ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	28 November 2024
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2503 – National Fraud Initiative
REPORT NUMBER	IA/AC2503
DIRECTOR	N/A
REPORT AUTHOR	Jamie Dale
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

1.1 The purpose of this report is to present the planned Internal Audit report on the National Fraud Initiative.

2. RECOMMENDATION

2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

3. CURRENT SITUATION

3.1 Internal Audit has completed the attached report which relates to an audit of the National Fraud Initiative.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal implications arising from the recommendations of this report.

6. ENVIRONMENTAL IMPLICATIONS

6.1 There are no direct environmental implications arising from the recommendations of this report.

7. RISK

7.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are detailed in the resultant Internal Audit reports. Recommendations, consistent with the Council's Risk Appetite Statement, are made to address the identified risks and Internal Audit follows up progress with implementing those that are agreed with management. Those not implemented by their agreed due date are detailed in the attached appendices.

8. OUTCOMES

8.1 There are no direct impacts, as a result of this report, in relation to the Council Delivery Plan, or the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place.

8.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

9. IMPACT ASSESSMENTS

Assessment	Outcome
Impact Assessment	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
Privacy Impact Assessment	Not required

10. BACKGROUND PAPERS

10.1 There are no relevant background papers related directly to this report.

11. APPENDICES

11.1 Internal Audit report AC2503 – National Fraud Initiative

12. REPORT AUTHOR CONTACT DETAILS

Name	Jamie Dale
Title	Chief Internal Auditor
Email Address	Jamie.Dale@aberdeenshire.gov.uk
Tel	(01467) 530 988

Internal Audit

Assurance Review of National Fraud Initiative

Status: Final
Date: 19 August 2024
Risk Level: Corporate

Report No: AC2503
Assurance Year: 2024/25

Net Risk Rating	Description	Assurance Assessment
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**

Report Tracking	Planned Date	Actual Date
Scope issued	02-Apr-24	01-Apr-24
Scope agreed	09-Apr-24	08-Apr-24
Fieldwork commenced	15-Apr-24	15-Apr-24
Fieldwork completed	10-May-24	23-May-24
Draft report issued	31-May-24	12-Jun-24
Process owner response	21-Jun-24	05-Aug-24
Director response	28-Jun-24	16-Aug-24
Final report issued	05-Jul-24	19-Aug-24
Audit Committee	26-Sep-24	

Distribution	
Document type	Assurance Report
Director	Andy MacDonald, Director - Corporate Services
Process Owner	Jonathan Belford, Chief Officer - Finance
Stakeholder	Angela Crawford, Finance Controls Manager
	Matthew Dickson, Counter Fraud Officer
	Donna Slater, Counter Fraud Officer
	Wayne Connell, Revenues and Benefits Manager
	Phyllis Kennedy, Council Tax and Recovery Manager
	Ronnie McKean, Corporate Risk Lead
	Vikki Cuthbert, Interim Chief Officer – Governance*
***Final only**	External Audit*
Lead auditor	Konstantinos Minas, Auditor

1 Introduction

1.1 Area subject to review

Audit Scotland carries out data matching under part 26A of the Public Finance and Accountability (Scotland) Act 2000 and Section 97 of the Criminal Justice and Licensing Act 2010. This legislation provides that Audit Scotland may carry out data matching exercises or arrange for them to be carried out on its behalf.

The National Fraud Initiative (NFI) is a data matching exercise that matches electronic data within and between participating bodies to prevent and detect fraud, taking place every two years. The Cabinet Office's NFI team conducts the matching work on Audit Scotland's behalf and Audit Scotland prepares a report on the results, which participating bodies are expected to investigate.

Each participating body in the NFI is required to identify people in two key roles – a Senior Responsible Officer and a Key Contact.

The Senior Responsible Officer (usually the Chief Officer – Finance) must:

- Nominate a Key Contact.
- Ensure the Key Contact has access to the matches, via the secure NFI web application, when they become available.
- Ensure that the key contact fulfils all privacy notice requirements.

The role of the Key Contact is to:

- Fulfil the organisation's privacy notice requirements via direct communication with the organisation's Data Protection Officer or equivalent.
- Ensure that the data formats guidance and data specifications are followed.
- Nominate appropriate users to upload data submissions, investigate the matches and act as the point of contact for other bodies about a match (preferred Dataset Contact).
- Coordinate and monitoring the overall exercise.
- Ensure that outcomes from the investigation of matches are recorded on the web application promptly and accurately.

The 2022/23 NFI exercise is ongoing at the time of review with Audit Scotland due to publish the results in 'summer 2024' according to the 2022/23 NFI timetable.

1.2 Rationale for the review

The objective of this audit is to review the Council's engagement and controls for actioning outputs of the National Fraud Initiative, specifically looking at the utilisation of information to gain assurance over areas such as Council Tax and Business Rates. This review will not look to recreate the NFI exercise or work on any out the outcomes.

This area has not been subject to a standalone audit previously and as such has been included in the agreed Internal Audit plan to ensure that the Council is investigating NFI matches, reporting outcomes in a timely manner and improving controls where necessary.

1.3 How to use this report

This report has several sections and is designed for different stakeholders. The executive summary (section 2) is designed for senior staff and is cross referenced to the more detailed narrative in later sections (3 onwards) of the report should the reader require it. Section 3 contains the detailed narrative for risks and issues we identified in our work.

2 Executive Summary

2.1 Overall opinion

The full chart of net risk and assurance assessment definitions can be found in Appendix 1 – Assurance Scope and Terms. We have assessed the net risk (risk arising after controls and risk mitigation actions have been applied) as:

Net Risk Rating	Description	Assurance Assessment
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**

The organisational risk level at which this risk assessment applies is:

Risk Level	Definition
Corporate	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.

2.2 Assurance assessment

The level of net risk is assessed as **MODERATE**, with the control framework deemed to provide **REASONABLE** assurance over the Council's approach to the National Fraud Initiative.

Reasonable assurance was available over the following areas reviewed:

- **Governance** – An experienced team of suitable officers (Key Contacts) are responsible for the Council's response to the National Fraud Initiative under the supervision of the Senior Responsible Officer, the Chief Officer - Finance. In addition, the Risk Board has monitored some relevant risks to the process and the Audit, Risk and Scrutiny Committee was informed in May 2024 of the outcome of the 2022/23 NFI exercise. In general, the 2022/23 NFI exercise was well managed using a risk-based approach and identified invoiceable recoverable amounts and Cabinet Office estimated savings resulting from the main exercise have increased compared to the last two exercises, mainly due to recovery of Council tenancies e.g. multiple tenancies for single resident. The recoverable sums and future estimated savings by dataset for the last two main NFI exercises and for the last two ancillary NFI "ReCheck" reviews of Council Tax single persons discount eligibility, are detailed at appendix 1 below.

Exercise Year	Actual	COES[1]	Total
2022/23	£345k	£988k	£1,333k
2020/21	£43k	£117k	£160k
2018/19	£27k	£11k	£38k

- **Lessons Learned** – Following the 2020/21 NFI exercise, a lessons learned exercise was completed identifying relevant risks and associated actions for improvement, which were subsequently monitored by the Risk Board.

However, the review identified some areas of weakness where enhancements could be made to strengthen the framework of control, specifically:

- **Operational Procedures** – The Council's Counter Fraud Policy is comprehensive and references the Chief Officer – Finance's responsibility to co-ordinate engagement with the NFI exercise. In addition, staff involved in the NFI exercise are notified of relevant legislation, policy,

[1] Cabinet Office Estimated Savings due to confirmed error / fraud.

and guidance they must comply with when seeking access to the secure NFI web application. Also, comprehensive web application user guidance is available to staff within the system. Furthermore, the Council has an NFI intranet site describing the purpose of the NFI; Council Key Contacts and the SRO; mandatory datasets to be provided; the timetable for the previous exercise; and contact details for the fraud team. In addition, Council Tax match procedures are in place. However, whilst available guidance is beneficial and clear it does not cover how to investigate and resolve all match types, with examples. This risks business continuity; limits the scope for training staff; and risks inappropriate investigation techniques and conclusions, risking prosecution and recovery success.

- **Security Checks (Users of NFI Web Application)** – In order to access the Cabinet Office's NFI web application, users must meet the Baseline Personnel Security Standard (BPSS). However, Basic Disclosure checks had not been completed to verify 19 users of the system for the 2022/23 exercise had no unspent criminal convictions as required, risking reputational damage and inappropriate use of match data.
- **Data upload quality** – Data specifications by dataset type were issued by the Cabinet Office for the 2022/23 NFI exercise. Whilst all mandatory datasets were submitted by the Council to the Cabinet Office via the secure NFI web application for the 2022/23 exercise between October 2022 and September 2023 there were challenges experienced with creditors and housing data quality. An initial decision was taken not to upload creditors and tenancy waiting list data as reported to the Risk Board in August 2022. However, Audit Scotland objected, and corrective action had to be taken to address this and consequently creditors data was uploaded 5 days late. Where Council systems contain inaccurate data, this risks a breach of data protection legislation where it relates to personal data, reputational damage where NFI data sharing obligations cannot be complied with, and fraud investigation efficiency and effectiveness.
- **Match Review and Closure** – 18,491 matches were reported to the Council through the 2022/23 NFI exercise (including via ReCheck for Council Tax data) across 92 different datasets. Whilst most data match reports showed evidence of review (some on a sample basis) and closure it was noted two (3%) reports relating to 40 (0.2%) matches were not reviewed at all. A Finance Key Contact advised these reports had not been made accessible during the review to Key Contacts via the web app due to a system access problem, this has been resolved post the audit fieldwork period.
- **Payment Fraud Controls** – It has been confirmed that it would not be possible for the previous NFI exercises to detect the recent Council Tax fraud since the Council Tax refunds are processed using bank account data held within the Revenues and Benefits system, which is not supplied for data matching purposes as part of the NFI exercise. However, this highlights a gap in exception reporting since the employee concerned used a bank account as part of the fraud which was held on the payroll system.
- **Data Protection and Information Management** – Council Tax match data has not been subject to a data protection impact assessment as required to assess the risks to sensitive personal data exported from the NFI web application, risking inappropriate processing of sensitive match data. Also, the exported data has not been named in accordance with HM Government classification policy.
- **Oversight Enhancements** – Whilst Finance completed the Audit Scotland 2022/23 NFI self-appraisal checklist for NFI Key Contacts and Users and reported this to Risk Board, the related checklist for those charged with governance included, was not completed, and monitored by Risk Board reducing oversight of these risks. In addition, key actions detailed in the Audit Scotland / Cabinet Office timetables and subsequent investigation of matches to agreed deadlines were not formally monitored by the Risk Board. Whilst the 2022/23 exercise was generally managed on time, certain data uploads to the secure web application were delayed by a short period and certain match reports were overlooked as described above. RAG based reporting of key timetabled tasks, with responsible officers and implementation due dates, and monitoring of the Audit Scotland NFI self-appraisal checklist for those charged with governance, would enhance oversight, help avoid delays, and potentially improve data upload and match investigation response times, fraud recovery and mitigation outcomes.

- **Fraud Risk Management** – Audit Scotland NFI guidance to those charged with governance recommends ensuring awareness of emerging fraud risks so preventative action can be taken. risks relevant to the successful delivery of the 2022/23 NFI exercise were monitored by Risk Board based on the outcome of a lessons learned review, currently emerging fraud risks are not monitored by the Risk Board or officers via a Council risk register, increasing the possibility that relevant new fraud risks will be overlooked and not mitigated where necessary.
- **Publishing Fraud Investigation Achievements (Internally and Externally)** – Audit Scotland guidance (the NFI self-appraisal checklist) recommends publishing internally and externally the achievement of fraud investigators. In addition, the Council's Counter Fraud Policy states *"Regular information relating to anti-fraud initiatives will be published on social media*." Whilst internally fraud and payment error savings resulting from the NFI exercise are reported to staff via the Council intranet, externally the annual NFI update report to Audit, Risk and Scrutiny is not made public and at the time of review anti-fraud initiatives were not being published on social media as per the Council's Counter Fraud Policy, reducing the opportunities for deterring future instances of fraud.

Recommendations have been made to address the above risks, including formalising written operational procedures; establishing control over system access and data quality; enhancing oversight by Risk Board; resolving match report access issues; and ensuring match data exported from the NFI web app is handled in compliance with data protection legislation and classified correctly. In addition, recommendations were made to ensure emerging fraud risks are monitored; additional NFI services are assessed and if appropriate procured; and fraud outcomes are advertised as a deterrent.

Furthermore, recommendations were made to address fraud risks presented by Council payment systems that are outwith the scope of the NFI process, by ensuring system level controls enforce segregation of duties where necessary, via privileged user access monitoring, and by establishing exception reports covering other relevant risks.

2.3 Severe or major issues / risks

Issues and risks identified are categorised according to their impact on the Board. The following is a summary of a higher rated issue / risk that has been identified as part of this review:

Ref	Severe or Major Issues / Risks	Risk Agreed	Risk Rating	Page No.
1.2	**Security Checks (Users of NFI Web Application)** – The Cabinet Office Security Policy Framework requires a minimum of the Baseline Personnel Security Standard (BPSS) to be applied to individuals with access to HM Government's sensitive assets, which includes data match reports generated by the National Fraud Initiative. However, 19 users of the NFI web application have not had a Basic Disclosure check (or another higher-level Disclosure Scotland check) to verify they meet criminal record requirements (i.e. have no unspent convictions) according to HR records, meaning BPSS verification has not taken place for these individuals. This is a breach of the Cabinet Office Security Policy Framework and risks unsuitable officers using fraud match data inappropriately.	Yes	**Major**	10

Ref	Severe or Major Issues / Risks	Risk Agreed	Risk Rating	Page No.
1.5	**Payment Fraud Controls** – It has been confirmed that it would not be possible for the previous NFI exercises to detect the recent Council Tax fraud since the Council Tax refunds are processed using bank account data held within the Revenues and Benefits system, which is not supplied for data matching purposes as part of the NFI exercise. However, this highlights a gap in exception reporting since the employee concerned used a bank account as part of the fraud which was held on the payroll system. A separate recommendation has already been agreed by Management as part of Internal Audit report AC2407 to standardise Council payee identification requirements for all Council payment systems. Finance has advised they are looking to establish internal exception reporting subject to data protection considerations to prevent a similar fraud in future.	Yes	**Major**	13

2.4 Management response

Following the lessons learnt from the 2020 NFI exercise the Council has put in place a range of improvements to ensure that gaps were filled, actions were completed and a more robust response provided to the 2022 NFI exercise. In general this audit provides assurance that data was provided, matches were identified and on the whole follow ups and checks of the matches were undertaken to establish if any fraud had taken place. The report identifies a number of recommendations all of which have been accepted and actions have been put in place to be implemented in the coming months and in order to support the 2024 NFI exercise.

There are opportunities for the Council to be more consistent in its approach to counter fraud measures and to track emerging risks and improvements will be made.

3 Issues / Risks, Recommendations, and Management Response

3.1 Issues / Risks, recommendations, and management response

Ref	Description	Risk Rating	Minor
1.1	**Written Policies, Procedures and Guidance** – Comprehensive written policies, procedures, and guidance, which are easily accessible by all members of staff reduce the risk of errors and inconsistency and provide management with assurance correct and consistent instructions are available, especially in the event of an experienced employee being absent or leaving. Good Practice The Council's Counter Fraud Policy referenced in the Council's Scheme of Governance in the Financial Regulations is comprehensive and describes the Chief Officer – Finance's responsibility to co-ordinate engagement with the NFI exercise. In addition, staff involved in the NFI exercise are notified of relevant legislation, policy, and guidance they must comply with through the application to access the NFI web application. Also, web application user guidance is available to staff within the system. Furthermore, the Council has a designated NFI website found in their Intranet; this provides additional information on the process, clearly defined Key Contacts, the timetable for the latest NFI exercise and details for contacting the counter fraud team. In addition, Council Tax match procedures are in place. Match Investigation and Resolution Guidance However, whilst available guidance is beneficial and clear, it does not generally cover how to investigate and resolve different match types, with examples. This risks business continuity, optimum use of existing available resources, reduces the scope for training additional suitable Council officers, and as stated in the NFI web application online resource and investigation guidance, risk prosecution and recovery success where matches are investigated inappropriately. Resourcing the NFI exercise was reported as a challenge for certain datasets, particularly where data quality was poor due to system recording issues. Comprehensive operational procedures would help address this for the reasons explained above. Baseline Personnel Security Standard Guidance As considered further at 1.2 below, the Cabinet Office Security Policy Framework requires a minimum of the Baseline Personnel Security Standard (BPSS) checks prior to granting access for users to access data from the NFI web application. These checks include verification of the user's identity, employment history, their right to work in the UK and, if appropriate, checks of any unspent criminal records. The Council's recruitment and selection guidance covers the need for managers to ensure a preferred candidate provides evidence of the right to live and work in the UK and Disclosure Scotland checks are undertaken where necessary, which People and Citizen Services advise covers BPSS identity requirements. However, BPSS employment history checks are an additional requirement and not covered by the standard pre-employment checks as detailed in the guidance. People and Citizen Services advise it is currently a very small number of Council roles that require a BPSS check, to use government systems, and where this is required, it is often not at the point of recruitment but instead during the course of an employee's employment and therefore these checks are required to be undertaken at that point instead. Whilst the point of recruitment may not be the most appropriate time to undertake BPSS checks to access the NFI system, in the absence of guidance for managers on how to complete or arrange these checks, there is an increased risk the Council will the breach		

	Cabinet Office Security Policy Framework requirements, risking facilitation of fraud by unsuitable officers with access to the NFI system.

IA Recommended Mitigating Actions

a) Match investigation, resolution and related fraud mitigation operational procedures should be formalised.

b) Recruitment and selection guidance and training should be updated to provide information to managers about when and how to undertake security checks required by staff including BPSS checks.

Management Actions to Address Issues/Risks

a) NFI Key contacts will work with respective team leaders to agree and record the approach to be taken to report investigation, the likely resources they will commit, and the expected timescale, and report this to the Risk Board.

b) Agreed.

Risk Agreed	Person(s)	Due Date
a) Yes	NFI Key Contacts Service Lead – People/ People and Organisation Development Advisor	November 2024
b) Yes		October 2024

Ref	Description	Risk Rating	Major
1.2	**Security Checks (Users of NFI Web Application)** – Audit Scotland NFI 2022/23 Instructions for Participants states: • *"Any information accessed, exported, downloaded or printed from this system must be handled in line with GDPR and the Cabinet Office Security Policy Framework (SPF)."* As stated at 1.1 above, the Cabinet Office Security Policy Framework requires a minimum of the Baseline Personnel Security Standard (BPSS) to be applied to individuals with access to HM Government's sensitive assets, which includes data match reports generated by the National Fraud Initiative. These checks include verification of the applicant's identity, employment history, their right to work in the UK and, if appropriate, checks of any unspent criminal records. However, 19 users of the NFI web application for the 2022/23 NFI exercise have not had a Basic Disclosure check (or another higher-level Disclosure Scotland check) to verify they meet criminal record requirements (i.e. have no unspent convictions), meaning it was not adequately verified that these individuals met the BPSS requirements. This is a breach of the Cabinet Office Security Policy Framework and risks unsuitable officers using fraud match data inappropriately.		

IA Recommended Mitigating Actions

A system of control should be established to ensure BPSS requirements are verified prior to NFI web application access being granted.

Management Actions to Address Issues/Risks

Agreed, a process for this will be put in place.

Ref	Description		Risk Rating	Major
	Risk Agreed	**Person(s)**	**Due Date**	
	Yes	NFI Key Contacts	September 2024	

Ref	Description	Risk Rating	Moderate
1.3	**Data Upload Quality** – Data specifications by dataset type were issued by the Cabinet Office for the 2022/23 NFI exercise, with the Cabinet Office NFI Timetable for 2022/23 stating: • *"Failure to submit all of your required data promptly and of acceptable quality…may incur additional fees and result in some datasets being excluded from the matching process."* Local authorities are required to upload data relating to payroll, pensions, housing (tenants and waiting lists), blue badges, trade creditors (payment history and standing data), taxi driver licences, council tax reduction scheme (CTRS), council tax, the electoral register, and non-domestic rates. Whilst most mandatory datasets were submitted by the Council to the Cabinet Office via the secure NFI web application for the 2022/23 exercise between October 2022 and September 2023 (see table below) there were challenges experienced with data quality, which slightly delayed the upload of creditors data and resulted in Housing Waiting List data not being uploaded as shown below.		

Dataset	Upload Deadline	Actual Upload
Payroll	18/11/2022	11/10/2022
Pensions	18/11/2022	07/11/2022
Housing Tenants	18/11/2022	10/10/2022
Housing Waiting Lists	18/11/2022	Not Uploaded
Blue Badge Resident Parking Permit	18/11/2022	31/10/2022
Taxi Driver Licenses	18/11/2022	10/10/2022
Trade Creditors Payment History Data	18/11/2022	23/11/2022
Trade Creditors Standing Data	18/11/2022	23/11/2022
Student Loans	18/11/2022	Uploaded by SAAS
Council Tax Reduction Scheme	18/11/2022	11/10/2022
Council Tax	27/01/2023	Sep 2022
Electoral Register	27/01/2023	Dec 2022
Non-Domestic Rates	Not Specified	22/09/2023
National Entitlement Cards	N/A	Uploaded by Scot Gov

Issues with data quality included multiple tenancy matches and multiple duplicate payment matches where there were no actual concurrent tenancies / duplicate payments. An initial decision was taken not to upload creditors and tenancy waiting list data as reported to the Risk Board in August 2022. However, Audit Scotland objected in relation to creditors data, and corrective action had to be taken to upload this.

Ref	Description	Risk Rating	Moderate
	Where Council systems contain inaccurate data, this risks a breach of data protection legislation where it relates to personal data and risks reputational damage where NFI obligations cannot be complied with. Furthermore, this presents an unnecessary staff resourcing commitment to review and cleanse data prior to submission where staff could be otherwise better deployed to undertake their routine responsibilities or identify and mitigate fraud.		
	IA Recommended Mitigating Actions Finance should coordinate with relevant system owners to highlight any data quality issues impacting the NFI exercise and those system owners should arrange for data to be cleansed where necessary within the relevant systems. System owners should establish the causes of data accuracy problems within these systems, and controls should be established to avoid these in future. Where possible relevant system controls should automate data input restrictions and escalate relevant exception reports to ensure data accuracy.		
	Management Actions to Address Issues/Risks *NFI Key Contacts will identify / summarise the data errors or inaccuracies and issue this to system owners and Digital &Technology colleagues with an instruction to resolve the data quality issues. This summary will also be provided to the Risk Board.*		
	Risk Agreed: Yes	**Person(s)**: NFI Key Contacts	**Due Date**: October 2024

Ref	Description	Risk Rating	Moderate
1.4	**Match Review and Closure** – When a data match is reported to the Council because of the NFI exercise, it does not mean a fraud has occurred. Prior to concluding an investigation is necessary, to determine the cause so that appropriate action can be taken, and the correct outcome recorded within the NFI web application. 18,491 matches were reported to the Council through the 2022/23 NFI exercise (including via ReCheck for Council Tax data) across 92 different datasets. Whilst the majority of data match reports showed evidence of review (some on a sample basis) and had been closed, it was noted two (3%) reports relating to 40 (0.2%) matches were not reviewed at all since they had no comments and were not closed. • Report 750 - Procurement – Payroll to Companies House (Director) – 32 matches. • Report 175.6 - Residential Parking Permit – Same Vehicle Registration – 8 matches. Report 750 related to employees who appear to be registered directors of companies that the Council had traded with, presenting a potential risk of conflicts of interest in procurement decisions, whilst report 175.6 related to residential parking permits in use where the permit holder had died, risking fraudulent continued use of the parking permit. In addition, it was noted the following report was also not reviewed and closed for the same reason. • Report 752 - Procurement – Payroll to Companies House (Director) – 85 matches – employee address linked to company director's or company address presenting procurement risk. A Finance Key Contact advised these reports had not been made accessible to key contacts during the review via the web application due to an access problem. This should be		

Ref	Description	Risk Rating	Moderate
	addressed as where match reports are not reviewed, particularly high-risk reports, there is a greater risk of unmitigated fraud.		
	IA Recommended Mitigating Actions		
	All NFI match reports should be reviewed and investigated as appropriate. Finance Key Contacts should establish why certain NFI match reports were unavailable for review and ensure access rights are resolved where necessary.		
	Management Actions to Address Issues/Risks		
	Since the completion of the audit fieldwork the NFI Helpdesk advised that NFI Key Contacts inability to view certain reports was the result of an NFI internal policy issue which they had to escalate. There was nothing that the NFI Key Contacts could have done. *Once shared, NFI Key Contacts processed the missing reports.* *Parking permit report would have been closed without investigation in any case because it matched parking permits sharing the same vehicle registration number across Councils and this is not fraud, or even contrary to ACC policy.* *The reports concerning company directors related largely to the appointment of councillors or appropriate council officers to community/ public interest endeavours and there was nothing inappropriate about remaining matches. The report matching payroll to company directors at the same address showed that none of the employees were employed in a capacity which could have induced the council to procure.*		
	Risk Agreed	**Person(s)**	**Due Date**
	Yes	NFI Key Contacts	Implemented

Ref	Description	Risk Rating	Major
1.5	**Payment Fraud Controls** – It has been confirmed that it would not be possible for the previous NFI exercises to detect the recent Council Tax fraud since the Council Tax refunds are processed using bank account data held within the Revenues and Benefits system, which is not supplied for data matching purposes as part of the NFI exercise. However, this highlights a gap in exception reporting since the employee concerned used a bank account as part of the fraud which was held on the payroll system. A separate recommendation has already been agreed by Management as part of Internal Audit report AC2407 to standardise Council payee identification requirements for all Council payment systems. Finance has advised they are looking to establish internal exception reporting subject to data protection considerations to prevent a similar fraud in future.		
	IA Recommended Mitigating Actions		
	Finance should liaise with Audit Scotland to highlight the potential for improvement in data matching through the NFI process via comparison of payroll employee bank details to bank details used by other payment systems.		
	Management Actions to Address Issues/Risks		
	Agreed		
	Risk Agreed	**Person(s)**	**Due Date**

Ref	Description		Risk Rating	Major
	Yes	Controls Accountant	September 2024	

Ref	Description	Risk Rating	Moderate
1.6	**Data Protection and Information Management** – Audit Scotland instructions for participants for the 2022/23 NFI exercise states: • *"Any information accessed, exported, downloaded, or printed from this system must be handled in line with GDPR and the Cabinet Office Security Policy Framework (SPF). Users and participating organisations must ensure that any information exported from the system is handled in line with HMG requirements for handling Personal and Protectively Marked information."* Council staff declare they will comply with these requirements by signing agreement to the following on application to access the system: • *"Any information accessed, exported, downloaded or printed from this system must be handled in line with GDPR and Data Protection Act 2018 and the Cabinet Office Security Policy Framework (SPF). Users and authorities must ensure that any information exported from the system is handled in line with HMG requirements for handling Personal and Protectively Marked information. If you have any questions about this, you should contact your Senior User, Key Contact or Senior Responsible Officer (as applicable)."* At the point of data export, the NFI web application also requires the user to acknowledge a pop-up stating: • *"The data that you are about to download and/or print is protected by the Data Protection Act 2018 and may be sensitive. Please ensure that you only extract the minimum of information necessary to achieve your intended purposes. Please also ensure that you comply with the policies and procedures your organisation has adopted to ensure appropriate technical and organisational measures are taken against (i) unauthorised or unlawful processing of personal data and (ii) any accidental loss, destruction or damage of personal data."* The above is relevant to Council Tax officers involved in the Council's NFI process since an extract of Council Tax match data is taken from the NFI web application for use by these officers. <u>Data Protection Impact Assessment</u> Whilst the Senior Responsible Officer has declared that data protection requirements have been complied with during the 2022/23 NFI exercise, it was noted that a data protection impact assessment (DPIA) has not been carried out covering the spreadsheet-based system (held within MS Teams) used by Council Tax officers to investigate Council Tax matches exported from the NFI system. The ICO recommends a DPIA be carried out before processing personal data when the processing is likely to result in a high risk to the rights and freedoms of individuals, as is the case for NFI match data which identifies potential fraud and therefore relates to criminal offences. In the absence of a DPIA there is a greater risk match data will be inappropriately accessed in breach of data protection legislation. <u>Information Classification</u>		

Ref	Description	Risk Rating	Moderate
	The Cabinet Office Government Security Classifications Policy and related guidance on Working at OFFICIAL requires the threat profile to an information asset to be assessed and the potential impact of an accidental or a deliberate compromise, to determine the right classification, markings, and controls to apply. However, match exports were not named in accordance with these requirements e.g. "Full List of Rising 18 Cases from NFI" was one saved export. Privacy Notice In accordance with GDPR Article 13, where personal data relating to a data subject is collected, the Council uses privacy notices to: explain the purposes of processing; the legal basis for processing; the data subjects rights in relation to their personal data held by the Council; whether the data will be shared with any other parties; whether there is any automated decision making or profiling using the personal data; and the retention period. A privacy notice is available for Council Tax as required which covers NFI related processing. However, a minor point was noted that the "Your Council Tax Bill Explained" section of the Council's website has a broken link under "how we use and administer your information" for NFI purposes. This should be corrected to improve transparency over NFI personal data processing.		
	IA Recommended Mitigating Actions a) A DPIA should be completed covering the use of NFI match data outwith the NFI web application. b) Exported NFI data should be classified / marked in line with Cabinet Office Government Security Classifications Policy. c) The Your Council Tax Bill Explained section of the Council's website should be updated to address the broken link relating to "how we use and manage your information".		
	Management Actions to Address Issues/Risks *a) Agreed* *b) Agreed* *c) Agreed*		

Risk Agreed	Person(s)	Due Date
a) Yes	a) NFI Key Contacts	a) December 2024
b) Yes	b) NFI Key Contacts	b) December 2024
c) Yes	c) Revenues & Benefits Manager	c) September 2024

Ref	Description	Risk Rating	Minor
1.7	**Oversight Enhancements** – The requirements of any project should be specific, measurable, attainable, responsible, and time-bound (SMART) to be meaningful and to ensure they are achieved as anticipated. Regular updates were provided to the Risk Board on progress addressing relevant weaknesses from the previous 2020/21 exercise and match investigation progress was also reported in October 2023.		

Ref	Description	Risk Rating	Minor
	However, whilst Finance completed the Audit Scotland 2022/23 NFI self-appraisal checklist for NFI Key Contacts and Users and reported this to Risk Board, the related checklist for those charged with governance included, was not completed and monitored by Risk Board reducing oversight of checklist risks e.g. awareness of emerging fraud risks; adequacy of fraud mitigations where fraud data not uploaded or investigated; communication of support for exercise to staff etc. In addition, key actions detailed in the Audit Scotland / Cabinet Office timetables and subsequent investigation of matches were not formally monitored by the Risk Board reducing oversight of progress and adequacy of resources deployed. Whilst the 2022/23 exercise was generally managed on time, certain data uploads to the secure web application were delayed by a short period and certain match reports were overlooked as described above. RAG based reporting of key timetabled tasks, with responsible officers and implementation due dates, and monitoring of the Audit Scotland NFI self-appraisal checklist for those charged with governance, would enhance oversight, help avoid delays, and potentially improve data upload and match investigation response times, and fraud identification and mitigation outcomes.		
	IA Recommended Mitigating Actions Risk Board reporting on NFI progress should be reviewed with consideration given to introducing a RAG based system of control covering Audit Scotland / Cabinet Office timetable requirements, match investigation progress, and the Audit Scotland self-appraisal checklist for those charged with governance.		
	Management Actions to Address Issues/Risks *It is acknowledged that Risk Board did not complete the self-assessment checklist for those charged with governance. For the next exercise, Key Contacts will request that an action be created for completion of the check list by the Board.* *Having considered the oversight that the Risk Board had of the 2022 NFI exercise the lead times and frequency of Risk Board meetings does not lend itself to RAG reporting on the next exercise. Based on the parameters of the next exercise the NFI Key Contacts will agree with the Risk Board the reporting requirements.*		
	Risk Agreed / **Person(s)** / **Due Date** Yes / NFI Key Contacts / May 2025		

Ref	Description	Risk Rating	Moderate
1.8	**Fraud Risk Management** – Audit Scotland NFI guidance to those charged with governance recommends ensuring awareness of emerging fraud risks so preventative action can be taken. In addition, the Council's Risk Management Policy states: • *"It is the Council's policy to be risk aware…registers and assurance maps [should be created] that reflect emerging risks, operational requirements and business objectives across the organisation [which] allows for the escalation and de-escalation of risks between risk registers."* As stated in the Council's Risk Appetite Statement, the Council is averse to risks associated with impairing financial stewardship, internal controls, and financial sustainability.		

Ref	Description	Risk Rating	Moderate
	Whilst risks relevant to the successful delivery of the 2022/23 NFI exercise were monitored by Risk Board as described at 1.4 above based on the outcome of a lessons learned review, currently emerging fraud risks are not monitored by the Risk Board or officers via a Council risk register, increasing the possibility that relevant new fraud risks will be overlooked and not mitigated against.		
	IA Recommended Mitigating Actions		
	Finance should ensure emerging fraud risks are adequately monitored using a suitable Council risk register.		
	Management Actions to Address Issues/Risks		
	The Council intends to implement a fraud risk management framework, which will take account of this recommendation.		
	Risk Agreed	**Person(s)**	**Due Date**
	Yes	Chief Officer - Finance	December 2024

Ref	Description	Risk Rating	Minor
1.9	**Publishing Fraud Investigation Achievements (Internally and Externally)** – Audit Scotland guidance (the NFI self-appraisal checklist) recommends publishing internally and externally the achievement of fraud investigators. In addition, the Council's Counter Fraud Policy states "Regular information relating to anti-fraud initiatives will be published on social media." This is with a view to deterring future instances of fraud. A dedicated NFI Council intranet page provides a comprehensive explanation of the NFI process, and this includes details of the value of fraud / error identified each year and the related notional cumulative savings calculated by the Cabinet Office. However, the annual report to Audit, Risk and Scrutiny Committee covering NFI 2022/23 outcomes was an exempt paper and details of anti-fraud initiatives have not been published in social media in line with the Counter Fraud Policy, reducing opportunities for deterring fraud.		
	IA Recommended Mitigating Actions		
	Anti-fraud initiatives should be publicised externally where possible.		
	Management Actions to Address Issues/Risks		
	NFI Key contacts will liaise with the Comms team to have press release ready for when Audit Scotland releases its report on the 2022/23 NFI, which is expected in August 2024.		
	Risk Agreed	**Person(s)**	**Due Date**
	Yes	NFI Key Contacts	August 2024

4 Appendix 1 – Invoiceable Sums and Cabinet Office Estimated Savings

Dataset	Actual 2022/23	Actual 2020/21	COES[2] 2022/23	COES 2020/21
Housing Benefit	£11k	£17k	£11k	£9k
CTRS	£35k	£1k	£17k	-
Blue Badge	-	-	£29k	£43k
Tenancy	-	-	£469k	-
Pensions	£1k	£3k	£4k	£65k
Payroll	£15k	-	£6k	-
Non-Domestic Rates	£89k	£22k	£44k	-
Main NFI Totals	**£151k**	**£43k**	**£580k**	**£117k**
ReCheck Council Tax Single-Person Discount (SPD) Review	£194k	£95k	£408k	£283k
Total Invoiceable Sums and Estimated Savings	**£345k**	**£138k**	**£988k**	**£400k**

[2] COES – Cabinet Office Estimated Savings – cumulative estimated future savings resulting from fraud / error detected via NFI exercise.

5 Appendix 2 – Assurance Terms and Rating Scales

5.1 Overall report level and net risk rating definitions

The following levels and ratings will be used to assess the risk in this report:

Risk level	Definition
Corporate	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.
Function	This issue / risk level has implications at the functional level and the potential to impact across a range of services. They could be mitigated through the redeployment of resources or a change of policy within a given function.
Cluster	This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer.
Programme and Project	This issue / risk level impacts the programme or project that has been reviewed. Mitigating actions should be taken at the level of the programme or project concerned.

Net risk rating	Description	Assurance assessment
Minor	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	**Substantial**
Moderate	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	**Reasonable**
Major	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	**Limited**
Severe	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	**Minimal**

Individual issue / risk	Definitions
Minor	Although the element of internal control is satisfactory there is scope for improvement. Addressing this issue is considered desirable and should result in enhanced control or better value for money. Action should be taken within a 12 month period.
Moderate	An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on the audited area's adequacy and effectiveness. Action should be taken within a six month period.
Major	The absence of, or failure to comply with, an appropriate internal control, such as those described in the Council's Scheme of Governance. This could result in, for example, a material financial loss, a breach of legislative requirements or reputational damage to the Council. Action should be taken within three months.
Severe	This is an issue / risk that is likely to significantly affect the achievement of one or many of the Council's objectives or could impact the effectiveness or efficiency of the Council's activities or processes. Examples include a material recurring breach of legislative requirements or actions that will likely result in a material financial loss or significant reputational damage to the Council. Action is considered imperative to ensure that the Council is not exposed to severe risks and should be taken immediately.

5 Appendix 3 – Assurance Scope and Terms of Reference

5.1 Area subject to review

Audit Scotland carries out data matching under part 26A of the Public Finance and Accountability (Scotland) Act 2000 and Section 97 of the Criminal Justice and Licensing Act 2010. This legislation provides that Audit Scotland may carry out data matching exercises or arrange for them to be carried out on its behalf.

The National Fraud Initiative (NFI) is a data matching exercise that matches electronic data within and between participating bodies to prevent and detect fraud, taking place every two years. The Cabinet Office's NFI team conducts the matching work on Audit Scotland's behalf and Audit Scotland prepares a report on the results, which participating bodies are expected to investigate.

Each participating body in the NFI is required to identify people in two key roles – a Senior Responsible Officer and a Key Contact.

The Senior Responsible Officer (usually the Chief Officer – Finance) must:

- Nominate a Key Contact.
- Ensure the Key Contact has access to the matches, via the secure NFI web application, when they become available.
- Ensure that the key contact fulfils all privacy notice requirements.

The role of the Key Contact is to:

- Fulfil the organisation's privacy notice requirements via direct communication with the organisation's Data Protection Officer or equivalent.
- Ensure that the data formats guidance and data specifications are followed.
- Nominate appropriate users to upload data submissions, investigate the matches and act as the point of contact for other bodies about a match (preferred Dataset Contact).
- Coordinate and monitoring the overall exercise.
- Ensure that outcomes from the investigation of matches are recorded on the web application promptly and accurately.

The 2022/23 NFI exercise is ongoing at the time of review with Audit Scotland due to publish the results in 'summer 2024' according to the 2022/23 NFI timetable.

5.2 Rationale for review

The objective of this audit is to review the Council's engagement and controls for actioning outputs of the National Fraud Initiative, specifically looking at the utilisation of information to gain assurance over areas such as Council Tax and Business Rates. This review will not look to recreate the NFI exercise or work on any out the outcomes.

This area has not been subject to a standalone audit previously and as such has been included in the agreed Internal Audit plan to ensure that the Council is investigating NFI matches, reporting outcomes in a timely manner and improving controls where necessary.

5.3 Scope and risk level of review

This review will offer the following judgements:

- An overall **net risk** rating at the **Corporate** level.
- Individual **net risk** ratings for findings.

5.3.1 Detailed scope areas

As a risk-based review this scope is not limited by the specific areas of activity listed below. Where related and other issues / risks are identified in the undertaking of this review these will be reported, as considered appropriate by IA, within the resulting report.

The specific areas to be covered by this review are detailed below:

- Written procedures and training
- Security Checks (for Users of NFI Web Application Tool)
- Data Protection
- Data Upload Completeness
- Match Allocation and Investigation
- Coordination and Monitoring
- Reporting of Outcomes

5.4 Methodology

This review will be undertaken through interviews with key staff involved in the process(es) under review and analysis and review of supporting data, documentation, and paperwork. To support our work, we will review relevant legislation, codes of practice, policies, procedures, and guidance.

Due to hybrid working arrangements, this review will be primarily undertaken remotely.

5.5 IA outputs

The IA outputs from this review will be:

- A risk-based report with the results of the review, to be shared with the following:
  - Council Key Contacts (see 1.7 below)
  - Audit Committee (final only)
  - External Audit (final only)

5.6 IA staff

The IA staff assigned to this review are:

- Kostas Minas, Auditor **(audit lead)**
- Andy Johnston, Audit Team Manager
- Jamie Dale, Chief Internal Auditor **(oversight only)**

5.7 Council key contacts

The key contacts for this review across the Council are:

- Andy MacDonald, Director – Corporate Services
- Jonathan Belford, Chief Officer – Finance

5.8 Delivery plan and milestones

The key delivery plan and milestones are:

Milestone	Planned date
Scope issued	02-Apr-24
Scope agreed	09-Apr-24
Fieldwork commences	15-Apr-24
Fieldwork completed	10-May-24

Milestone	Planned date
Draft report issued	31-May-24
Process owner response	21-Jun-24
Director response	28-Jun-24
Final report issued	05-Jul-24