workshops with groups of staff;
    - research on an organisation’s unrecognised fraud risks and threats; and
    - research on the fraud risks and threats faced by other, comparative organisations.

5. All fraud risks identified in a business whether through research, risk work or intelligence activity should be recorded.

6. Fraud risks considered must include both internal and external risks, and cover all of the business' services.

7. In the Fraud Risk Log fraud risks must be clearly defined in line with the definition of a fraud risk. A fraud risk is an event that could happen that would result in a fraud attempt or actual loss. The more specific these are, the more targeted controls to reduce the risk can be.

8. Fraud risks must have a clear description of the inherent fraud risk and its consequence. Fraud risks must be captured in the following structure:
    - **Actor:** Who commits the fraud (may be a single individual or more individuals)
    - **Action:** What the fraudulent action is
    - **Outcome:** What is the resulting impact or consequence(s). This will be mainly financial, but consider whether other aspects are relevant such as: reputational; social; physical harm; environmental; the extent to which fraud might undermine government policy objectives; or harm to national security

9. Fraud risks should have a unique reference.

10. The identification of risk is a creative process and should be approached from the perspective of trying to model how one could break the system and defraud it. This is opposed to a defensive process that seeks to justify why fraud is unlikely.

11. The Fraud Risk Log must be populated in clear language without unexplained abbreviations. It must be understood without the need to refer to other information sources and should have a key to aid understanding i.e. any colour codes or key definition.

12. Fraud risks in the Fraud Risk Log should be clearly categorised between risks and sub-risks.

13. Fraud risks and sub-risks should be structured logically, with sub risks sitting below umbrella/higher level risks, where appropriate.

14. The Fraud Risk Log should also be structured by service areas/business or operational unit areas/stakeholders or any other structure that breaks down different areas of the organisation into manageable and meaningful chunks for analysing full fraud risks.

15. The fraud risks should be structured and categorised in the Fraud Risk Log in a way that is specific, simple, meaningful and accessible.

- Specific: identifying separate risks for how individual instances of fraud may occur rather than having a more general risk. e.g. instead of having a single risk saying an applicant may submit a fraudulent grant application identify as separate fraud risks all the different ways that specific grant eligibility criteria may be misrepresented or ineligible factors not declared.
- Simple: simple to understand and follow;
- Meaningful: expressed in a way that it makes sense to the organisation; and
- Accessible: easy to navigate and find individual and related fraud risks, sub-risks and causes.

D6.8 Fraud Risk Register

The key product of any FRA is a fully populated register. An organisation is likely to have a number of Fraud Risk Registers, covering individual payment / service / business areas. It may also have an overall one for the business, which is a combination of the key risks or high level/umbrella risks from the different areas.

1. Fraud Risk Registers must be clearly structured and accessible. Language used should be simple and understandable with minimal reference to other documents.

2. Statements must be based on evidence rather than based on assumptions. If assumptions are used, these must be clearly acknowledged.

3. The scope of the business area that the Fraud Risk Register covers and any areas that have been deemed out of scope must be clearly recorded.

4. If any risks, issues or controls are omitted from the Fraud Risk Register for reasons of sensitivity, this should be clearly recorded.

5. Ideally an organisation would populate every field. However, there might be reasons why some columns may not be populated due to sensitivity[24]. Where possible generic information should be included to aid management response.

6. In the final presentation, the Risk Register must be clearly structured and should be organised with the most important risks first.

7. At the minimum, all prioritised risks where additional mitigating action is being considered must have clearly defined owners in the business. Ideally all risks in the risk register would have clearly defined owners. These may be at individual risk level or in line with the structure for fraud risk agreed with the business. It is important that risk owners are identified who will have sufficient authority to be able to make decisions and take action on the residual fraud risks identified. Where an owner cannot be identified, the counter fraud functional lead should

[24] Where there are sensitive risks or controls that the business feels cannot be recorded in the overall FRA, there is an option to have a separate confidential FRA with limited circulation that considers these risks/controls.

direct where ownership should rest until senior management agree the responsible individual.

Assessing Inherent Risk

8. All Fraud Risk Registers can have an assessment of the inherent risk that the risk poses, which would include an assessment of the likelihood and impact of the risk occurring in the absence of the control framework.

9. All risks must be assessed and scored against the likelihood of their occurrence and the impact if they do occur.

10. A scoring system of one to five (one being the lowest, five being the highest) should be used for both the likelihood and impact assessments.

11. When assessing the likelihood and impact of a fraud risk, it is vital that scoring definitions that are meaningful for the risks are articulated.

12. When assessing likelihood, it must be acknowledged that fraud risks are often not limited to a single occurrence.[25] A scoring system should be used that acknowledges that assessing fraud risk needs to consider both the occurrence, whether a risk will come to pass at all, and also the frequency with which risks can occur. The result is a quantification of the risk.

13. When assessing the impact of a risk, the duration of any potential fraud mustbe considered alongside the potential impact and materiality of the likely frequency of occurrence. Take into account timescales and consider if it is an operational risk that will occur just within a single year, a project risk within the project timescales or a strategic risk covering 3 to 5 years. When prioritising risks, high impact should override a low likelihood event. However, there is a tendency to underestimate likelihood. When assessing likelihood, one off events should be considered equally.

14. When assessing corruption risks as part of a fraud risk assessment, the impact of corruption on both the frequency and likelihood must be considered. For example, the assessor should consider how collusion can affect the likely occurrence and frequency of risks coming to pass (would it make it more or less likely to happen frequently), and whether it might make a risk more likely to succeed.

[25] For example, when assessing the risk that 'a false quantity and quality of products/services are invoiced on X project for payment, resulting in a loss to the organisation', we need to assess whether we mean this is likely to happen once during the lifespan of the project or more frequently i.e. several times a month. In assessing the fraud risk, we need to be clear what likelihood we are assessing. Are we assessing that it may happen once over a specific time period, or the life of the project, or are we assessing the likelihood it will happen with a certain frequency or coverage of overall spend i.e. we expect 3% of payments to be subject to this risk. There are two ways to deal with this. One is through more specific definition of the risk. For instance, one could say "*The risk that during the course of project X, contractors will submit invoices for payment that contain fraudulent information as to the quality and / or quantity delivered, resulting in a loss to the project*" with a clearly defined probability timeframe (3 months, 6 months, 12 months) and then within that we can focus the assessment on the frequency with which we expect that to occur. The other is to assess against both overall likelihood that it will happen at all (Occurrence) and then the frequency within which it is expected to occur. Again, it is helpful to set a time period. This approach allows the Assessor and stakeholders to take a more informed view on the financial impact i.e. one off medium value v. multiple medium value submissions that is equal to a larger amount.

15. When assessing likelihood and impact, all potential impacts (not just financial ones) of a fraud risk should be explored and understood.[26] This is a creative process where impacts should be explored rather than assumed.

16. The mechanisms for capturing an organisation's view of likelihood and impact should remain consistent throughout the FRA process, in order to prevent the skewing of outcomes.

17. Different approaches can be taken to score the likelihood and impact. For instance, some organisations may use voting technology to capture views in a workshop setting whereas others may be assessed in a group setting by a show of hands or discussion to reach agreement. There is no right or wrong way and an organisation should take a view on what serves their needs best. However, there is a tendency to under-estimate the risk of fraud and an experienced fraud risk assessor can choose to use their professional judgement based upon their own organisation's and the government's evidence base of known fraud risk and instances of fraud. Technology-enabled capture has many benefits in relation to anonymity and accuracy. However, the limitations of the approach used should be acknowledged by the Fraud Risk Assessor and recorded in the Fraud Risk Register. For instance, whilst group voting is a good tool for obtaining engagement and a wide variety of views, it can result in a lowering of the overall risk scoring.

Identifying Mitigating Controls and Assessing Residual Risk

18. Identified controls must be recorded clearly in the fraud risk assessment. To follow good practice, this must be accompanied by a description of how this impacts the fraud risk.

19. When identifying controls, the COSO's definition of internal control should be considered[27].

20. This must be followed by an assessment of the residual risk remaining, after the control framework is considered. The scoring mechanism must be consistent with

[26] Using the example above, there could be multiple consequences to this risk. There are financial risks, health and safety risks (should a substandard material be provided and passed off as one of greater quality) and reputational risks arising from both of these risks. The financial risk, the risk to life and reputational risk should all be acknowledged, in order to facilitate effective evaluation and prioritisation.

[27] COSO definition of internal control:

'Internal control is a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.'

This definition reflects certain fundamental concepts. Internal control is: geared to the achievement of objectives in one or more categories e.g. operations, reporting, and compliance; a process consisting of on-going tasks and activities, means to an end, not an end in itself; affected by people; not merely about policy and procedure manuals, systems, and forms, but about people and the actions they take at every level of an organisation to affect internal control; able to provide reasonable assurance but not absolute assurance, to an entity's senior management and board of directors; and adaptable to the entity structure, flexible in application for the entire entity or for a particular subsidiary, division, operating unit, or business process. This definition is intentionally broad. It captures important concepts that are fundamental to how organisations design, implement, and conduct internal control, providing a basis for application across organisations that operate in different entity structures, industries, and geographic regions.

that used for inherent risk, the only difference being that the control framework is taken into account.

21. The Assessor must ensure that the review of residual risk is critical of the control framework and does not rely on assumptions. It must explore not only the limitations and weaknesses of the controls in relation to a specific fraud risk but also consider how the controls could be avoided or circumvented by potential fraudsters, as well as exploring how the controls reduce the risk. If any assumptions are made these must be acknowledged i.e. the assumption that a manual control framework will be consistently followed.

22. When recording and agreeing residual risk this must include a narrative of the remaining residual risk in terms of the fraud risk exposure and how the fraud event could still happen despite the controls in place, why and how it could happen - including circumvention of the controls, and what the consequences might be. It is not sufficient to assess the residual risk at a high level and score the risk without describing the residual risk that remains.

23. In addition, Assessors **may** wish to record the agreed effectiveness of controls identified in the FRA to prevent fraud, if this is discussed. If this is done, the five levels of control mitigation detailed below should be applied.

    1. Non-existent: No controls exist so there is nothing in place to prevent the incident from occurring.

    2. Poor: Control/s exist, but are poorly designed and have major deficiencies. The control is largely ineffective, offering very limited or no mitigation.

    3. Satisfactory: Control/s design reasonably fit for purpose but there might be opportunities for improvement. It offers a reasonable level of mitigation.

    4. Good: Control/s design is fit-for-purpose. Control/s is/are operating and provides a good level of mitigation and there are minor opportunities for improvement.

    5. Excellent: Control/s design is fit-for-purpose. Control/s is/are operating fully as intended and offers an excellent level of mitigation.

24. FRA **may** also wish to assess the likelihood that if the fraud materialised it would be detected through the controls and systems in place.

25. The assessment of each residual fraud risk must include scoring to allow risks to be prioritised. Scoring must be consistent with the narrative assessment of the risk description (including outcomes), the effectiveness of the controls in preventing and detecting fraud arising from a specific fraud risk, and the residual risk. Scoring

must cover both the likelihood of the fraud risk occurring and its impact. For Likelihood the separate elements of a single occurrence and the frequency of occurrences should be considered. For Impact the separate elements of the possible duration of a fraud remaining undetected should be considered as well as the materiality of the outcomes.

26. Organisations will need to provide a scoring mechanism that is appropriate for their organisation, but definitions must be provided to allow the assessor to allocate a score appropriately and consistently.

27. The following is an outline of a matrix for scoring residual risk on a 1-5 scale that may be used for guidance:

Assessment of Residual Risk (Scores)			
Likelihood of Occurrence	**Likelihood** of Frequency	**Impact** - Duration of Fraud	**Impact** - Materiality
1 Unlikely	1 Only likely to be a occasional occurrence	1 Fraud should be prevented or detected immediately	1 Unlikely to result in a material loss / reputational risk
2 A possibility it will happen	2 A few instances likely to occur	2 Fraud should be prevented or detected quickly	2 Material loss / reputational risk likely to be avoided
3 Likely to happen	3 A number of instances likely to occur	3 Fraud could go undetected for a period of time	3 Could result in some material loss / reputational risk
4 Quite certain to happen	4 Likely to be a lot of instances	4 Fraud could go undetected for a long duration	4 Could bring high material loss / reputational risk
5 Certain to happen	5 Likely to be multiple instances	5 Fraud could remain undetected	5 Could result in significant material loss / reputational risk

28. To facilitate the reporting of risks on a 5x5 heatmap (see section D7) by arriving at a single score for both Likelihood and Impact, it is suggested that assessors can add together the two scores for Likelihood and also for Impact and divide each by two. The resulting overall scores for both Likelihood and Impact are then multiplied to give an overall score for the residual risk on a 1-25 scale. A worked example would be: Occurrence 5 + Frequency 3 divided by 2 = a Likelihood score of 4; Duration 4 + Materiality 5 divided by 2 = an Impact score of 4.5. The total score for the residual risk is calculated as 4 multiplied by 4.5 = 18.

Facilitating Full Fraud Risk Assessments

29. A Counter Fraud Professional may be asked to help facilitate the completion of a Full FRA. It is vital that the facilitator enables consideration of the different ways fraud could happen that would result in harm arising out of the spend activity.

30. In undertaking this role the facilitator might employ a number of techniques such as identifying areas, and sources, for research, including providing an evidence base for fraud and its extent and impact within similar areas of spend; the identification of key stakeholders, including risk, control and counter fraud experts who can inform the assessment; organising and running meetings or fraud risk workshops; arranging for walk-throughs of processes and associated controls; and providing a sense check of the assessment to ensure that the fraud risks identified are comprehensive and detailed to be as specific as possible, rather than general, with consistency between the narrative and scoring elements.

Quality Assurance of the Full Fraud Risk Assessment

29. If a Counter Fraud Professional[28] has been asked to complete a quality assurance review of a completed Full Fraud Risk Assessment, the following steps must be taken:
    - Check that the FRA has been completed in line with the FRA Standard.
    - Provide quality assurance feedback comments based on the extent to which the following has been achieved:
        i. Specific, rather than general, fraud risks have been identified and the coverage of the fraud risks is comprehensive.
        ii. That there is a clear understanding of how controls operate to mitigate each specific risk and that any limitations and weaknesses have been identified.
        iii. That there is a narrative description of residual risk that explains how fraud could still happen despite the controls in place, and how fraudsters might seek to circumvent identified controls and exploit the fraud risk exposure identified.
        iv. That scoring of residual risk is consistent with the narrative assessment and other available evidence, and that a clear rationale has been provided for each score given.
        v. That the scores and prioritisation within the assessment is logical and consistent across all the risks.

30. When assessing a FRA, the Assessor should indicate whether a follow up is required to address any concerns that have arisen from the quality assurance assessment of the FRA.

31. The explanation for a follow up should be provided in clear language without unexplained abbreviations.

[28] This includes Professionals from department Counter Fraud teams, Government Internal Audit Agency or the wider Government Counter Fraud Function Centre of Expertise

D7 Reporting

D7.1 Prioritisation Reports and Heatmaps

1. Prioritisation reports are an effective way to demonstrate what the key fraud risks are that the organisation overall, or an area within the organisation, should focus on.

2. Prioritisation reports must clearly and simply communicate what the key risks are.

3. Fraud risks must be clearly defined, in line with the definition of a fraud risk. A fraud risk is an event that could happen that would result in a fraud attempt or actual loss.

4. It should be made clear whether the risks referred to are umbrella/higher level risk or detailed sub risks.

5. Any links between risks should be referenced.

6. The limitations of the FRA that has produced the risk prioritisation/heat map should be transparent. For example:
    - if there was no intelligence of potential fraud instances to feed the fraud picture this should be acknowledged;
    - if a decision was taken to spend limited time on identifying fraud risks, which may limit the comprehensiveness of the FRA, this should be noted; and
    - if the control framework which mitigated the fraud risks was not fully understood, this should be recognised.

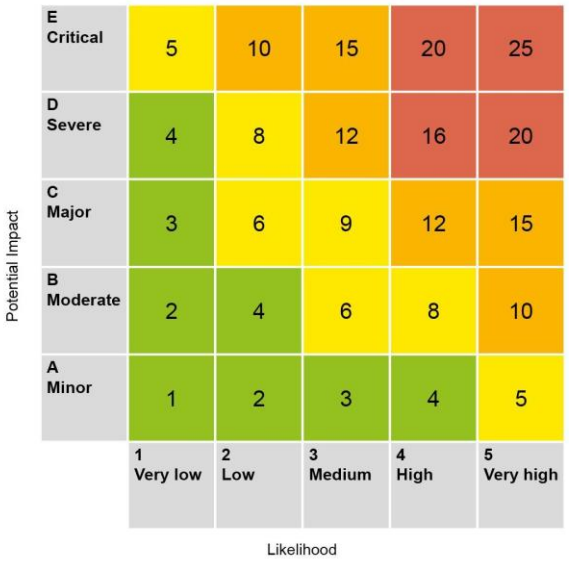
7. It is the role of the Assessor(s) to be aware of the limitations of the FRA and to communicate this effectively.

8. If possible, the prioritisation report should set the fraud risk priorities in the context of the organisation's defined appetite for fraud loss.

9. It is often helpful to present fraud risks in the form of a heat map. An example of a heat map is given below. The comparative scoring of the different grid spaces i.e. whether they are assessed as immediate, high, medium or low priority will be based on the organisation/area's risk assessment appetite and should be agreed with the counter fraud functional lead and overall owner of that area of fraud risk within the business.

10. A prioritisation report will often be one component of a wider Fraud Risk Management Report that details options and activity to reduce key fraud risks. A standard for this product can be found in the Leadership, Management and Strategy product standards document.

Below is a suggested heat map with four levels. Organisations should not use a heat map with less than four levels for this process to be effective. Impact definitions will need to be agreed in advance with both the Counter Fraud functional lead and the overall owner for the related area of business.



Priority 1: Immediate priority	16 - 25
Priority 2: High priority	9 - 15
Priority 3: Medium priority	5 - 8
Priority 4: Low priority	1 - 4

E. Guidance for Professionals - Organisational

E1. Introduction

Every government organisation faces a variety of uncertainties, which can adversely affect its objectives; these can be defined as risks. Executive Boards in every organisation should make arrangements for recognising, tracking and managing risks and should be able to make a considered choice about its desired risk appetite. The Executive Board's strategic guidance on risk appetite should permeate every organisation's programmes, policies, processes and projects.[29]

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

In the same way that organisations should manage risks within their programmes, projects and operations, an organisation should consider and manage the risk of fraud. The policies and processes in place should be visible at executive board level and integrated into the organisation's overall approach to managing fraud.

As with any other risk, the key to managing the risk of fraud is having an evidence-based understanding of the specific risks that might come to pass and how they might occur. Robust fraud risk assessment gives an organisation this understanding.

The resources dedicated to, and therefore comprehensiveness of, an organisation's fraud risk assessment will depend on the perceived fraud risk that an organisation, and its supply chain, faces. This will have to be prioritised against other key risk and delivery areas.

The Accountable Individual at board level **must** be able to determine if the level, coverage and depth of fraud risk assessment (FRA) is appropriate to the vulnerability or exposure an organisation feels it has in relation to fraud.

An FRA lies at the core of effective fraud management and is compulsory for all central government organisations. HM Treasury in their publication 'Managing Public Money' advises "each organisation should identify and assess at different levels how it might be vulnerable to fraud with reference to the HMG standards for Fraud Risk Assessment. Fraud should be always considered as a risk for the departments' risk register."

If an organisation is unaware of the fraud risks it faces it will be unable to put in place an effective strategy, controls and resources to tackle and reduce the likelihood and consequences of these risks coming to pass.

Accountability and responsibility for fraud risk management at board level should be clearly defined. The counter fraud functional lead should seek the sponsorship of the fraud risk management programme at the highest level of the organisation[30]. This will

[29]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/454191/Managing_Public_Money_AA_v2_-jan15.pdf

[30] See GCFF Leadership, Management and Strategy standards

help the fraud risk Assessor(s) to work with the business to deliver effective and meaningful fraud risk assessments.

These standards outline what a public sector organisation is expected to have in place to enable an effective fraud risk assessment, which will enable the organisation to manage fraud risk.

E2. General

1. All organisations must have an Organisational (Enterprise) level fraud risk assessment supported by Grouped / Thematic fraud risk assessments, as well as Initial Fraud Impact Assessments and Full Fraud Risk Assessments for the areas of highest risk and materiality. The fraud risk assessments must allow the organisation to understand where it has the potential to be vulnerable to fraud and error by describing the fraud risks that the organisation faces and assessing their likelihood and impact. The HMG Functional Standards outline the requirements of all organisations and regular reviews by the Counter Fraud Function's Centre of Expertise are completed to monitor and report progress against the standards.

2. At board level, organisations should have a document that describes what the key fraud risks are and what the organisation is doing about this.

3. To deliver and renew their FRAs all organisations should have an annual FRA plan (the Plan)[31] against which the progress and output of the FRAs can be measured.

4. All organisations should ensure that FRAs are completed/facilitated by assessors with the appropriate skills. This may be one individual or a group of people with the mix of appropriate skills e.g. an experienced risk assessor working with an experienced counter fraud specialist. The counter fraud functional lead can assist in this.

5. The organisation should make sure there are arrangements in place to check the quality of fraud risk work.

6. The accountable individual at board level[32] should sign-off the Plan and the Organisational level Fraud Risk Assessment, which would have been communicated to them by the counter fraud functional lead[33].

7. All FRAs must have an operational business unit sponsor e.g. Head of Finance, Head of Procurement, Head of Operations, Head of Policy. Where there is no single sponsor, a single point of contact should be nominated to deal with logistics.

[31] See FRA Product standards

[32] See GCFF Functional Standards SO13

[33] See GCFF Leadership, Management and Strategy standards

8. The relationships and roles of the counter fraud resource; internal and external audit; finance; organisational risk management; and board/committees in delivering and assuring the effectiveness of fraud risk assessments, should be agreed and stipulated in the Plan or Counter Fraud Strategy.

9. The organisation should provide Assessors with unfettered access to relevant information.[34]

10. The organisation's Organisational (Enterprise) level FRA, supported by other FRAs, should form the basis of the organisation's counter fraud strategy[35].

11. FRAs should be tailored to the organisation's structure and operations to ensure that the most significant fraud risks are captured.

E3. Continuing Professional Development (CPD)

12. Where there are specialist fraud risk assessors within the business, the organisation should ensure that they undertake regular learning and development to keep their skills and knowledge up to date.

E4. Quality Assurance

13. Fraud Risk Assessors within the GCFP should seek to have a sample of their fraud risk assessments periodically reviewed and quality assured against this Standard by other professionals who the GCFP designates as qualified to undertake such assessments.

E5. Infrastructure

14. Risks and intelligence are not the same or interchangeable. The organisation should not rely on intelligence alone to inform them of their fraud risks. This will lead to a distorted picture of only prioritising known and reported fraud and make an organisation reactive.

15. The organisation should refresh their FRA Plan[36] on a frequent basis, as set out in the FRA Product Standard.

16. The FRA as well as other related documents[37] on which it depends should be reviewed regularly. The fraud risk profile of the organisation, as well as changes in circumstances/projects and horizon scanning, should drive the timeframe between FRAs. If best practice is followed, fraud risk assessment should become

[34] This include but is not limited to: information on structure and human capital (headcount, use of contractors, change programmes recent and planned), overarching departmental objectives and strategy (at a high level), budget and key areas of spend/major projects planned or underway, history or current and past fraudulent incidents, counter fraud capacity/capability, role of Internal Audit and IA reports into areas subject to a FRA, risk management processes/procedure, supply-chain /relationship with third parties

[35] See GCF Standards on Leadership, Management and Strategy

[36] See FRA Product standards

[37] See Product standards for FRA and Leadership, Management and Strategy

a continuous process to maintain awareness of fraud risks and ensure changes in the risk level are proactively identified.

F. Glossary

F1. Further Information

These Professional Standards and Guidance have been created in order to align counter-fraud capability across government.

If you have any questions surrounding the Government Counter Fraud Profession, and how you can get yourself and your organisation involved, 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

F2. Glossary

This Standard contains both mandatory and advisory elements, described in consistent language (see table below).

Term	**Intention**
must / shall	denotes a requirement; a mandatory element
should	denotes a recommendation; an advisory element
may	denotes approval
might	denotes a possibility
can	denotes both capability and possibility
is/are	denotes a description

Other key terms used within the Standard are defined below:

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

Controls: The policies, processes, tasks, behaviours and other aspects of an organisation that taken together: facilitate effective operation by enabling it to respond appropriately to significant risks to achieve its objectives; ensure the quality of internal and external reporting; and ensure compliance with applicable laws and regulations as well as internal policies. There are different categories of controls such as Physical controls; Authorisation and approval limits; Segregation of duties; Management and supervisory controls; Arithmetic and accounting controls; and Human resources controls.

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

Error: are similar occurrences to fraud but where the elements of dishonesty or intent (see definition of Fraud) are missing or cannot be proved. However, error also results in losses to public funds and for the purposes of this Standard is considered alongside fraud.

Expenditure Area: is spending by public bodies within a specific category. Categories could include: Infrastructure and Construction, Transformation and Service Delivery, Military Capability and Information and Communication Technology.[38]

Fraud: is defined as set out in the Fraud Act 2006. The Act gives a statutory definition of the criminal offence of fraud, defining it in three classes - fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. In HMG we use this definition but for reporting instances of fraud we apply the standard from civil law, the balance of probabilities test.

In all three classes of fraud, it requires for an offence to have occurred, the person must have acted dishonestly and that they acted with the intent of making a gain for themselves or anyone else, or inflicting a loss (or risk of loss) on another. Whilst intent is a key factor in determining fraud, it may not always be apparent and so for the purposes of protecting the UK public purse we incorporate the risk of **Error** alongside the risk of Fraud when undertaking Fraud Risk Assessments. Therefore all references to fraud risk within this document should be taken to also include the risk of error, which represent losses where there is insufficient evidence to prove intent.

Fraud Risk Assessment: is a process aimed at proactively identifying and addressing an organisation's vulnerabilities to both internal and external fraud. It is an essential element of an effective counter fraud response and whilst it should be integrated into the organisation's overall risk management approach, it requires specific skills, knowledge, processes and products.

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

Function: also defined as a business process or set of specialist activities that together support the organisation.

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

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

[38] Examples of categories taken from the Government Major Project Portfolio.

Mature Environment: denotes an 'established' way of managing counter fraud activities, including the use of Fraud Risk Assessments, across the organisation. Importantly, in a mature environment fraud risks identified across all spend areas feed into strategic documents.

Outcomes: are defined as the delivery of; planned products; financial savings; beneficial procedural and/or behavioural changes; and improved cultural changes as a result of approved activities.

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

Risk: the possibility of an adverse event occurring or a beneficial opportunity being missed. If realised, it may have an effect on the achievement of objectives and can be measured in terms of likelihood and impact.

Risk Appetite: the amount of risk the organisation is willing to accept at the enterprise level, which manifests itself in the type and number of activities and associated risks that the organisation is willing to undertake.

Risk Tolerance: the threshold levels of risk exposure and target levels of incidences and losses that with appropriate approvals can be exceeded, but which, when exceeded, will trigger some form of response e.g. reporting the situation to senior management.[39]

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

Threat: a person or group, object or activity that has the potential to cause harm to the achievement of the organisation's objectives. It takes into account capability and intent to do so.

[39] M_O_R/ Office of Government Commerce: Management of Risk