



Public Sector
Fraud Authority

Government
Counter Fraud
Profession



CENTRE OF LEARNING

Enterprise Fraud Risk Assessment

Practice Note

Contents

1	Purpose and Scope	1
2	What is an Enterprise Fraud Risk Assessment?	2
3	Defining Fraud Risks, Threats and Drivers	4
4	How to Present Assessed Impacts of Risk	5
5	How Detailed Should the EFRA Be?	7
6	How EFRAs are Built	9
7	How to Visually Present Your EFRA	11
8	EFRA as Part of the Wider Fraud Risk Assessment Approach	13
9	Further Information	14

Purpose and Scope

This guide 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 agreed standards for professionals produced by the GCFP and is aimed at counter fraud professionals with responsibility for overseeing the counter fraud function within their department or organisation, and those responsible for the completion of **Enterprise (Organisational) Fraud Risk Assessment**.

Fraud against the public sector is a crime that affects everyone. It is often underestimated and underreported and includes a wide range of risks which can have major consequences, with the cost of fraud and error in public spending estimated to be between £55-£81 billion.¹ This represents a considerable loss of funds meant for public services and causes significant reputational damage.

All organisations are vulnerable to fraud and in order to effectively manage the risks, **it is crucial for all boards² and senior leaders to understand the fraud landscape of their organisations and focus on key areas to mitigate and manage the fraud risks they are faced with.** The Enterprise Fraud Risk Assessment (EFRA) provides organisations with a product that enables them to understand their risk and prioritise their actions.

Until the introduction of the GCFP Fraud Risk Assessment Standard and Government Functional Standard GovS013 - Counter Fraud, there were no common definitions across the public sector for fraud risk or threat, nor a common approach or structure to fraud risk assessments.

The Government Functional Standard GovS 013: Counter Fraud Section 5.1 states;³

“The organisation should undertake varying levels of risk assessments including:

A high-level fraud, bribery and corruption risk assessment that gives an overview of the main risks and challenges facing the organisation to the board or executive risk committee.”

This is the Enterprise Fraud Risk Assessment.



This Practice Note brings together leading practice from across the public sector and provides guidance on Enterprise Fraud Risk Assessments and what to include in them

1 <https://www.nao.org.uk/overviews/the-impact-of-fraud-and-error-on-public-funds-2023-24>

2 https://assets.publishing.service.gov.uk/media/5a747d24e5274a7f9902893d/PU2077_code_of_practice_2017.pdf

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

What is an Enterprise Fraud Risk Assessment?

An Enterprise Fraud Risk Assessment (EFRA) is a senior engagement tool which helps counter fraud professionals explain the importance of addressing fraud to senior management and stakeholders who may not be fraud specialists. An EFRA highlights the main fraud risks that the organisation faces, and that the board should be concerned with, to drive focus and direct resources to mitigate these risks.

An Enterprise Fraud Risk Assessment is the most general level of fraud risk assessment, looking at the organisation as a whole and how susceptible to fraud it may be across all of its business activities.

Since each organisation is unique, an EFRA will be different for each organisation.

An EFRA should be customised to the organisation, its people, and its operations. It should use the language of the organisation and be adapted to align to its objectives.

“An Enterprise Fraud Risk Assessment is a senior management engagement tool which draws from other risk assessments to identify the biggest fraud risks to an organisation and directs resources to mitigate these risks”

An EFRA should be customised to the organisation, its people, and its operations



An Enterprise Fraud Risk Assessment should include the following elements:

- ✓ **Structure:** Organise the EFRA by key schemes, business areas, or cross-cutting risks. Ensure each risk has a clear owner, no matter the structure used.
- ✓ **List of Main Specific Fraud Risks:** Identify the main fraud risks the organisation faces.
- ✓ **Risk Owners:** Assign owners for the main risks. The counter fraud leader should not be the risk owner. Instead, risk owners should work in the department where the risk exists and have enough seniority to implement necessary controls and changes. They should not be the risk assessor.
- ✓ **Evidence-Based Residual Risk Assessment:** Provide an evidence-based assessment of residual risk.
- ✓ **Scale of Impact and Financial Loss:** Where possible assess the potential impact and financial loss specific to the organisation arising from the main risks. This assessment should include data on both detected and undetected fraud and errors related to these risks.
- ✓ **Risk Management Options:** Indicate if risks are being tolerated, treated, terminated or transferred.⁴
- ✓ **Summarise the Key Ongoing Activities:** Summarise key actions across the business for treating risks and clearly identify the owners of the actions.
- ✓ **Drivers of Risks:** Describe the key drivers of fraud risk for the organisation and how they currently affect and will continue to affect the overall level of risk. For example, a driver could be an important supplier not receiving an increase in their contract or instability in the industry/sector.
- ✓ **Areas of Uncertainty:** Clearly indicate where information is not available or has not been reviewed.
- ✓ **Approval Details:** Note who approved the EFRA, the date of approval, and the mechanism used (e.g. which board or governance forum).
- ✓ **Review Period:** An EFRA must be time-limited, updated at least annually, and should consider all new or recent fraud risk assessments.

Key Considerations for an Enterprise Fraud Risk Assessment:

- ✓ **Avoid being overly detailed:** Be clear and succinct.
- ✓ **Counter fraud teams should not be risk owners:** Counter fraud team members can suggest potential controls to mitigate fraud risks.
- ✓ **Base assessments on evidence:** Not opinion or anecdotal evidence.
- ✓ **Do not treat the EFRA as a one-off task:** It should be ongoing.
- ✓ **Avoid using a generic scoring matrix:** Define the scoring matrix to make it unique and meaningful to the organisation.
- ✓ **Ensure an EFRA is carried out by counter fraud experts.**
- ✓ **Where evidence is limited** of the scale of a risk, comparators from other organisations, sectors or countries should be used.

4 N.B. reputational impact of fraud cannot be transferred.

Defining Fraud Risks, Threats and Drivers⁵

To understand Enterprise Fraud Risk Assessments and all FRAs, it is important to know what is meant by risk.

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



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

Example:

Under increasingly difficult market conditions (driver), 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 reduced public trust in the agency (impacts).



How to describe risks in Risk Assessments - Actor, Action, Outcome:

Fraud risks must be clearly described and should be documented using the following structure:

- **Actor:** Who commits the fraud (may be an individual or multiple 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.

⁵ See "Definitions" in GCFP Fraud Risk Assessment Standard.

How to Present Assessed Impacts of Risk

Enterprise fraud risk assessments draw information directly from the other levels of fraud risk assessments used in the wider organisation approach. A decision needs to be made on how best to present enterprise fraud risk, and the wider organisational fraud risk assessment approach will influence this. For example:

- If there are strong Thematic Fraud Risk assessments (TFRAs) in place, then a “middle out” approach where the TFRAs are the key input for the EFRA should work well. Where TFRAs are not part of the approach, but there is comprehensive coverage through full Fraud Risk Assessments (FRAs), then full FRAs should drive the EFRA based on assessed residual risks.
- Where organisations are less mature and looking to do a top down approach, then basing the EFRA on Initial Fraud Impact Assessments (IFIAs) can be effective as a starting point.
- Regardless of which approach is chosen, the EFRA should be drawn from assessed fraud risks.

Scoring

When using the middle out and bottom up approach 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.

With all approaches, organisations will need to provide a scoring mechanism that is appropriate for their organisation, and definitions must be provided to allow the assessor to allocate a score appropriately and consistently.



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.

How Detailed Should the EFRA Be?

The EFRA serves as a senior engagement tool, providing sufficient information to enable informed decision making about risk management, resource allocation, and capability enhancement. To make the EFRA impactful for the board:

- **Executive Summary** - Provide a narrative that summarises the main fraud risks and highlights where resources are needed most, supported by detailed evidence in an annexe.
- **Present Evidence and Examples** - Use specific cases, figures, statistics, and intelligence from horizon scanning to illustrate points.
- **Fraud Risk Register** - Maintain a fraud risk register that underpins the EFRA, ensuring that all identified fraud risks are documented and tracked.

The more specific the detail contained in the EFRA, the more impactful the risk assessment will be. However, this must be reconciled with the difficulty of managing a large number of risks. The skill of the Enterprise fraud risk assessor is in structuring the EFRA to balance the level of detail with the need to make it engaging for stakeholders.

By presenting a well rounded EFRA, the board can better understand the organisation's fraud risk landscape and make strategic decisions to mitigate these risks effectively.

Effective engagement and communication are crucial for the successful completion of an Enterprise Fraud Risk Assessment. It is important to convey to the organisation's board how addressing the fraud risk is beneficial, as it allows the organisation to take appropriate action and focus on core functions.

The EFRA deals with complex and varied risks. The goal is to simplify these complexities and tailor the communication to the specific needs of the organisation. Use language that the organisation's board understands, clearly explaining what can and cannot be done due to losses from fraud. Emphasise why the organisation's board should allocate resources to areas where fraud has not yet occurred but could potentially arise.

As a counter fraud professional, your insights are invaluable. If you foresee a potential risk, it is important to frame this in a way your organisation's board will understand, using reasoning and examples of where similar risks have materialised before. External comparisons with similar organisations that have experienced similar risks and the impacts can help illustrate the likelihood of these risks. Horizon scanning, intelligence, and analysis should feed into the EFRA, providing a broader context for the board. Communicating specific risks clearly enables the organisation's board to take action where appropriate.




By framing the discussion in terms of tangible impacts such as the impact on reputation or service delivery, the board will better understand the fraud risk and its implications for the organisation's overall success. This approach can help the organisation's board to be fully engaged and responsive to the identified fraud risk.

The approach to presenting the results of the EFRA must capture the board's attention by highlighting key areas of concern for example;

- **Risk Areas** - What specific risks should the board be worried about?
- **Fraud Threat Dynamics** - Is the threat of fraud increasing or decreasing? What are the drivers behind these changes?

By presenting a well-structured EFRA, tailored to the needs and understanding of the board, you can effectively communicate the importance of proactive fraud management and the rationale behind resource allocation decisions. This approach ensures that the board is well informed and equipped to take strategic actions against fraud risks.

An Enterprise level FRA must be time limited. It should be updated at least annually, and take into account recent Initial Fraud Impact Assessments. It should also be updated following any "trigger event" as defined by the organisation - including any material or structural change to the organisation. 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.



The approach to presenting the results of the EFRA must capture the board's attention by highlighting key areas of concern

How EFRAs are Built⁶

A well developed Enterprise Fraud Risk Assessment should be constructed from Thematic (Grouped) FRAs, IFIAs and full FRAs 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
- 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



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?

Enterprise Fraud Risk Assessments built from Thematic (Grouped) FRAs, Full FRAs and IFIAs may also include:

- key identified threats
- a summary of key identified control weaknesses in the area
- a summary of the identified potential fraud impacts
- any areas of uncertainty where information was not available at the time of assessment

These lists are not exhaustive and the content of the EFRA should be tailored to your specific board and organisation's needs

⁶ <https://assets.publishing.service.gov.uk/media/625fd0e0d3bf7f600782fdcb/Fraud-Risk-Assessment-Standards-2022-03-25.pdf>

An EFRA which is not built from the other assessments (i.e. from the top down approach), should include coverage of⁷:

- 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 in foreign countries, if so include fraud indices of the relevant country/countries
- who the organisation's customers are and what their normal attributes are
- 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
- what previous audits and audit reports have indicated



How to Visually Present Your EFRA

To drive engagement from your board, the key consideration for design is to select the language and structure that are most likely to resonate **within your organisation**.

An EFRA should highlight specific risks. To help with the creative process, two example presentation options that include key information to present to the board are detailed below:

Option 1 is where the top risks are presented by Business Area - which may work well if you are drawing insight primarily from Full FRAs (the “bottom up” approach):

Presentation of an EFRA

Department for Fictional Examples⁸

Option 1 - By Business Area

Stairlift Scheme Risk Owner **Jake Burton**

Known Fraud and Error 23/24 £1.5m, Estimated Fraud and Error £20m - £30m per year

Top Residual Fraud Risks

1. Application false declaration of earnings - Score 22 (V High) - Decision = Treat
2. Contractor invoices for approved model installs sub-standard one - Score 19 (High) Decision = Treat
3. Contractor invoices the applicant and the department - Score 18 (High) Decision = Treat

Mobility Scooter Scheme.....Risk Owner **Oscar Ahmed**

Known Fraud and Error 23/24 £1.1m, Estimated Fraud and Error £14m - £17m per year

Top Residual Fraud Risks

1. Contractor submits invoice for scooter not purchased - Score 20 (V High) Decision = Treat
2. Applicant forges medical evidence to prove eligibility - Score 18 (High) - Decision = Tolerate
3. External actor uses stolen ID to create false claims - Score 16 (High) - Decision = Treat

Free Prescriptions Scheme.....Risk Owner **Mia Power**

Known Fraud and Error 23/24 £800k, Estimated Fraud and Error £8m - £11m per year

Top Residual Fraud Risks

1. Contractor submits inflated invoice - Score 20 (V High) - Decision = Treat
2. Applicant false declaration of capital - Score 16 (High) - Decision = Treat
3. Applicant false declaration of age - Score 14 (Medium) - Decision = Tolerate

Key Cross-Cutting Fraud Risks

- False Declaration of Income
- Contractor False Invoicing
- External actor identity takeover

Drivers of Fraud Risk

- Increased costs of living
- Negative press coverage for the department
- Challenging market conditions for suppliers

It is Important to Track Actions on All Risks with Treat Decision

8 Fictional example for illustrative purposes only.

Option 2 is where the top risks are presented by Cross-Cutting Risk. This may work well when you are drawing insight primarily from TFRAs (the “middle out” approach):

Presentation of an EFRA

Department for Fictional Examples⁹

Option 2 - By Cross-Cutting Risk

Applicant false declaration of income

Known Fraud and Error 21/24 £2.5m. Residual Risk Score 22 (V High) - Decision = Treat

Top Schemes Affected

1. Stairlift Scheme - Risk Owner **Jake Burton**
2. Mobility Scooter Scheme - Risk Owner **Oscar Ahmed**
3. Winter Fuel Payment - Risk Owner **Eloise Freeman**

Contractor false invoicing

Known Fraud and Error 23/24 £1.6m. Residual risk Score 21 (V High) - Decision = Treat

Top Schemes Affected

1. Stairlift Scheme - Risk Owner **Jake Burton**
2. Mobility Scooter Scheme - Risk Owner **Oscar Ahmed**
3. Free Prescription Scheme - Risk Owner **Mia Powar**

External actor identity takeover

Known Fraud and Error 23/24 £400k. Residual risk Score 20 (High) - Decision = Treat

Top Schemes Affected

1. Stairlift Scheme - Risk Owner **Jake Burton**
2. Mobility Scooter Scheme - Risk Owner **Oscar Ahmed**
3. Winter Fuel Payment - Risk Owner **Eloise Freeman**

Key Schemes Impacted by Fraud and Error

- Stairlift Scheme - estimated £20m per year
- Mobility Scooter Scheme - estimated £16m per year
- Free Prescriptions Scheme - estimated £8m per year

Drivers of Fraud Risk

- Increased cost of living
- Negative press coverage for the department
- Challenging market conditions for suppliers

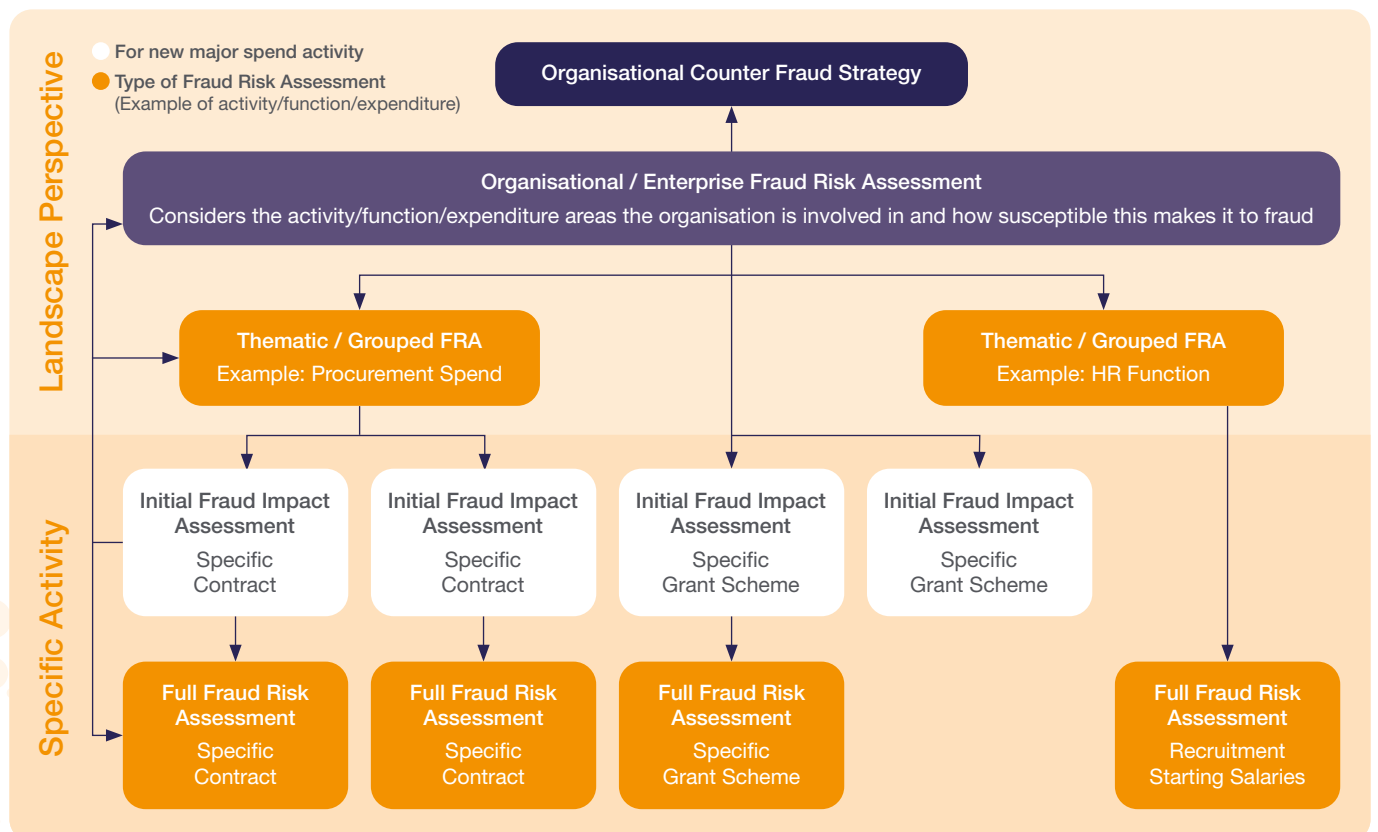
It is Important to Track Actions on All Risks with Treat Decision

EFRAs as Part of the Wider Fraud Risk Assessment Approach¹⁰

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



10 <https://assets.publishing.service.gov.uk/media/625fd0e0d3bf7f600782fdcb/Fraud-Risk-Assessment-Standards-2022-03-25.pdf>

Further Information

Fraud Risk Assessment Standard

<https://assets.publishing.service.gov.uk/media/625fd0e0d3bf7f600782fdcb/Fraud-Risk-Assessment-Standards-2022-03-25.pdf>

Initial Fraud Impact Assessment Practice Note

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

Government Functional Standard GovS 013: Counter Fraud

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

The Government Counter Fraud Functional Strategy 2024-2027

<https://assets.publishing.service.gov.uk/media/65f01d1f9812270011f61283/Cross-Government-Counter-Fraud-Functional-Strategy-2024-2027.pdf>

Commonwealth Fraud Prevention Centre - Fraud Risk Assessment Guidance and Tools

<https://www.counterfraud.gov.au/library/fraud-risk-assessment-guidance-and-tools>

National Audit Office-Tackling fraud and corruption against government

<https://www.nao.org.uk/wp-content/uploads/2023/03/tackling-fraud-and-corruption-against-government.pdf>

Corporate governance in central government departments: code of good practice

https://assets.publishing.service.gov.uk/media/5a747d24e5274a7f9902893d/PU2077_code_of_practice_2017.pdf