Public Sector
Fraud Authority

Government
Counter Fraud
Profession
CENTRE OF LEARNING

Full Fraud Risk Assessment

Practice Note

Government Counter Fraud Profession | January 2026, Version 1

Contents

Purpose and Scope

This Practice Note has been developed by the Government Counter Fraud Profession (GCFP) Centre of Learning, operating out of the Public Sector Fraud Authority. The guidance aligns to, and should be read in conjunction with, the agreed standards for professionals produced by the GCFP for fraud risk assessment in government. It brings together leading practice from across the public sector to provide guidance for those responsible for the completion of Full Fraud Risk Assessments and what to include in them.[1]

All organisations are vulnerable to fraud, bribery and corruption and in order to effectively manage the risks, the risks need to be identified and assessed.[2]

Full Fraud Risk Assessments (Full FRA's) identify and assess the fraud risks within a specific spend, scheme or project area in order to identify mitigations and controls to manage or reduce the risk of fraud, while also highlighting weaknesses or gaps in controls and identifying any remaining residual risks.

A Full Fraud Risk Assessment provides the Senior Responsible Officer (SRO) with an understanding of the fraud, bribery and corruption risks and enables identification and prioritisation of actions that may be required as a result. It helps organisations to understand the relevant fraud risks and develop a practical plan for targeting resources to reduce the risks.

Full Fraud Risk Assessments should be completed for all business areas where there is a considerable risk to the organisation from fraud. Ideally this information should be known from and driven by Enterprise or Thematic-level FRAs and also include areas identified by an Initial Fraud Impact Assessment as high or very high impact to ensure that resourcing for Full FRAs is being used for priority areas. Actual risks identified via a Full FRA as key risks to be prioritised should feed back into the organisation's Thematic and/or Enterprise Fraud Risk Assessments.

Full Fraud Risk Assessments are a requirement under Managing Public Money to ensure fraud risk is mitigated and the loss to fraud and error is minimised, thereby increasing efficiency and protecting public money.[3]

The responsibility for managing fraud risks rests with the organisation's accounting officer, supported by an accountable individual at board level, supported by the senior officer accountable for counter fraud (the counter fraud functional lead) within the organisation.[4]

> Full Fraud Risk Assessments identify and assess the fraud risks within a specific spend, scheme or project area

[1] https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government

[2] The term 'Fraud' throughout this document refers to offences of fraud, bribery and corruption.

[3] https://www.gov.uk/government/publications/managing-public-money

[4] https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud

What is the role of those assessing Fraud Risk?

For those assessing fraud risk, the role is varied and dynamic. From thinking like a fraudster and developing process maps, to engaging and negotiating with stakeholders, an assessor supports the organisation to understand the current fraud risk environment.

Fraud risks are organisational risks requiring an organisational response. Therefore, assessors should be able to assess and evaluate these risks and provide a prioritised list to the SRO/ Governance Board for them to consider how these are best managed in line with the organisations fraud risk appetite and tolerance levels.

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 in order to further understand and assess fraud risks and communicate them effectively.

Under the Government Counter Fraud Function Continuous Improvement Assessment Framework (CIAF) maintained by the PSFA, all Fraud Risk Assessments carried out by central government departments and their Arms Length Bodies should be quality assured and regularly reviewed by fraud risk assessors that have successfully completed fraud risk assessment training and assessment to the GCFP Standard.[5]

A review may be triggered by a significant change to spend profile, changes in control framework, or fraud risks materialising as well as changes in services, systems, or structures.

Engage People Early

Early engagement in the assessment process with internal and external stakeholders such as risk owners, contractors or delivery partners ensures that the right individuals are involved and informed from the beginning. This includes identifying the correct risk owners in the first place, involving colleagues from various departments with valuable insights into potential vulnerabilities, who understand the processes that help in risk identification and risk definition, control descriptions, assessment and residual risk. Early engagement creates a sense of ownership and can also mitigate challenges that may arise later on in fraud risk assessments.

[5] The emerging role of Fraud Control Specialist is intended to be included within this scope.

Those assessing fraud risk are:-

Creative Thinkers – adopting the mindset of a fraudster to effectively identify and mitigate potential risks. By replicating the methodology of fraudsters, a fraud risk assessor can inform or develop robust strategies aimed at anticipating potential fraudulent activities, ultimately contributing to the creation of a resilient organisational framework that can proactively address and minimise fraud risks.

Translators – converting complex risk data into clear, actionable insights that are accessible to various stakeholders across the organisation. This involves not only communicating the nuances of fraud vulnerabilities but also ensuring that the implications are understood in a practical context.

Negotiators – working collaboratively with different departments and teams helping to cultivate a culture of fraud awareness and prevention while balancing operational needs with fraud risk management.

Trained Advisors – providing the technical expertise on fraud risks and fraud risk assessments allowing the SRO who owns the risk to properly prioritise, address and manage the risk. 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 and how these relate to the individual spend, scheme or project under assessment.[6]

Professional – Fraud risk assessors must be able to conduct professional and competent reviews to the 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.

[6] https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government

Defining and Identifying Fraud Risks

Defining Fraud Risks

To understand Full Fraud Risk Assessments and all FRAs, it is important to know what is meant by risk. There is a subtle difference between risk and the drivers of risk but it is necessary to understand the difference to ensure the actual fraud risk is defined and recorded.

What is meant by risk?

A **risk** is the possibility of an adverse event occurring or a beneficial opportunity being missed. If realised, it may affect the achievement of objectives and can be measured in terms of likelihood and impact.

However, a fraud risk always represents an adverse event (rather than a beneficial opportunity being missed).

A risk arises from threats.

A **threat** is a person, group, object, or activity that has the potential to harm the achievement of the organisation's objectives.

Drivers are the underlying factors, conditions, or motivations that increase or decrease (drive) the likelihood of fraud occurring. They influence the scoring of risks but are not risks or threats themselves. Understanding these drivers can help identify and prevent fraudulent activity within an organisation.

A fraud risk is an event that could happen that would result in a fraud attempt or actual loss, it is not the circumstances that might allow it to occur.

When assessing the risk you should take into account any drivers which increase the likelihood of it happening (and include these in the "rationale" section when adding the narrative assessment for scoring of the risk).[7]

Example:

Under increasingly difficult market conditions combined with a lack of controls (drivers), a corrupt supplier (threat) may falsify invoices in order to receive payment for work not completed (risk). A fraud of this nature could result in financial loss and damage public trust in the organisation (impacts).

[7] See "Rationale" section further in this Practice Note.

Identifying Fraud Risks

After gathering information from various sources and research activities[8], assessors can then use the information to identify specific risks by utilising one, or ideally both, of the following approaches:

The Three Lens approach

Eligibility Criteria

Individuals

Process Steps

In this methodology you employ three different perspectives to help you identify different fraud risks: Eligibility Criteria; Individuals; and Process Steps.

By taking each of these perspectives in turn, the assessor considers how a specific instance of fraud could occur.

- For example, to be eligible for a grant, benefit or contractual payment, someone would have to meet certain **eligibility criteria**. There is the potential for misdeclaring that any particular eligibility criteria has been met when it has not. Therefore every single eligibility criteria, or clause in a contract may represent a separate risk of fraud through misrepresentation.
- The next perspective is to look at the different **individuals** involved in the process (both external and internal to the organisation) and consider the different ways that they might commit fraud. The purpose is to identify any additional risks that the Eligibility Criteria perspective has not identified.
- The third perspective is to look at the **process steps**. This is a walk through of the process being examined from end to end, to consider at each stage how fraud might be committed. Again the purpose is not to duplicate fraud risks already identified but to identify additional risks that the Eligibility Criteria and Individuals perspectives have not identified.

[8] https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government

The Offences approach

False representation

Failure to disclose information

Abuse of position

In this approach you take each of the main fraud offences in turn and use them to consider how fraud could happen within the scheme or business area you are assessing.

For example, the Fraud Act 2006 gives three main offences of fraud by false representation; failing to disclose information; and abuse of a position, as well as a number of other offences including the separate offence of obtaining services dishonestly.[9]

By looking at each offence, the assessor considers how they might apply to the process, scheme or business area they are assessing.

- Starting with **false representation** the fraud risk assessor should think about all the information that someone (a potential fraudster) has to provide, and the recognition that each item of information could be misrepresented and therefore be a potential fraud risk.
- Next the fraud risk assessor should consider information that would be required to be declared but which a potential fraudster might **choose to omit**.
- Thirdly the assessor should consider the individuals involved in the process and the different ways and extent to which they might be able to commit fraud through **abuse of position**.

Applying these perspectives methodically allows the assessor to see if there are any additional risks that have not been already identified. The purpose of taking these different perspectives is to identify very specific ways that fraud can happen. Remember, fraud 'happens in the detail' and understanding every single way that fraud could happen allows the fraud risk assessor to provide the Senior Responsible Officer with a comprehensive picture of exactly how these instances of fraud could happen, and the extent to which they are likely to occur and the associated impact.

For further information on risk assessments specific to bribery and corruption, please see the GCFP Standard for the Counter Bribery and Corruption Professional.[10]

[9] https://www.legislation.gov.uk/ukpga/2006/35/contents

[10] https://www.gov.uk/government/publications/a-standard-for-the-counter-bribery-and-corruption-professional

Building the Full Fraud Risk Assessment

Actor, Action, Outcome

All risks recorded must be fraud risks, that is, each risk should amount to and describe an economic crime, and not some other form of risk (e.g. risk of control failure). For each risk the Actor, Action, and Outcome must be clearly defined and articulated. This identifies who commits the fraud, how they do it and what the impact is, which ensures clarity and avoids overly generic risk descriptions.

A clear risk description also aids appropriate ownership of a specific risk to be assigned.

- **Actor** – This is the individual(s) or group who might carry out fraudulent activity. This may include internal employee(s), or an external third party. Define their role or relationship to the organisation or the spend area, scheme or project.
- **Action** – This is the specific fraudulent act the actor carries out. Examples could include submitting false documentation, altering records, creating a fake vendor or diverting payments. Defining action in this way helps avoid vague risk descriptions and clearly describes what is being done. This will depend on the legal or regulatory framework your organisation operates in but may include for example, the Fraud Act 2006 or Bribery Act 2010 offences. Combining actions (risks) should be avoided.
- **Outcome** – This describes the impact if the fraudulent action succeeds.[11] 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.

This approach helps the rest of the fraud risk assessment to ensure that relevant controls are identified and assessed, in particular to determine the extent to which they target the Actor identified and would mitigate the risk by preventing or detecting it, and/or deterring and directing the actor away from committing the action. Any remaining residual risk identified can then be assessed in terms of the extent to which identified outcomes would still happen.

Each identified risk should be addressed individually and assigned a unique identification number and descriptor for easy reference.

They should also be prioritised in line with the organisations fraud risk appetite and risk tolerance within the spend/scheme/project.

Identify the Risk Owner

Identifying a dedicated owner for each risk is critical. This individual is responsible for deciding what action will be taken in the risks that they are the owner for. Establishing clear ownership not only ensures accountability but also facilitates more effective communication and decision making throughout the Fraud Risk Management Cycle.[12]

Risk owners should have the authority to make a decision as to whether the residual fraud risk can be tolerated and to be able to take action if not. This means that they will be able to deploy resources needed to implement necessary controls and responses. Risk owners should also engage with relevant stakeholders to ensure that the insights from the FRA are incorporated into wider organisational strategies and processes. Clear communication regarding roles and responsibilities will create a collaborative environment that supports proactive risk management. Where programme risk ownership is divided between multiple people, then each risk in the register must have its own individual owner.

[11] https://assets.publishing.service.gov.uk/media/5e4bedb986650c10e5a91d89/2377_The_Impact_of_Fraud_AW__4_.pdf
[12] https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government

It is not enough to assign ownership of a risk to a third party. If a risk has been transferred to a third party but some impacts of the risk remain (e.g. reputational, environmental[13]), then the risk will still need to be held by the organisation and should be assigned to an internal risk owner.

Counter fraud leaders and risk assessors will not be the owners of risks outside of their own service area.

Identifying and Assessing Controls

Controls should be described in relation to the effect they have on the specific fraud risk, showing both what the control does to mitigate the risk and equally what it would not do (weaknesses and limitations) to stop that risk.

There are different types of controls[14] and these should be categorised by the effect that they have on the fraud risk as follows:

- Directive
- Deterrent
- Preventative
- Detective
- Corrective

Each control should be documented, and any limitations and weaknesses related to how each control applies to a specific risk must be assessed and recorded. Control dependencies, including those involving third parties, should be noted to evaluate the overall effectiveness of the controls and should be summarised to gauge the residual risk. Additionally, some control types are dependent on others. For example, a corrective control depends on there being an effective detective control that triggers the corrective action.

The current vulnerability to each individual fraud risk must be identified through an accurate assessment of the residual risk, clarifying how the fraud risk may still materialise despite the existing controls.

Identifying and Assessing Residual Risk

Understanding the residual risk is central to a Full Fraud Risk Assessment. Residual risk describes the different ways that each specific fraud risk could still happen despite the controls that are in place.

Therefore, when assessing and describing residual risk the starting point for the fraud risk assessor is the analysis they have completed in the controls section.

The **first** consideration is to determine whether there are controls in place which will stop the fraud risk from happening (preventative controls) or to find it if it does happen (detective controls). Other controls such as directive or deterrent are useful but do not actually do anything to stop fraud. Directive controls provide guidance (and may be more effective in stopping error) but are unlikely to stop a determined fraudster from ignoring the rules. Similarly, deterrent controls may reduce the overall incidence of fraud, but have limited effect on actually stopping one from happening.

If preventative and detective controls have not been identified, then there is nothing to stop that fraud risk from happening or to find it if it does happen and so the residual risk will be the same as the inherent risk (the risk before any control comes into play).

[13] https://assets.publishing.service.gov.uk/media/684ae4c6f7c9feb9b0413804/Managing_Public_Money.pdf
[14] See GCFP Fraud Prevention Standard for Counter Fraud Professionals.

If preventative and detective controls have been identified then the next step is to consider how effective they will be against the specific fraud risk that is being assessed. Remember, controls may have different effects on different fraud risks, so avoid the temptation to 'cut and paste' an assessment from an earlier risk. The key thing is to take into account the limitations and weaknesses that were identified in the previous step of the FRA. How might those limitations and weaknesses allow this particular fraud risk to still happen? Perhaps in certain circumstances if not all the time.

Finally, when assessing the residual risk consider how a fraudster might find ways of circumventing the controls in place.

The residual risk section should then be written up as a narrative to describe how that fraud risk can still happen. It may be helpful to preface your narrative with the phrase: 'This fraud risk could still happen because...'.

Risk Scoring

Having assessed and described the residual risk for each fraud risk, it is important to distinguish the different level of risk that each fraud risk presents. This is where scoring comes in to help identify the different levels of exposure that each fraud risk presents and how to prioritise between them.

Residual risk scores "should" be recorded and inherent risk "may" be recorded. Like any risk assessment we assess on Likelihood and Impact. However, for fraud risk assessment we bring in additional dimensions to help the assessor understand and present what the likelihood and impact actually are. The risk scoring will provide evidence of the individual components of **Likelihood of Occurrence**, **Likelihood of Frequency**, **Impact - Duration** of Fraud, and **Impact - Materiality** that contribute to these scores.

For assessing **Occurrence** you are assessing how likely it is that a single instance of that fraud risk will materialise; whereas **Frequency** is an assessment of the volume. When scoring Occurrence and Frequency for the residual risk you will particularly want to take into account preventative controls. Deterrent controls might also be judged to have some effect on occurrence.

For assessing the impact of **Duration** you will need to consider how long a single incidence of a fraud risk occurring might continue without getting picked up. For this, a key consideration is the presence of effective detective controls. The absence of any detective controls that would have an effect on a specific fraud risk will mean that fraud risk has the potential to continue in perpetuity. It is important, however, to distinguish between frauds that are one-off instances and frauds that can be repeated over and over again.

For assessing the impact of **Materiality** you will need to consider the 'Outcome' you identified when describing the fraud risk and make an assessment of the extent to which these outcomes will come into play now you have identified and described the residual risk.

For all risks you need to do a sense check to ensure that the scores you have given for the residual risk are commensurate with the rest of your fraud risk assessment and in particular the Outcome section, Controls and Residual Risk. If you have scored the inherent risk (the risk before any control comes into play) then you should also consider the difference between the two and whether they make sense. If there is a big difference between the inherent risk score and the residual risk score then you are assessing the controls as very effective in mitigating the risk. On the other hand, if there is only a small difference between the two scores then you have assessed the controls as having little or no effect on that fraud risk.

The following is an outline of a matrix for scoring both inherent and residual risk on a 1-5 scale that may be used for guidance. Please note it is important that you add values to this generic matrix to fit the context for the area you are assessing and organisation you are working in. For example, in your context what does ‘a few’ compared to ‘many’ instances look like? 10,000 instances of fraud might be ‘multiple’ in one organisational context and ‘only a few’ in the context of another organisation.

To ensure quality it is important to undertake a moderation session with others once all the risks are scored to check the results and ensure that the scores are appropriate and make sense in terms of risk prioritisation. The fraud risk assessor must exercise objective, professional judgment, to ensure scores accurately reflect the available evidence, in other words that the scores do not reduce (or increase) where the evidence does not support this.

Assessment of Residual Risk (Scores)

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

This grid is for illustrative purposes only as a generic example at a basic level, **it is not a template**. It is crucial for practitioners to build their own scoring matrix with a defined scoring criteria which is meaningful and appropriate to their organisational setting.

Rationale

For each risk score you must provide a Rationale describing your thought processes in giving the score you did and why that score is appropriate. The Rationale must show the reason for the scoring of each element separately: Occurrence; Frequency; Duration and Materiality; and should draw upon and refer back to the rest of the FRA as appropriate (for example a control limitation). If other information influences the score assigned to that fraud risk, that should be referenced and explained. If there have been no recorded cases of a specific fraud risk occurring, that is not a sufficient reason for a low overall score.

Fraud Risk Management

The completed Full Fraud Risk Assessment will help risk owners to manage each of the risks identified in accordance with the Fraud Risk Management Cycle, with the scoring and rationale aiding them in deciding how to prioritise any actions to mitigate the risks. The fraud risk management process is outside of the scope of this Practice Note, however, risk owners will have to decide for each residual fraud risk between the following four options for risk management:

1. **Tolerate** – the Senior Responsible Owner (SRO) is content that the residual risk is within the tolerance, and so no action is required to reduce its impact or likelihood. In some instances, it may be necessary to seek a Ministerial direction if the risk exceeds organisational appetite and tolerance.

2. **Treat** – the impact and/or likelihood exceeds the SRO's agreed tolerance (aligned to the organisation's risk appetite), and so action is required that will impact the control environment or in some other way reduce either or both of the likelihood or impact scores. The SRO should set out what additional controls are planned, and the timeline for these to be developed and implemented.

3. **Transfer** – in some circumstances it may be possible for some of the impact of a risk to be borne by another organisation. An example of this is the use of insurance to mitigate the financial impact of a risk event. However, this is likely to be an unusual occurrence in the public sector, and even where some of the impact of a risk can be transferred, for example to a delivery partner, the reputational risk (and other impacts, such as knock-on effects that delay delivery of commitments) will still sit with the commissioning organisation and must therefore be managed accordingly.

4. **Terminate** – ultimately, if none of the other options listed are sufficient then a programme may be closed if the overall risk is too great. This is unlikely to be an option in the public sector, where services and payments are essential, whereas a commercial business would be able to withdraw from a market if the risk exceeded tolerable levels and could not be managed in a commercially viable way. However, in the context of an individual fraud risk it may be possible to terminate a specific risk by redesigning the scheme or process.

Presenting Findings

When presenting the findings from the Full Fraud Risk Assessment it is important to convey the information clearly and concisely. A structured approach should be used to highlight the identified risks, their potential impacts, and the recommended actions. Using visual aids, such as heat maps or prioritisation reports, can effectively highlight key fraud risks and their significance to the organisation's overall risk profile and risk appetite.

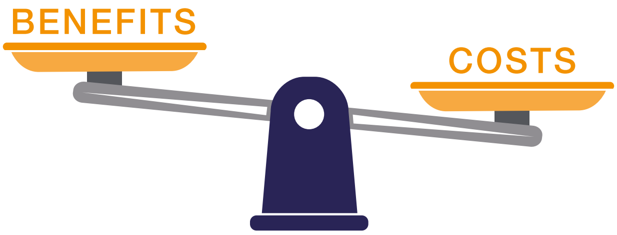
Presenting a summary of the Full FRA will provide a comprehensive overview that engages the SRO and risk owners in discussions about the implications of these risks. Having a stated fraud risk appetite means that residual risks can be presented in that context. Achieving organisational objectives will always involve accepting a level of risk (including a risk of fraud) and having a defined risk appetite helps organisations make informed decisions about trade-offs they are willing to accept in terms of identified risks (in this case the likelihood of loss from fraud or error) and the likely success of other objectives.

It is essential to showcase how each risk links to spend/scheme/project objectives while demonstrating the potential consequences of inaction. Using the language of the organisation spend/scheme/project area, and showing how the costs of implementing controls will bring greater benefits through enhanced fraud prevention and savings creates a compelling narrative that encourages dialogue and actionable outcomes among stakeholders. Equally, avoid recommending expensive controls that will bring little benefit just because some residual risk remains, as this would be poor value for money. Incorporating case studies or examples from similar organisations can illustrate the practical implications of the findings.

Documenting the Fraud Risk Assessment process

The approach taken to developing the Full Fraud Risk Assessment should be documented and will be informed by policies, guidance documents, processes, insights from known risks, workshops, structured interviews, intelligence, investigations, and audits. The Full FRA must identify a named assessor along with the date of its creation, and it should also document the approval date, have a version control number, and highlight a designated owner responsible for its oversight. Additionally, the Full FRA should be reviewed and updated within 12 months of its creation or following any significant "trigger" events such as a change in spend profile, changes in control framework, or fraud risks materialising, as well as changes in services, systems, or structures. There should be clear evidence of it being reviewed, challenged, and approved by an Accountable Board Member or Senior Responsible Owner (SRO).

> The FRA development approach should be documented and guided by policies, risk insights, workshops, interviews, intelligence, investigations, and audits



Full Fraud Risk Assessment - Top Tips

A Full Fraud Risk Assessment should be thorough and effectively identify potential vulnerabilities to fraud within an organisation. Guidance on the “what” and the “why” of Full Fraud Risk Assessment is set out below.

FRA Development Approach →

Fraud Risks →

Control Environment →

Residual Risk →

Scoring of Inherent and Residual Risk →

Actions →

Governance →

FRA Development Approach	Why / Reasoning
Document and present the approach taken in developing the Full FRA and/or how it was informed using a variety of techniques (i.e. policy, guidance document, procedure, process map, insights from known risks, errors, workshops, walk throughs, structured questionnaires, structured interviews, management information, audits).	This shows how the assessment is formed so that any gaps can be challenged or addressed if necessary.
The Full FRA should cover a specific spend/scheme/project.	This shows that consideration has been given to the end-to-end process to provide a full fraud risk landscape for the spend/scheme/project.
The Full FRA should have a named author and date of development, the date it was approved and a version control number.	To ensure accountability and audit trail.
The Full FRA should have a named owner.	To ensure accountability and audit trail. The SRO ultimately owns the overall management of risks for spend/scheme/project so must ensure risks are being managed in line with risk appetite and tolerance.
The Full FRA should be updated within 12 months of creation and/or when a "trigger" event occurs. This should be documented with appropriate sign-off.	The Full FRA is a living document that should be reviewed annually or as a result of a trigger event to ensure current and relevant risks are documented.
The Full FRA should be reviewed, challenged and approved by an Accountable Board Member/SRO.	The SRO is the ultimate decision maker in taking decisions to manage the fraud risks including requesting further action. This should be recorded and be open to, and be able to withstand robust challenge and justify the rationale should a fraud risk materialise.
Both internal and external risk should be considered.	Fraud can be perpetrated by anyone. Employees, those connected with employees, contractors, and any third party contractors should all be considered as potential 'actors' when identifying fraud risks. There is no such thing as 'trusted partners'.
The Full FRA should be presented in a way to suit the organisation's needs.	A comprehensive Full FRA layout considers the specific spend/scheme/project end-to-end process to ensure that the Full FRA is the best fit and provides context of risks and controls and any additional information/data that may inform the assessment.

Fraud Risks	Why / Reasoning
Fraud risks should be identified using a clear methodology.	To ensure that the set of fraud risks identified is as comprehensive as possible.
Individual fraud risks should have a Risk ID.	To enable easy referencing when referring to a particular risk.
Risk actor(s), action and outcome should be clearly defined.	Demonstrates the fraud offence by defining the person, people or groups committing the fraud, what they are doing, and the impact.
Duplicated fraud risks should be considered and recorded (same Action by different Actor.	It is important to list these individually even if they only have minor differences as these would require different controls (e.g. for internal or external Actors) which would in turn affect the residual risk and the scoring.
Each fraud risk should have a Risk Owner.	This creates accountability and the risk owner will be responsible for resourcing any mitigations/controls required to manage the risk.
Fraud risks are relevant to the spend/ scheme/project type.	Fraud risks likely to occur have been considered for the type of spend, end-to-end process etc.

Control Environment	Why / Reasoning
Controls should be clearly identified and detailed.	Helps to identify what they do and do not do (weaknesses and limitations).
Controls should be clearly categorised.	Helps to identify the types of control categories (deterrent, directive, preventative, detective and corrective), any gaps in control types and can help with scoring and rationale.
Controls should be specific to the risk and currently in operation.	Otherwise, they will have no effect/not be effective. Planned or aspirational controls are not currently "live" and therefore do not mitigate or control the risk, and should not be included in the control description.
Limitations must be described for each control identified	To provide a full picture of how that control affects that risk, and in what circumstances (if any) that control does not affect that specific fraud risk (what it does and does not do in relation to that risk).
Controls should apply to the specific fraud risk being assessed.	The controls should be relevant to the actual spend/scheme/project risks and be reassessed following any ‘trigger events’ such as a significant change to spend profile, changes in control framework, or fraud risks materialising as well as changes in services, systems, or structures.

Residual Risk	Why / Reasoning
The residual risk remaining despite the controls in place should be clearly identified and described.	This is central to the Full Fraud Risk Assessment and describes how a particular fraud risk can still happen with the controls in place.
The assessment of the residual risk must align with and be consistent with the analysis of the controls.	Residual risk can only be understood if it is constructed upon sound evidence of the controls in place and the effect they have on a specific fraud risk.
The residual risk should describe the limitations/weaknesses of the controls that would allow fraud to happen and consider how controls might be circumvented	This provides the risk owner with a clear understanding of the gaps (or vulnerabilities) that allow fraud to happen.

Scoring of Inherent[15] and Residual Risk	Why / Reasoning
A scoring matrix should be used.	This allows for clear scoring parameters and consistency.
Residual risks should be scored and recorded.	To identify how fraud could still happen, how likely a fraud risk will materialise and the extent to which it will result in negative outcomes. This will assist the risk owner prioritise risks for consideration in relation to the four Ts (Tolerate, Treat, Transfer, Terminate) and to evaluate the effectiveness of controls.
Likelihood (occurrence and frequency) should be recorded for each risk.	To help prioritise risks.
Impact (duration and materially) should be recorded for each risk.	To help prioritise risks.
The risk scores should be explained with clear rationale.	To ensure that the thought processes and supporting evidence used by the fraud risk assessor wh en scoring a residual risk are transparent and understood by anyone reading the Full FRA.
Inherent and residual risks should be clearly identified.	To support risk owners and SROs to understand the difference and be able to understand the effect that the controls are having on a particular risk. This will help with risk prioritisation. Visual aids such as heatmaps can help illustrate this difference e.g. showing the effect that controls have on a risk by tracing its movement between different segments on the heatmap.
The effectiveness of controls (what it does and does not do, limitations and weaknesses) should be assessed and recorded.	To help understand the difference between the inherent and residual risk and the impact that the controls in place have on the inherent risk to arrive at a score for residual risk. This also assists in identifying what four Ts (Tolerate, Treat, Trasnfer, Terminate) action is appropriate)

[15] Note - scoring of Inherent risk is currently optional for Full FRAs.

Actions (Tolerate, Treat, Transfer, Terminate and Risk Owner Decision)	Why / Reasoning
Risk owner agrees accountability for the risk.	Risk owners are managing the risk and agree they own the risk, so should have a clear understanding of risk and controls and whether the residual risk is being tolerated or not.
"Tolerate" decisions should be clearly justified.	Risk owner should provide clear explanation aligned to risk appetite and tolerance to explain why they are tolerating this risk. This explanation should withstand robust challenge, should a fraud risk materialise.
Treat, Transfer or Terminate decisions should be accompanied by specific actions to achieve this.	If risk cannot be tolerated (i.e. does not align to risk appetite or tolerance) the risk owner should identify and be accountable for any further action required to mitigate the residual risk within tolerance, whilst representing value for money (cost vs. benefit).

Governance	Why / Reasoning
The FRA should be reviewed, challenged and approved by an Accountable Board Member/SRO.	This provides accountability. The SRO is the ultimate decision maker in taking decisions to manage the fraud risks including requesting further action. These decisions should be recorded and be open to, and be able to withstand robust challenge should a fraud risk materialise.
Differences of opinion should be recorded.	The risk assessor and business unit or others may have a differing view. Decisions should be recorded when they occur and be open to robust challenge and be open to, and able to withstand, robust challenge should a fraud risk materialise.

After the Full Fraud Risk Assessment

Review and updates

Full Fraud Risk Assessments are live documents and should be kept up to date over the lifetime of the spend, scheme or project. Reviews and updates should take place at regular intervals and in response to trigger events mentioned previously. These might include when the project or spend moves into a new phase, where there are changes in the supply chain or customer base, new legislation or guidance, or frauds observed in other areas which might be a risk to the current project or spend. Where there are significant changes, this might result in changes to the risk tolerance. This should be put through the appropriate governance and if necessary highlighted to your audit and risk committee.

Keeping the Full Fraud Risk Assessment current allows the SRO to be assured that fraud risk is being managed to protect public funds and ensure that resources are spent on delivering public services.

> Full Fraud Risk Assessments should be regularly updated to ensure fraud risks are managed effectively, protecting public funds and ensuring resources are used for public services

Assurance

The PSFA undertakes assurance of FRAs in line with Government Functional Standard GovS 013: Counter Fraud. A Continuous Improvement Assessment Framework is used to conduct the Functional Standard Assurance process[16] and a FRA Assurance Framework. Assurance may also be provided by a range of other HMG organisations including the Government Internal Audit Agency.

HM Government

Government Functional Standard

GovS 013: Counter Fraud

Management of counter fraud, bribery and corruption activity

Version: 2.0
Date issued: August 2021

Approved

[16] https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud

Full Fraud Risk Assessment as Part of the Wider Fraud Risk Assessment Approach[17]

The levels of fraud risk assessment 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.

There are four levels of Fraud Risk Assessment (FRA):-

Organisational (Enterprise)

The Organisational (Enterprise) level gives an overview of the main fraud risks the organisation faces.

Thematic (Grouped)

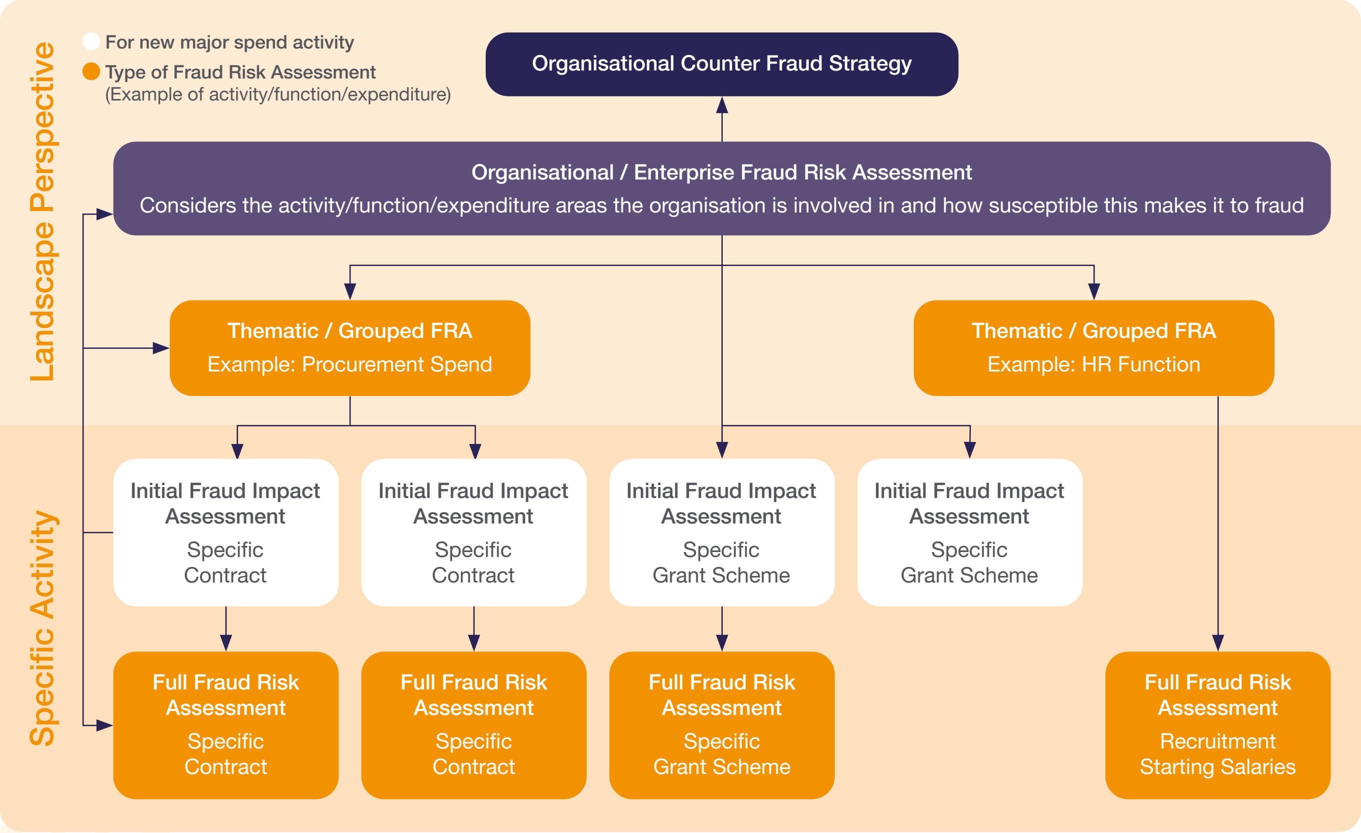
The Thematic (Grouped) level focuses on areas of spend or various programmes across the organisation, depending on its operations and structure.

Initial Fraud Impact Assessment (IFIA)

An IFIA provides an initial upfront focus of the main fraud impacts and challenges facing a new spend activity.

Full Fraud Assessment (FRA)

A Full FRA would focus on, and provide a detailed analysis of, specific fraud risks within an individual spend activity, business unit or programme.



Landscape Perspective

Specific Activity

○ For new major spend activity

● Type of Fraud Risk Assessment (Example of activity/function/expenditure)

Organisational Counter Fraud Strategy

Organisational / Enterprise Fraud Risk Assessment
Considers the activity/function/expenditure areas the organisation is involved in and how susceptible this makes it to fraud

Thematic / Grouped FRA
Example: Procurement Spend

Thematic / Grouped FRA
Example: HR Function

Initial Fraud Impact Assessment
Specific Contract

Initial Fraud Impact Assessment
Specific Contract

Initial Fraud Impact Assessment
Specific Grant Scheme

Initial Fraud Impact Assessment
Specific Grant Scheme

Full Fraud Risk Assessment
Specific Contract

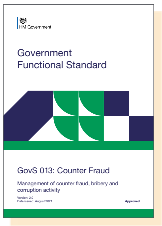
Full Fraud Risk Assessment
Specific Contract

Full Fraud Risk Assessment
Specific Grant Scheme

Full Fraud Risk Assessment
Recruitment Starting Salaries

[17] https://www.gov.uk/government/publications/professional-standards-and-guidance-for-fraud-risk-assessment-in-government

Further Information


HM Government

Government Functional Standard

GovS 013: Counter Fraud

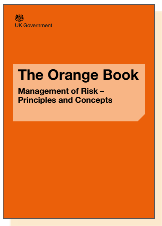
Management of counter fraud, bribery and corruption activity

Version: 2.0
Date issued: August 2021

Approved

Government Functional Standard GovS 013: Counter Fraud

https://www.gov.uk/government/publications/government-functional-standard-govs-013-counter-fraud

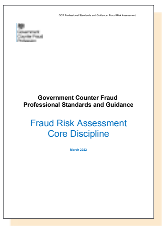

UK Government

The Orange Book

Management of Risk – Principles and Concepts

The Orange Book Management of Risk – Principles and Concepts

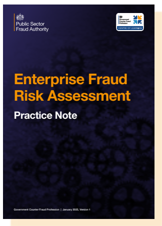
https://www.gov.uk/government/publications/orange-book


Government Counter Fraud Professional Standards and Guidance

Fraud Risk Assessment Core Discipline

Government Counter Fraud Professional Standards and Guidance Fraud Risk Assessment Core Discipline

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


Public Sector Fraud Authority

Enterprise Fraud Risk Assessment

Practice Note

Enterprise Fraud Risk Assessment Practice Note

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

Public Sector Fraud Authority

Initial Fraud Impact Assessment (IFIA)

Practice Note

Initial Fraud Impact Assessment Practice Note

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