

# Public Document Pack



Neuadd y Sir  
Y Rhadyr  
Brynbuga  
NP15 1GA

County Hall  
Rhadyr  
Usk  
NP15 1GA

Wednesday, 8 January 2025

## Notice of Reports Received following Publication of Agenda.

### Governance and Audit Committee

Thursday, 16th January, 2025 at 2.00 pm,  
County Hall, The Rhadyr, Usk, NP15 1GA

Attached are reports that the committee will consider as part of the original agenda but were submitted to democratic services following publication of the agenda.

Item No	Item	Pages
7.	Anti Fraud, Bribery and Corruption Risk Assessment	1 - 42

**Paul Matthews**  
Chief Executive

This page is intentionally left blank



**SUBJECT: MONMOUTHSHIRE COUNTY COUNCIL  
COUNTER FRAUD, CORRUPTION &  
BRIBERY RISK ASSESSMENT**

**DIRECTORATE: Resources**  
**MEETING: Governance & Audit Committee**  
**DATE: January 2025**  
**DIVISION/WARDS AFFECTED: All**

## 1. PURPOSE

- 1.1 To consider the adequacy and appropriateness of Council's first Counter Fraud, Corruption and Bribery Risk Assessment.

## 2. RECOMMENDATION(S)

- 2.1 That the Governance and Audit Committee comments on and endorses the Council's Counter Fraud, Corruption and Bribery Risk Assessment.
- 2.2 The Governance & Audit Committee recognises the Council's commitment to a zero tolerance approach to Fraud, Corruption and Bribery and requires that all Members, Lay Members and Officers of the Council complete the required e-Learning in this area as soon as possible and at the latest by the end of June 2025.
- 2.3 That the Governance and Audit Committee receive an updated report and assessment during the 2025/26 financial year (September 2025).

## 3. KEY ISSUES

- 3.1 Fraud is considered a significant risk to the public sector and various estimates have been made as to the total loss to the public purse. However, it is clear that financial losses due to fraud diverts funds from essential services and may also result in reputational damage and loss of confidence.
- 3.2 Monmouthshire County Council has a zero-tolerance culture and attitude to fraud, bribery, and corruption.
- 3.3 In accordance with the Council's Risk Appetite Statement, Monmouthshire County Council is 'risk averse' when it comes to fraud, bribery and corruption.
- 3.4 The purpose of the Risk Assessment is to systematically identify, assess, and mitigate potential fraud risks within the Council's operations, ensuring the integrity and trust in public services. It will encompass all departments and activities like procurement, grant allocations, and service delivery.

3.5 This assessment is designed to safeguard the resources and reputation of Monmouthshire County Council complementing the Anti-Fraud, Corruption and Bribery Policy which was approved by Cabinet in January 2024.

#### **4. REASONS**

4.1 The Auditor General for Wales in 2019 noted that the sums lost annually in the Welsh public sector to fraud and error are significant – and could be anywhere between £100 million and £1 billion.

4.2 Fraudsters are becoming more sophisticated and evaluating opportunities and risks in real time. New fraud threats are continually emerging, both globally and nationally.

4.3 The Auditor General released a report in July 2020, [‘Raising Our Game’ Tackling Fraud in Wales](#), requiring public sector bodies to ensure that their arrangements for preventing and detecting fraud are effective. This Risk Assessment is part of our response to this report.

4.4 In addition to completion of the Risk Assessment, as part of the restructure of the Internal Audit team in April 2024, it was agreed that a Counter Fraud Officer position would be added to the structure. This has been recruited to and forms another part of our response.

4.5 Local Government Employees have a range of powers and functions, from licensing and housing to awarding contracts for local amenities. It makes them targets for people and organisations who seek to either gain an unfair advantage or are looking to exploit information they hold.

4.6 An e-Learning module covering Fraud, Corruption and Bribery has been developed by the Chief Internal Auditor for the Council’s Thingi learning management system. It has been deemed necessary to mark the completion of this module as being mandatory for all Members and Officers of the Council. The completion of the module will be monitored and reported to the Senior Leadership Team. Completion statistics will be reported to the Governance & Audit Committee within the Internal Audit End of Year report (May 2025).

4.7 The Fraud Risk Assessment has identified the key areas of potential fraud and the mitigations to reduce the risk of fraud. These are included within the Fraud Risk Register as detailed in Appendix 1 of the document.

4.8 Monmouthshire County Council will continue to take an active role in the National Fraud Initiative, conducting investigations and recording outcomes where necessary. MCC and its Senior Leadership Team are fully committed to the NFI process.

4.9 The Audit Wales National Fraud Initiative Self-Appraisal Checklist has been completed (Appendix 2) and actions highlighted to improve the Council’s work in this area.

- 4.10 An Action Plan (Appendix 3) has been developed to improve Monmouthshire County Council's response to Fraud, Corruption & Bribery.
- 4.11 The Fraud Risk Register and Action Plan will be reviewed and updated regularly, and an annual report will be presented to the Governance and Audit Committee in accordance with the Council's Counter Fraud, Corruption and Bribery Policy. As this is a major review of the current arrangements an additional interim review and report will be presented to the Committee during the year.

## **5. RESOURCE IMPLICATIONS**

Internal Audit team resource in proactively investigating allegations and data matches resulting from the National Fraud Initiative.

## **6. CONSULTEES**

Acting Chief Executive & Chief Officer – Resources  
Head of Finance (Acting S151 Officer)  
Performance & Data Insight Manager

## **7. BACKGROUND PAPERS**

MCC Counter Fraud Risk Assessment  
MCC Fraud Risk Register  
Audit Wales National Fraud Initiative Self-Appraisal Checklist

## **8. AUTHOR AND CONTACT DETAILS**

Jan Furtek, Acting Chief Internal Auditor  
Telephone: 01600 730521  
Email: [janfurtek@monmouthshire.gov.uk](mailto:janfurtek@monmouthshire.gov.uk)



monmouthshire  
sir fynwy

# FRAUD, CORRUPTION & BRIBERY RISK ASSESSMENT

DECEMBER 2024

Date of Report Issue

12<sup>th</sup> December 2024

Report Status

Draft v5

Report Author(s)

Jan Furtek, Acting Chief Internal Auditor

Page 4



## 1. Introduction

- 1.1 Fraud is considered a significant risk to the public sector and various estimates have been made as to the total loss to the public purse. However, it is clear that financial losses due to fraud diverts funds from essential services and may also result in reputational damage and loss of confidence.
- 1.2 **Monmouthshire County Council has a zero-tolerance culture and attitude to fraud, bribery, and corruption.**
- 1.3 Monmouthshire County Council commits to investigating all allegations of Fraud, Corruption and Bribery at all levels of the organisation. This will include actions being taken under the Council's disciplinary policy and referrals to the Police and external regulators when necessary. The Council will look to recover all money and assets subject to proven fraudulent processes.
- 1.4 In accordance with the Council's Risk Appetite Statement, Monmouthshire County Council is 'risk averse' when it comes to fraud, bribery and corruption.
- 1.5 The purpose of this document is to systematically identify, assess, and mitigate potential fraud risks within the Council's operations, ensuring the integrity and trust in public services. It will encompass all departments and activities like procurement, grant allocations, and service delivery.
- 1.6 Local Government Employees have a range of powers and functions, from licensing and housing to awarding contracts for local amenities. It makes them targets for people and organisations who seek to either gain an unfair advantage or are looking to exploit information they hold.
- 1.7 Members of the public and suppliers of the Council may seek to obtain an unfair advantage or personal gain through defrauding Monmouthshire County Council. We commit to investigating all instances and are dedicated to data matching exercises such as the National Fraud Initiative.
- 1.8 This assessment is designed to safeguard the resources and reputation of Monmouthshire County Council complementing the Anti-Fraud, Corruption and Bribery Policy which was approved by Cabinet in January 2024.

## 2. Risk Identification

Including but not limited to:

### 2.1 Internal Risks:

- *Employee Fraud*: Unauthorized use of funds, manipulation of financial records, or fraudulent expense claims, possibly motivated by financial need or opportunity.
- *Resource Misuse*: Employees using Council resources, such as vehicles or office supplies, for personal gain.
- *Conflicts of Interest*: Situations where employees have undisclosed interests in companies that are awarded contracts, leading to biased decision-making.

### 2.2 External Risks:

- *Contractor/Supplier Fraud*: Overbilling, delivering substandard goods or services, providing kickbacks, or collusion with internal staff to manipulate contract awards.
- *Beneficiary Fraud*: Individuals or organizations falsely claiming benefits, grants, or public services through deception or forged documents.
- *Cyber Fraud*: Individuals or organisations looking to illegally acquire sensitive information or monetary gain.

## 3. Risk Analysis & Fraud Risk Register

- 3.1 It is intended that this initial risk register, its findings and methodology will be, from the 2025/26 financial year, embedded into individual Service Business Plans across the Council. These plans will be aligned to this risk assessment, with service managers encouraged to consider fraud, corruption and bribery when completing their service risk register. Information included in service plans will then help inform the MCC fraud risk register and also the annual Internal Audit Plan.
- 3.2 A copy of the Fraud Risk Register can be found as Appendix 1 to this report. All risks identified have been assessed against;
- 3.3 **Likelihood**: Measured as, unlikely, possible, likely, almost certain based on historical data, trends, expert judgment and time.
- 3.4 **Impact / Consequence**: Assesses the potential consequences of each risk. For example:
- a. *Financial Loss*: Quantify the possible monetary loss.
  - b. *Reputational Damage*: Evaluate the impact on public trust and confidence.



- c. *Operational Disruption*: Measure the potential disruption to service delivery.

Major (4)	Low (4)	Medium (8)	High (12)	High (16)
Substantial (3)	Low (3)	Medium (6)	Medium (9)	High (12)
Moderate (2)	Low (2)	Low (4)	Medium (6)	Medium (8)
Minor (1)	Low (1)	Low (2)	Low (3)	Low (4)
	Unlikely (1)	Possible (2)	Likely (3)	Almost certain (4)

- 3.5 Risks with a score of 1-4 are considered to be low risk; a score of 6-9 is considered medium risk; and a score of 12-16 is considered to be high risk.
- 3.6 A number of control / mitigation processes including management controls and other processes have been considered for each of the identified risks, and the residual risk remaining following these mitigations is reflected in the Risk Register.
- 3.7 Fraud risk identification is essential to understand the specific exposures to different types of risk and changing patterns of threat and consequences. The risk assessment is designed to identify those areas with the greatest potential for the risk of fraud.

## 4. Control Measures

### 4.1 Preventive Controls:

- *Internal Controls*: Implement policies that define acceptable use of resources, enforce segregation of duties, and restrict access to sensitive information.
- *Regular Audits*: Schedule regular internal and external audits to review compliance and detect anomalies.
- *Due Diligence*: Conduct thorough background checks on employees and contractors.

### 4.2 Directive Controls:

- *Policies*: These dictate how certain activities should be conducted within the organization.
- *Training*: Regular training sessions to ensure that employees are aware of the policies and procedures.
- *Code of Conduct*: A set of rules outlining the responsibilities and proper practices for individuals within the organization.

- *Culture & Raising Awareness*: Regularly communicating and promoting the importance of compliance and ethical behaviour.

#### 4.3 **Detective Controls:**

- *Monitoring Systems*: Employ technology to monitor transactions and identify unusual patterns indicative of fraud.
- *Whistleblower Mechanisms*: Create confidential reporting channels for employees and the public to report suspected fraud, ensuring protection against retaliation.

#### 4.4 **Corrective Controls:**

- *Investigation Protocols*: Develop step-by-step procedures for investigating suspected fraud, including timelines and responsibilities.
- *Disciplinary Actions*: Define clear, consistent consequences for fraudulent activities, including termination of employment and legal prosecution where appropriate.

### 5. Risk Mitigation

#### 5.1 **Training and Awareness:**

- Conduct regular, mandatory training sessions for all employees on fraud awareness, detection, and prevention.
- Promote a culture of integrity, where ethical behaviour is valued and expected.

#### 5.2 **Policy Development:**

- The Council has an Anti-Fraud, Corruption and Bribery Policy which was approved by Cabinet in January 2024.
- Ensure policies are regularly reviewed and updated to reflect new risks and emerging trends.

#### 5.3 **Collaboration:**

- Partner with external bodies such as the National Fraud Initiative to share information and best practices.
- Foster relationships with other local Councils, Welsh Government and Central Government to learn from their experiences and collaborate on initiatives.

### **National Fraud Initiative**

- 5.4 The National Fraud Initiative (NFI) is a biennial UK-wide counter-fraud exercise. The NFI matches electronic data within and between public and private sector bodies to prevent and detect fraud. Monmouthshire County Council takes an active part in this exercise and has submitted data as

required in October 2024. The resulting data matches are due to be returned in January 2025 for review / investigation.

- 5.5 Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows fraudulent claims and payments to be identified. Where a match is found it indicates that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.
- 5.6 Beyond any financial savings, the benefits of participation and reviewing data matches include the assurance that NFI results can provide around systems of internal control.
- 5.7 Monmouthshire County Council has historically reported a relative low instance of fraud through these exercises. This demonstrates the strength of our internal control mechanisms, however, it is acknowledged that there is always room for improvement in this area and a full review of the 2024/25 NFI data matches will be undertaken.
- 5.8 The Council has completed the Audit Wales recommended NFI Self Appraisal Checklist (Appendix 2). Required actions have been identified through this to strengthen the usage of the NFI within Monmouthshire. These will be implemented as part of the Fraud Action Plan (Appendix 3).

## **6. Monitoring and Review**

### **6.1 Regular Assessments:**

- Schedule periodic fraud risk assessments, at least annually, to re-evaluate risks and update control measures.
- Use findings from audits and investigations to inform assessments and identify areas for improvement.

### **6.2 Continuous Improvement:**

- Incorporate lessons learned from past incidents and near-misses.
- Stay updated with emerging fraud trends and techniques through training, research, and collaboration with external partners.

## **7. Reporting**

### **7.1 Documentation:**

- Maintain detailed records of all fraud risk assessments, control measures implemented, and incidents of fraud.
- Ensure documentation is thorough and accessible for review by internal and external auditors.

## 7.2 Reporting Mechanisms:

- Establish clear, accessible channels for reporting suspected fraud internally and externally.
- Publicize reporting mechanisms widely to ensure they are trusted and utilized by employees and the public.

7.3 In accordance with the Councils Counter Fraud, Corruption & Bribery Policy. Members and Officers of the Council along with members of the public and Council suppliers are able to raise any concerns via the following methods;

- The Chief Executive, Chief Officers, Heads of Service, or the Council's Monitoring Officer, who will report such concerns to the Chief Internal Auditor;
- Directly to the Chief Internal Auditor;
- Where line management is suspected of fraud, directly to the Chief Officer or Chief Internal Auditor;
- External Auditor (Audit Wales), who, depending upon the nature of the concern will liaise with the Chief Internal Auditor;
- Trade Union Representative;
- The MCC Whistleblowing Policy.

## 8. Conclusion

- 8.1 The Fraud Risk Assessment has identified the key areas of potential fraud and the mitigations to reduce the risk of fraud. These are included within the Fraud Risk Register as detailed in Appendix 1.
- 8.2 An Action Plan (Appendix 3) has been developed to improve Monmouthshire County Councils work in this area.
- 8.3 Monmouthshire County Council will continue to take an active role in the National Fraud Initiative, conducting investigations and recording outcomes where necessary.
- 8.4 The Fraud Risk Register and Action Plan will be reviewed and updated regularly, and an annual report will be presented to the Governance and Audit Committee in accordance with the Councils Counter Fraud, Corruption and Bribery Policy. As this is a major review of the current arrangements an additional interim review and report will be presented to the Committee during the year.

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
1	HR	Authority employs worker who does not have the right to work in the UK / has provided false identification documents to demonstrate the right to work in the UK.	Ineffective pre employment checks due to lack of staff awareness / training / policies / procedures. Job advert does not state that applicants must hold the right to work within the UK.	Reputational risk. Fine from Border Agency - £60k per employee. Cost of re-running recruitment process. Cost of interim staff.	Almost Certain	4	Major	4	16	Staff training. Policies / procedures include adequate guidance. Job adverts include wording re right to work in UK. Adequate eligibility checks undertaken. Regular ongoing eligibility checks. Consider as appropriate criminal/civil proceedings.	Possible	2	Moderate	2	4	Chief Officer - People, Policy & Performance
2	HR	Authority employs worker who does not have the required experience / qualification for the role, or has provided false or misleading information e.g. false identification, employment history, qualifications.	Ineffective pre employment checks due to lack of staff awareness / training / policies / procedures.	Reputational risk. Cost of re-running recruitment process. Cost of interim staff.	Almost Certain	4	Major	4	16	Staff training. Policies / procedures include adequate guidance. 2 references obtained. Adequate I.D. checks undertaken. Adequate qualification checks undertaken. Consider as appropriate criminal/civil proceedings.	Possible	2	Moderate	2	4	Chief Officer - People, Policy & Performance

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
3	Payroll	Creation of fictitious 'ghost' employees.	Lack of oversight / segregation of duties.	Financial loss. Reputational Damage.	Likely	3	Substantial	3	9	Regular payroll internal audits. Segregation of duties upon setting up new employees on the payroll system. Regular staff budget monitoring across departments. Take appropriate action such as appropriate criminal/civil proceedings.	Unlikely	1	Minor	1	1	Chief Officer - People, Policy & Performance
4	Payroll	Unauthorised changes to payroll e.g. pay rate alteration.	Lack of oversight / segregation of duties.	Financial loss. Reputational Damage.	Likely	3	Substantial	3	9	Regular payroll internal audits. Segregation of duties for changes on payroll system. Regular staff budget monitoring across departments. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Unlikely	1	Minor	1	1	Chief Officer - People, Policy & Performance

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
5	Payroll	Prolonging the pay of a leaver and/or redirecting their pay into a fraudster's account.	Lack of oversight / segregation of duties.	Financial loss. Reputational Damage.	Likely	3	Substantial	3	9	Regular payroll internal audits. Segregation of duties throughout payroll system. Regular staff budget monitoring across departments. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Unlikely	1	Minor	1	1	Chief Officer - People, Policy & Performance
6	Procurement	Bid Rigging / Cover pricing.	Lack of competition. Insufficient oversight. Lack of training / awareness. Collusion.	Financial Loss. Reputational damage. Lack of value for money / poor goods / services.	Almost Certain	4	Substantial	3	12	Management checks. Tendering process. Well communicated financial regs / standing orders. Internal audit checks. Encourage whistleblowing.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  ARDAL Procurement Partnership

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
7	All Service Areas	False declarations of mileage expenses.	Lack of authorisation process. Lack of expenses policy.	Financial loss. Reputational Damage.	Almost Certain	4	Minor	1	4	Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing. Managers authorisation of expenses. Regular checks by Internal Audit. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Possible	2	Minor	1	2	Chief Officer - People, Policy & Performance  Strategic Leadership Team



Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
8	All Departments	False declarations of overtime hours.	Lack of authorisation process.	Financial loss. Reputational Damage.	Almost Certain	4	Moderate	2	8	Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing. Managers authorisation of overtime / additional hours. Regular checks by Internal Audit. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Possible	2	Minor	1	2	Chief Officer - People, Policy & Performance  Strategic Leadership Team

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
9	All Service Areas	Employees undertaking alternative work while sick.	Employees who are disengaged / dissatisfied at work. Lack of sickness policy / attendance monitoring. Cost of living crisis.	Financial loss. Cost of supply / cover staff. Delay / halt / decline in quality of service delivery. Reputational damage.	Likely	3	Moderate	2	6	Foster a positive work environment. Clear and well communicated sickness / managing attendance policies. Conducting regular reviews of absence patterns. Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing. NFI data matching. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Possible	2	Minor	1	2	Chief Officer - People, Policy & Performance  Strategic Leadership Team

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
10	Procurement	Bribery / kick backs for Procurement official collusion.	Financial incentives. Pressure to meet targets. Weak internal controls. Culture. Close supplier relationships.	Financial Loss. Reputational damage. Lack of value for money / poor goods / services.	Almost Certain	4	Substantial	3	12	Management checks. Tendering process. Well communicated financial regs / standing orders. Internal audit checks. Anti bribery policy. Rotation of duties Encourage whistleblowing.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  ARDAL Procurement Partnership
11	All Service Areas	Employee working for a third party on Council time.	Lack of monitoring by management. Cost of living crisis. Disengaged employees.	Reputational Damage. Poor work performance. Decline in service delivery.	Likely	3	Moderate	2	6	Regular performance monitoring. Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing. NFI data matching. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Possible	2	Minor	1	2	Chief Officer - People, Policy & Performance  Strategic Leadership Team

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
12	All Departments	Abuse of position.	Lack of management oversight. Cultural values and expectations. Bullying.	Financial losses, reputational damage, poor performance and sickness or high staff turn over. Reputational damage.	Likely	3	Moderate	2	6	Regular performance monitoring. Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing.	Possible	2	Minor	1	Chief Officer - People, Policy & Performance  Strategic Leadership Team	
13	Insurance	False insurance claims. Exaggerated insurance claims. Duplicate insurance claims.	Ineffective claim checks. Ineffective supporting evidence checks. Lack of procedures / staff training.	Financial loss. Drain on staff resource.	Almost Certain	4	Moderate	2	8	Experienced claim handlers. Rigorous authenticity checks. NFI data matching.	Possible	2	Minor	1	2 Deputy Chief Executive & Strategic Director Resources (S151 Officer)	
14	Grants	Any fraud that involves the false payment of grants, loans or financial support to any private individual, company, charity etc through fake applications / collusion.	Ineffective claim checks. Ineffective supporting evidence checks. Lack of staff training.	Financial loss. Reputational damage. Operational disruption (investigations / remedial action can divert resource away from other services / functions.	Almost Certain	4	Substantial	3	12	Educate / train staff on risks of grant fraud / ethical behaviour. Regular checks by Internal Audit. Well communicated procedures for grant distribution.	Possible	2	Minor	1	2 Deputy Chief Executive & Strategic Director Resources (S151 Officer)	

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
15	Procurement	Overcharging.	Insufficient oversight to identify inflated invoicing / falsified cost reports / unapproved charges.	Financial Loss. Reputational damage. Lack of value for money / poor goods / services.	Almost Certain	4	Substantial	3	12	Management checks / Internal Audit checks / well communicated procedures / regulations.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  ARDAL Procurement Partnership
16	Procurement	False claims and variations.	Insufficient oversight. Lack of staff awareness / training. Lack of procedures / regulations.	Financial Loss. Reputational damage. Lack of value for money / poor goods / services.	Almost Certain	4	Substantial	3	12	Management checks / Internal Audit checks / well communicated procedures / regulations.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  ARDAL Procurement Partnership
17	All Service Areas	Theft of Council information / intellectual property.	Insufficient cyber security measures. Phishing attacks. Employees misconduct. Lack of training / awareness. Inadequate security / access controls. Out of date software.	Financial loss. Reputational damage. Large fines / sanctions.	Likely	3	Major	4	12	Security policy. Restricted access to buildings. Encryptions. Password controls. Access controls. Staff awareness / training.	Possible	2	Major	4	8	Strategic Leadership Team  Heads of Service  Head of Info Technology & Security

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
18	Procurement	Cheaper materials substituted for those specified in contracts. The use of sub-standard materials may also carry health and safety risks and environmental risks.	Lack of sufficient checks. Lack of staff awareness / training / procedures / regulations.	Financial Loss. Reputational damage. Lack of value for money / poor goods / services. Fines / sanctions.	Almost Certain	4	Substantial	3	12	Management checks / Internal Audit checks / well communicated procedures / regulations. Inspections of materials.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  ARDAL Procurement Partnership
19	Finance	Bank mandate fraud.	Lack of staff awareness / training / procedures for dealing with requests to change supplier bank details.	Financial loss. Reputational damage.	Almost certain	5	Major	4	20	Staff awareness - emails / training.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)
20	Finance	Treasury management unauthorised investments and loans.	Lack of policies and procedures, lack of training. Lack of segregation of duties. Poor authorisation controls and inappropriate access to banking and finance systems.	Financial loss, possibly high value. Reputational damage.	Almost Certain	4	Major	4	16	Robust policies, strict access controls segregation of duties and authorisation policies. Regular Internal Audit reviews.	Likely	3	Substantial	3	9	Strategic Director - Social Care & Health  Head of Adult Services
21	Adult Social Services	Non-declaration of capital which can involve the transfer or disguise of property in order to avoid paying for residential or domestic care provision.	Lack of checks. Lack of staff awareness / training / procedures.	Financial loss. Increased resource intensive investigations. Costly legal proceedings. Reputational damage.	Almost Certain	4	Major	4	16	Sound staff understanding of the legal framework and processes.	Likely	3	Substantial	3	9	Strategic Director - Social Care & Health  Head of Adult Services

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
22	Adult Social Services	Theft of residents cash.	Lack of segregation of duties. Not adhering to Financial Regulations.	Reputational damage. Financial loss. Loss of staff. Cost of cover / re-employment of new staff.	Almost Certain	4	Major	4	16	Well communicated financial regulations. Robust internal controls i.e. segregation of duties / recording of transactions. Regular internal audit inspection.	Likely	3	Substantial	3	9	Strategic Director - Social Care & Health  Head of Adult Services
23	Adult Social Services	Theft of residents valuables.	Lack of segregation of duties. Not adhering to Financial Regulations.	Reputational damage. Financial loss. Loss of staff. Cost of cover / re-employment of new staff.	Almost Certain	4	Major	4	16	Well communicated financial regulations. Robust internal controls i.e. segregation of duties / recording of transactions. Regular internal audit inspection.	Likely	3	Substantial	3	9	Strategic Director - Social Care & Health  Head of Adult Services
24	Finance	Cyber crime including Ransomware, Whaling, hacking and Denial of Service attack. Human error is a high risk factor.	Lack of staff awareness / training / procedures for dealing with attacks. Insufficient cyber security measures.	Fiancial loss. Loss of access to systems essential to service delivery. Data breaches. Reputational damage. Large fines / sanctions. Operational disruption.	Almost certain	5	Major	4	20	Data Protection training for all staff and members (mandatory) . Multifactor Authentication. Firewalls and Email filtering / anti phishing tools. Restricted access. Continous monitoring. Penetration testing. Vendor due diligence.	Likely	3	Major	4	12	Head of Info Technology & Security

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
25	Finance	Duplicate invoices.	Weak controls over payment and authorisation of invoices. Lack of staff training / awareness.	Financial loss. Reputational damage.	Almost Certain	4	Major	4	16	Staff training. Robust internal controls. Segregation of duties. Regular internal audit checks.	Possible	2	Moderate	2	4	Deputy Chief Executive & Strategic Director Resources (S151 Officer)
26	Finance	Fictitious suppliers.	Weak controls surrounding the creation, payment of suppliers. Lack of staff training / awareness.	Financial loss. Reputational damage.	Almost Certain	4	Major	4	16	Staff training. Robust internal controls. Supplier verification checks. Segregation of duties. Regular internal audit checks.	Possible	2	Moderate	2	4	Deputy Chief Executive & Strategic Director Resources (S151 Officer)
27	Finance	Payments to bank / bank employee accounts relatives accounts.	Weak controls surrounding the creation, payment of suppliers. Lack of staff training / awareness.	Financial loss. Reputational damage.	Almost Certain	4	Major	4	16	Staff training. Robust internal controls. Segregation of duties. Strict authorisation process. Regular internal audit checks.	Possible	2	Moderate	2	4	Deputy Chief Executive & Strategic Director Resources (S151 Officer)



Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
28	Council Tax	Council Tax discount and exemption fraud.	Inadequate checks / evidence requests. Lack of staff awareness / training / procedures.	Financial loss. Increased costs of investigations. Resource diversion. Loss of public trust. Service cuts.	Almost Certain	4	Major	4	16	NFI participation/use of Datatank to verify SPD's. Other revalidation done on a cyclical basis. Trained staff. Regular internal audit. Raised staff and public awareness. Encouragement to report suspected cases of fraud. Proactive recovery of discounts and exemptions wrongly claimed. Identify cases that should attract premiums.	Likely	3	Substantial	3	9	#VALUE!

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
29	Property	Sale or lease of high value assets, land or buildings at undervalue.	Appropriate checks not undertaken. Lack of staff training. Lack of procedures. Collusion.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk.	Almost Certain	4	Major	4	16	Asset registers up to date. Independent valuations obtained where appropriate. Policies and procedures in place. High value transactions subject to member approval. Maintenance of a managed and monitored Corporate Asset management plan.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  Head of Landlord Services
30	All Service Areas	The increasing sophistication of Artificial Intelgence leading to 'fake' documents or communications.	Appropriate checks not undertaken. Lack of staff training. Lack of procedures. Collusion.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk.	Almost Certain	5	Major	5	25	Staff awareness of what 'real' documents look like. Ensuring a culture of challenge is in place across the Council.	Likely	3	Substantial	3	9	Deputy Chief Executive & Strategic Director Resources (S151 Officer)  Head of Info Technology & Security  Head of Digital Services

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
31	All Service Areas	False sickness claims.	Employees who are disengaged / dissatisfied at work. A workplace culture that tolerates the use of sick leave for non medical issues. Employees using sick leave to address personal issues.Lack of sickness policy / attendance monitoring.	Financial loss. Cost of supply / cover staff. Delay / halt / decline in quality of service delivery.	Almost Certain	4	Moderate	2	8	Foster a positive work environment. Clear and well communicated sickness / managing attendance policies. Conducting regular reviews of absence patterns. Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Likely	3	Moderate	2	6	Chief Officer - People, Policy & Performance  Strategic Leadership Team

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
32	All Service Areas	Employee abuse of flexitime or annual leave systems.	Employees who are disengaged / dissatisfied at work. Lack of policy / leave monitoring.	Financial loss. Cost of supply / cover staff. Delay / halt / decline in quality of service delivery. Reputational damage.	Almost Certain	4	Moderate	2	8	Foster a positive work environment. Clear and well communicated flexi / leave policies. Officer code of conduct in place and declared by all employees which details expected behaviours, corporate policies and potential penalties of wrongdoing. Take appropriate action such as disciplinary action and appropriate criminal/civil proceedings.	Likely	3	Moderate	2	6	Chief Officer - People, Policy & Performance  Strategic Leadership Team
33	Adult Social Services	Blue Badge fraud.	Appropriate checks not undertaken. Lack of awareness / training / procedures.	Reputational damage. Effect quality of life for disabled residents / visitors.	Almost Certain	4	Minor	1	4	NFI participation. Enforcement Officer checks.	Likely	3	Minor	1	3	Strategic Director - Social Care & Health  Head of Adult Services

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood	Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood	Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner	
34	All Service Areas	Theft of assets and equipment.	Financial difficulties. Employer dissatisfaction. Perceived harmless. Lack of consequence. Poor inventory maintenance. Lack of cash reconciliation.	Financial loss. Disruption to service delivery. Reputational damage. Negative impact on employee morale.	Almost Certain	4	Substantial	3	12	Likely	3	Moderate	2	6	Strategic Leadership Team Heads of Service
35	All Service Areas	Unauthorised sale of assets and equipment.	Financial difficulties. Employer dissatisfaction. Perceived harmless. Lack of consequence. Poor inventory maintenance.	Financial loss. Disruption to service delivery. Reputational damage. Negative impact on employee morale.	Almost Certain	4	Substantial	3	12	Likely	3	Moderate	2	6	Strategic Leadership Team Heads of Service

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
36	Finance	Improper use of corporate purchase cards including personal use.	Lack of controls / not adhering to Purchase Card Regulations. Poor authorisation process.	Financial loss. Reputational damage.	Almost Certain	4	Substantial	3	12	Staff must sign Purchase Card User / Authoriser Regulations /Agreements. Segregation of Duties. Regular internal audit checks. Robust controls. Staff must produce receipt / invoice for every transaction.	Likely	3	Moderate	2	6	Deputy Chief Executive & Strategic Director Resources (S151 Officer)
37	Adult Social Services	Direct payment fraud.	Lack of monitoring of compliance with policies and best practice by management.	Irrecoverable financial loss. Potential for financial abuse of vulnerable adults. HMRC fraud.	Likely	3	Moderate	2	6	Monitoring and support, training and guidance.	Likely	3	Moderate	2	6	Strategic Director - Social Care & Health  Head of Adult Services

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
38	Housing Benefit	Benefit fraud.	Appropriate checks not undertaken. Lack of staff training. Lack of procedures.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk.	Almost Certain	4	Substantial	3	12	Trained staff. NFI participation. Internal Audit. Documentary evidence. Raised staff and public awareness. Encouragement to report suspected cases of fraud. Share information with DWP and support investigations conducted by DWP. Actively recover overpayments. Take sanction action where appropriate.	Likely	3	Moderate	2	6	Deputy Chief Executive & Strategic Director Resources (S151 Officer)
39	Council Tax Benefit	Council Tax Benefit (Council Tax reduction scheme) fraud.	Appropriate checks not undertaken. Lack of staff training. Lack of procedures.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk.	Almost Certain	4	Substantial	3	12	Trained staff. NFI participation. Internal Audit. Documentary evidence. Raised staff and public awareness. Encouragement to report suspected cases of fraud.	Likely	3	Moderate	2	6	Deputy Chief Executive & Strategic Director Resources (S151 Officer)

Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
40	NNDR	Flase claim for rate relief, incorrect occupancy information supplied.	Appropriate checks not undertaken. Lack of staff training. Lack of procedures.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk.	Almost Certain	4	Substantial	3	12	Trained staff. Internal Audit. Documentary evidence. Raised staff and public awareness. Encouragement to report suspected cases of fraud.	Likely	3	Moderate	2	6	Deputy Chief Executive & Strategic Director Resources (S151 Officer)
41	Housing	Tenancy Fraud including subletting or manipulation of succession.	Appropriate checks not undertaken. Lack of staff training. Lack of procedures.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk.	Almost Certain	4	Substantial	3	12	Trained staff. NFI participation. Internal Audit. Documentary evidence. Raised staff and public awareness. Recover properties where tenancy fraud is identified. Undertake criminal prosecutions (Prevention of Social Housing Fraud Act 2013). Encouragement to report suspected cases of fraud.	Likely	3	Moderate	2	6	Head of Housing, Strategic Partnerships & Reform



Appendix 1 – Fraud Risk Register

Ref	Business Area	Risk	Root Cause	Consequence	Pre-Mitigation Risk Likelihood		Pre-Mitigation Risk Impact		Overall Pre-Mitigation Risk Risk	Control Measures	Post-Mitigation Risk Likelihood		Post-Mitigation Risk Impact		Overall Post-Mitigation Risk Residual	Risk Owner
42	All Service Areas	Abuse of trust / power / position.	Lack of a segregation of duties.	Financial loss. Increased costs of investigations. Resource diversion. Reputational risk. Negative impact on employe morale.	Almost Certain	3	Moderate	2	6	Regular reconcilation of inventory / cash. Regular stock checking. Segregation of duties. Encourage confidential reporting of suspicious activity. Asset labelling / security marking of equipment. Reguar internal audit checks. Restricted access to bulidings / asset storage. Robust financial monitoring. Documenting of key decisions with detailed reasoning / business cases in support.	Likely	3	Minor	1	3	Chief Executive, All Strategic Directors, Chief Officers and Heads of Service.



## National Fraud Initiative Self-Appraisal Checklist

Date issued: November 2024

Version: Final

Document reference: 4608A2024

## Contents

About the National Fraud Initiative.....	34
About this document .....	34
Self-appraisal checklist .....	35

## About the National Fraud Initiative

- 1 The National Fraud Initiative (NFI) is a biennial UK-wide counter-fraud exercise. It uses computerised techniques to compare information about individuals held by different public bodies, and on different financial systems, that might suggest the existence of fraud or error.
- 2 Fraud, error and overpayment outcomes valued at £7.1 million were recorded by participants for the [NFI 2022-23 exercise](#). Beyond any financial savings, the benefits of participation and reviewing data matches include the assurances that NFI results can provide around systems of internal control. NFI results may also highlight areas for improvement.
- 3 The [Public Sector Fraud Authority](#) (PSFA) – part of the UK Government's Cabinet Office and HM Treasury – oversees the NFI across the UK. Audit Wales leads the exercise in Wales under the Auditor General's powers in the [Public Audit \(Wales\) Act 2004](#). The Auditor General's [Code of Data Matching Practice](#) summarises the key legislation, and controls, governing the exercise in Wales.
- 4 The Auditor General has mandated that unitary local authorities, NHS bodies, police forces, and fire and rescue authorities participate in the NFI. Other organisations participate on a voluntary basis, such as the Welsh Government and some Welsh Government arm's length bodies.
- 5 Information about the NFI is also available on the [Audit Wales website](#).

## About this document

- 6 The NFI is one aspect of an organisation's counter-fraud arrangements. We have prepared this checklist to help participating bodies self-appraise how they are engaging with the NFI.
- 7 We encourage all participating bodies to complete the checklist and present it to those charged with governance to support scrutiny of their NFI arrangements.

## Self-appraisal checklist

		Yes / Partly / No	Comments / action required	If action is required, who by and when?
<b>Leadership, commitment, and communication</b>				
1	Are we committed to the NFI? Has the council / board, those charged with governance and senior management expressed support for the exercise and has this been communicated to relevant staff?	Yes	The Councils Governance & Audit Committee and Senior Management of the Council support the NFI. This has been communicated to all staff via 'Fraud Awareness Week' (November 2024) and will be reiterated through Anti-Fraud, Corruption & Bribery training due to be launched in January 2025.	n/a
2	Have we committed specific resources to support the overall management of the NFI?  If information is available, how much time was spent by the Key Contact on the last exercise, and how much has been allocated for the next exercise?	Yes	As part of the restructure of the Internal Audit team in April 2024 a dedicated Counter Fraud Officer was added to the structure. This was recruited to in October 2024 with the postholder due to start with MCC in January 2025.  Resource also sits with the Shared Benefit Service with Torfaen CBC to investigate Council Tax and Housing Benefit data match's.  The data is not available for how long the Key Contact spends directly on NFI. The Key Contact takes a lead in ensuring appropriate coverage and completion to statutory deadlines.	n/a
3	Is our NFI Key Contact the appropriate officer for that role, ie has sufficient authority to ensure the NFI exercise is delivered effectively?	Yes	The Key Contact is the Chief Internal Auditor.  As per the Internal Audit Charter the Chief Internal Auditor has a direct reporting line to the Chief Executive, Chair of the Council and the Chair of the Governance & Audit Committee to report issues arising.	n/a
4	Does internal audit, or equivalent, monitor our approach to NFI and our main outcomes, ensuring that any weaknesses are addressed in relevant cases?	Yes	As detailed, the Chief Internal Auditor co-ordinates and monitors the exercise on behalf of Monmouthshire County Council. Issues raised through the NFI exercise are followed-up as per the agreed Internal Audit protocol with the Governance & Audit Committee.	n/a

			The Internal Audit team will for the 2024/25 exercise have a dedicated resource.	
<b>Planning and preparation</b>				
5	Do we plan properly for all aspects of the NFI exercise and set our own internal deadlines?	Yes	<p>Planning took place for the 2024 collection of data and regular communication and reminders were issued to key staff for the data sets to ensure compliance with the specification.</p> <p>Internal deadlines were set to allow data to be returned and quality checked by the Internal Audit team prior to upload. All statutory deadlines were met with time to spare.</p> <p>Internal deadlines for the review of data match's will be set once the data has become available.</p>	n/a
6	For the NFI 2024-25 exercise, did we provide all NFI data on time using the secure data file upload facility properly?	Yes	<p>All data was submitted 14<sup>th</sup> October 2024. Deadline was 25<sup>th</sup> October 2024.</p> <p>Data was password protected as per the security guidance and uploaded via the secure data file upload facility.</p>	n/a
		<b>Yes / Partly / No</b>	<b>Comments / action required</b>	<b>If action is required, who by and when?</b>
7	For the NFI 2024-25 exercise, did we confirm promptly (using the online facility on the secure website) that we have met the fair processing notice requirements?	Yes	<p>Compliance was confirmed 09<sup>th</sup> August 2024 via the secure website.</p> <p>Deadline was 30<sup>th</sup> August 2024</p>	n/a
8	Do we review our Data Quality results before starting our investigations? <sup>1</sup>	n/a	This checklist is being completed prior to starting 2024/25 investigations.	Chief Internal Auditor January 2025

<sup>1</sup> The Data Quality module could indicate that there are issues with the data submitted that may have affected some of the matches. The module can be accessed from the relevant National Exercise page of the web app.

			<b>Action:</b> Ensure that we review our Data Quality results before starting our investigations.	
9	Do staff take time to read the guidance that is provided on how to follow up the NFI matches (which are especially important for those users encountering the NFI for the first time), and do they consult the NFI team if they are unsure about how to record outcomes?	Yes	Guidance has been provided to team members.  NFI System Training has been arranged via the Cabinet Office for January 2025 for the new Counter Fraud Officer and also as a refresher for the Chief Internal Auditor and Senior Auditor prior to reviewing the 2024/25 data matches.  The NFI helpdesk has been contacted where queries existed and MCC will continue to do so as and when required.	n/a
10a	Have we considered using the point of application data matching service offered by the NFI team (AppCheck) to improve internal controls and prevent fraud and error from happening?	No	To be considered as part of the Councils Counter Fraud Arrangements once the new Counter Fraud Officer is in post. A mid-year review of the Councils Counter Fraud Risk Assessment will include this review once the main NFI exercise has been completed.  <b>Action:</b> To consider the use of AppCheck as part of the mid year review of the Counter Fraud Risk Assessment.	Chief Internal Auditor September 2025
10b	If not using AppCheck, is there a clear rationale for this?	As above	As detailed above. This is work in progress.	See 10a
<b>Effective follow-up of matches</b>				
11	Have we documented our approach for risk assessing data match reports and investigating data matches? <sup>2</sup>	Partly	The approach used by MCC in previous exercises has been to investigate ALL high risk matches followed by a sample of medium / low risk's based on auditor judgement. Matches not investigated were clearly marked as such. This approach will be formally documented for the 2024/25 exercise.	Chief Internal Auditor February 2025

<sup>2</sup> We do not expect organisations to look at every data match or report. Instead, they should prioritise which matches to look at and the order in which they are followed up. They may want to assess your matches by fraud risk area and then by match risk scores. Alternatively, they may want to set up bespoke filters using the filter tool. Matches not investigated should be Closed – Not Selected for Investigation.

			<b>Action:</b> To formally document the approach to assessing data match reports and investigating data matches in conjunction with the Shared Benefits Service.	
		<b>Yes / Partly / No</b>	<b>Comments / action required</b>	<b>If action is required, who by and when?</b>
12	Does our approach give priority to local fraud risks? <sup>3</sup>	Yes	The completion of this document has formed part of the Councils Counter Fraud Risk Assessment which considers the organisations fraud risk register and wider control environment. Internal Audit planning prioritises areas where concerns exist regarding the internal control environment or where historical instances of fraud have occurred both within Monmouthshire County Council and the wider region / Wales / Country.	n/a
13	Does our approach give priority to following up high-risk matches, those that become quickly out of date and those that could cause reputational damage if a fraud or error is not stopped quickly? <sup>4</sup>	Yes	All high risk matches are reviewed as priority. This will be documented and refined as per the action stated for control 11.	See action for control 11.
14	Are sufficient resources and expertise available at the right time to maximise the outcomes of the NFI exercise? <sup>5</sup>	Yes	Counter Fraud Officer has been recruited to for 2024/25 exercise. Resource also sits with the Shared Benefit Service.	n/a
15	Does the Key Contact coordinate investigations across internal departments to prevent duplication of effort or delays in	Yes	Data matches relating to Council Tax and Housing Benefit are reviewed by the dedicated resource within the Shared Benefit Service.	n/a

<sup>3</sup> We suggest that the NFI Key Contact (with support from Internal Audit/Counter Fraud) should review the organisation's overall control environment and systems. Existing internal audit reports and/or your organisation's risk register should assist this review. We advise prioritising data match reports that are linked to areas that have unknown or weak internal controls or areas that have had historical instances of fraud. Organisations should also look back to see which reports in a previous exercise gave them outcomes.

<sup>4</sup> Use the tools within the web application, such as the filter and sort options or data analysis software, to help prioritise matches deemed the highest risk.

<sup>5</sup> When nominating users to investigate matches, organisations should choose the person with the most knowledge about the dataset. For example, trade creditors matches are best dealt with by a nominated person in internal audit or the accounts payable team. We also suggest assigning a user to act as lead dataset contact for each dataset your organisation submits, so that, if necessary, other NFI participants can contact the most suitable person to assist their investigation. If organisations do not nominate a lead dataset contact, the default contact will be the Key Contact.



	identifying overpayments and ensure all relevant actions are taken, for example, organising joint investigation of single person discount matches involving housing benefit?		All other data reviews are conducted initially by the Internal Audit team with investigations co-ordinated when required across departments.	
		<b>Yes / Partly / No</b>	<b>Comments / action required</b>	<b>If action is required, who by and when?</b>
16	(In health bodies) Are we drawing appropriately on the help and expertise available from NHS Counter Fraud Service Wales?	n/a	n/a	n/a
17	Are we investigating the circumstances of matches adequately before reaching a 'no issue' outcome, in particular?	Yes	A full investigation will be conducted for each match to satisfy the Officer. Reasons will be documented where a 'no issue' outcome has been recorded.	n/a
18	Do we review how frauds and errors arose and use this information to improve our internal controls?	Yes	A continual process of review is undertaken. The outcomes of the 2024/25 NFI exercise will help inform the mid-year review of the Councils Anti-Fraud Risk Assessment. The Council commits to highlighting where fraud has occurred to help improve it's internal control environment.	n/a
19	Are we taking appropriate action in cases where fraud is alleged (whether disciplinary action, penalties/cautions or reporting to the Police or NHS Counter Fraud Service Wales) or errors are identified, eg recovering funds?	Yes	During the previous NFI exercise a case was investigated under the Councils disciplinary policy. This will remain the case, when appropriate, during 2024/25. When necessary reports to the Police will be made. All overpayments / fraud will be recovered.	n/a
20	Do we respond promptly to enquiries from other organisations that take part in the NFI? <sup>6</sup>	Yes	Internal deadline will be set for 2024/25 exercise. We will look to provide a response within 5 working days. This will be monitored by the Chief Internal Auditor.	n/a
<b>Recording and reporting</b>				
21	Are we recording outcomes properly in the secure website and keeping it up to date?	Yes	Ongoing once data matches for 2024/25 have been returned and investigations commence.	n/a

<sup>6</sup> The web application shows the number of shared comments which require a response (Outstanding Actions). These responses should be prioritised if they relate to an ongoing investigation so that it can be progressed promptly.

			Outcomes have been properly reported via the secure website in previous years.	
22	Do we provide appropriate and regular feedback to senior management, board / council members and those charged with governance on NFI activity and outcomes?	Yes	Memo issued following previous NFI exercise to senior management and assurance opinion reported through Governance & Audit Committee. A similar feedback mechanism will be completed for the 2024/25 exercise but with the addition of direct reporting through an SLT meeting and through the Councils mid-year review of the Fraud Risk Assessment.	n/a
		<b>Yes / Partly / No</b>	<b>Comments / action required</b>	<b>If action is required, who by and when?</b>
23	Do we provide those charged with governance assurances that the reasons for fraud and error happening are understood and that action is taken to address them and improve internal controls?	Yes	As part of the Counter Fraud Risk assessment which this review is part of.	n/a
24	Where we have not submitted data or not used the matches returned to us, eg council tax single person discounts, are we satisfied that alternative fraud detection arrangements are in place and that we know how successful they are?	Yes	Ongoing review by the Shared Benefits Service.	n/a
25	Do we publish, as a deterrent, internally and externally the outcomes of the NFI exercise?	No	Has not been published previously but will be included as part of future reporting and awareness campaigns. <b>Action: To include in future awareness campaigns.</b>	Chief Internal Auditor September 2025
26	If, out of preference, we record some or all outcomes outside the secure website, have we made arrangements to inform the NFI team about these outcomes? <sup>7</sup>	n/a	All outcomes are reported to the NFI via the secure website.	n/a

<sup>7</sup> Although preferable for all NFI work to be recorded within the secure web application, we appreciate there may be instances when organisations need to do work on the matches outside it. As soon as data is extracted from the secure NFI web application organisations are responsible for the security of the data, including avoiding inappropriate disclosure and ensuring it is destroyed when no longer needed. Therefore, we only advise exporting data when it is essential to do so.

Audit Wales

Tel: 029 2032 0500

Fax: 029 2032 0600

Textphone: 029 2032 0660

E-mail: [info@audit.wales](mailto:info@audit.wales)

Website: [www.audit.wales](http://www.audit.wales)

We welcome correspondence and telephone calls in Welsh and English. Rydym yn croesawu gohebiaeth a galwadau ffôn yn Gymraeg a Saesneg.

### Appendix 3 – Counter Fraud, Corruption & Bribery Action Plan

Identified Need	Action	Implementation Date	Responsible Officer
To raise awareness across the Council of Fraud, Corruption and Bribery.	<ul style="list-style-type: none"> <li>To ensure regular staff communications are sent highlighting fraud risks and sign-posting to the Policy.</li> <li>Taking part in International Fraud Week</li> </ul>	<p>Quarterly</p> <p>November 2025</p>	Chief Internal Auditor
Organisational wide training.	<ul style="list-style-type: none"> <li>Develop a mandatory training module on ThinQI for all Members and Officers of the Council.</li> <li>Monitor completion and report to Governance &amp; Audit Committee.</li> </ul>	<p>January 2025</p> <p>IA Annual Report – May 2025</p>	Chief Internal Auditor
Specific counter fraud training for Council staff.	<ul style="list-style-type: none"> <li>Ensure a sufficient number of staff have completed formal Counter Fraud Training such as CIPFA Accredited Counter Fraud Specialist.</li> </ul>	September 2025	Chief Internal Auditor
Improve the organisational response to Fraud.	<ul style="list-style-type: none"> <li>Recruitment to Counter Fraud Officer post.</li> <li>Ongoing review of current arrangements.</li> <li>Look to embed fraud management arrangements within Service Business Plan guidance.</li> </ul>	<p>January 2025</p> <p>October 2025</p>	<p>Deputy Chief Executive / Strategic Director (Resources)</p> <p>Head of Finance (Acting S151 Officer)</p> <p>Chief Internal Auditor</p>
Strengthen the approach to the National Fraud Initiative across Monmouthshire.	<ul style="list-style-type: none"> <li>Implement the required actions from the NFI Self Appraisal Checklist. (Appendix 2)</li> </ul>	Included within NFI Self Appraisal.	Chief Internal Auditor
Promptly investigate data matches arising from the National Fraud Initiative. Investigate and record outcomes where necessary.	<ul style="list-style-type: none"> <li>Following data matches being returned in January 2025, ensure dedicated resource is available to promptly</li> </ul>	April 2025	<p>Deputy Chief Executive / Strategic Director (Resources)</p> <p>Head of Finance (Acting S151 Officer)</p> <p>Chief Internal Auditor</p>