

CEREDIGION COUNTY COUNCIL

Report to:	Governance and Audit Committee
Date of meeting:	6 June 2022
Title:	Internal Audit Counter Fraud Report 2021/22
Purpose of the report:	To provide Members with a summary of the counter fraud work undertaken by internal audit during 2021/22
Cabinet Portfolio and Cabinet Member:	Councillor Matthew Vaux, Cabinet Member for Legal and Governance, Housing, People and Organisation and Public Protection

The IA Annual Report provides a summary of the internal audit activity during the year to 31 March and incorporates the audit opinion.

In the past, the Annual Report contained a section on Fraud, outlining the type of work IA had undertaken in the area. This has now been replaced by a separate Counter Fraud Report to support IA's Annual Report at year-end.

The work undertaken on the National Fraud Initiative is included in the report: <https://www.audit.wales/publication/national-fraud-initiative-wales-2018-20>

Recommendation(s):	To APPROVE the Report
Reasons for decision:	That the Governance and Audit Committee is satisfied that the Internal Audit Section has undertaken sufficient and appropriate work in this area to support the Internal Audit Annual Report at year-end.
Appendices:	Internal Audit Counter Fraud Report 2021/22
Head of Service:	Elin Prysor Corporate Lead Officer Legal & Governance Services / Monitoring Officer
Reporting Officer:	Alex Jenkins Corporate Manager – Internal Audit
Date:	4 May 2022

Mae'r adroddiad yma ar gael yn Gymraeg.
This report is available in Welsh.

**GWASANAETHAU
CYFREITHIOL A
LLYWODRAETHU**

**LEGAL & GOVERNANCE
SERVICES**

**GWASANAETH ARCHWILIO MEWNOL
INTERNAL AUDIT SERVICE**



Cyngor Sir
CEREDIGION
County Council



ADRODDIAD ARCHWILIO 2021/22 – ATAL TWYLL

AUDIT REPORT 2021/22 – COUNTER FRAUD

Report Prepared by: Alex Jenkins,
Corporate Manager - Internal Audit

Date of Issue: 4 May 2022

Presented to Governance & Audit Committee:
6 June 2022

ADRODDIAD ARCHWILIO 2021/22 – ATAL TWYLL

AUDIT REPORT 2021/22 – COUNTER FRAUD

Introduction

Ceredigion County Council has a duty to safeguard money that should be used in the public interest. Fraudulent behaviour threatens the Council, therefore there is a high degree of commitment to ensure an effective strategy exists which is designed to prevent, detect, and identify fraud, bribery and corruption, and any other malpractice to include money-laundering.

The Council has a Strategy to Counter Fraud, Corruption and Bribery (to include Anti-Money Laundering), which is regularly reviewed and presented to Governance and Audit Committee (GAC), prior to approval by Council. The current Strategy was presented to and approved by GAC on 3 June 2021 and was approved by Council on 17 June 2021. It is supported by a suite of accompanying policies and procedures, such as the Codes of Conduct, Whistleblowing Policy, etc to acknowledge the Council's commitment to addressing fraud and minimise the potential of any risk or damage it can cause.

Counter Fraud work undertaken by Internal Audit

- 1.1 It is the responsibility of all managers to maintain sound arrangements and controls in order to prevent and detect fraud and corruption. Incidents of fraud usually arise if system controls, risk and/or governance processes are weak, or are present but not being observed.
- 1.2 IA obtains assurance from certain services as systems are in place in order to detect and prevent fraud, eg:
 - The Council was an early adopter of the Governments secure e-mail standard to help reduce the risk of e-mail addresses being used fraudulently,
 - Payments system incorporates an in-house software programme to detect duplicate payments,
 - Council tax single person discounts (SPD) declarations requested and reviewed annually,
 - Mandate fraud detection procedures in place, and
 - Centralisation of payments section to reduce order / invoice anomalies.
- 1.3 The methods of reporting of any suspected fraud, theft, irregularity, improper use or misappropriation of the Council's property or resources is contained in the Council's Strategy to Counter Fraud.

- 1.4 This could result in an investigation being undertaken by Internal Audit (IA). The Corporate Manager - Internal Audit (CMIA) is an Accredited Counter Fraud Technician (ACFTech) whilst the Audit Manager (AM) holds a CIPFA Certificate in Investigative Practice (CCIP). The Council also periodically trains a 'pool' of internal investigators across all services; and certain enforcement staff have PACE training.
- 1.5 IA's Annual Audit Plan has a section on "Counter Fraud" and the service has a right of access to:
- Enter any Council premises or land at any reasonable time,
 - Access all assets, records, documents, correspondence and control systems relating to any financial and other transactions of the Council,
 - Require and receive any such information and explanations considered necessary concerning any matter under consideration / examination,
 - Require any employee of the Council to account for cash, stores or any other Council property under his/her control, and
 - Have access to records belonging to third parties, such as contractors or partnership agencies, according to the relevant contractual terms.

This forms part of the Council's Financial Regulations and Accompanying Financial Procedures contained in the Council's Constitution.

- 1.6 The Council is also proactive by participating in Audit Wales' 'National Fraud Initiative' (NFI) exercise, which is a national data matching exercise that tackles a broad range of fraud risks faced by the public sector. This work is co-ordinated throughout the Council by the AM.
- 1.7 The NFI testing is complemented by further data analysis exercises, where possible. IA has used the IDEA system to analyse data in the past, but currently uses the Active Data software which works alongside Excel. These systems can perform different audit-relevant tasks using data matching techniques and features to help detect anomalies.
- 1.8 External influences which may have a bearing on Council services may also trigger a special investigation eg there continue to be many fraudulent attempts against local authorities to change suppliers' bank account details (mandate fraud). IA receives notifications from CIPFA, NAFN (National Anti-Fraud Network) and other external bodies which may alert the Council of any prevalent national / corporate fraud.
- 1.9 This ensures issues are brought to IA's attention promptly and can be dealt with by reinforcing appropriate controls beforehand.
- 1.10 Similarly, the CMIA is in contact with the heads of audit from all the Welsh local authorities, who meet on a quarterly basis, and will also circulate any correspondence to members citing any fraudulent attempts / incidents they

have experienced / are made aware of. The North Wales' heads of audit also meet and share this information.

- 1.11 Audit Wales requires authorities to report details of all frauds to their External Auditors, and to the Chair of GAC.
- 1.12 Where cases of fraud or other wrongful activity are discovered and investigated, it may also be necessary for IA to undertake a separate review to address the weaknesses discovered and recommend actions to strengthen controls. The corrective actions required following such investigations by IA are reported at their conclusion in the quarterly Progress Reports to the GAC. Follow-up reviews are conducted by IA where appropriate.
- 1.13 However, it must be stressed that assurances re fraud can never be absolute.

National Fraud Initiative

- 2.1 The NFI is a data matching exercise which helps to detect and prevent fraud. It is conducted in Wales by the Auditor General under his statutory data matching powers set out in out in the Public Audit (Wales) Act 2004.
- 2.2 The NFI matches data across organisations and systems to help public bodies identify fraud and overpayments at a national level. The Auditor General collaborates with the Cabinet Office, Audit Scotland and the Northern Ireland Audit Office to run NFI as a UK-wide exercise. Since its commencement in 1996, NFI exercises have resulted in the detection and prevention of more than £35.4 million of fraud and overpayments in Wales and £1.69 billion across the UK.
- 2.3 The NFI is constantly developing, in order to continue to prove an effective tool for detecting and preventing fraud and error across the UK. It acknowledges that fraudsters are always looking for new areas to exploit and make money at others' expense. NFI tries to counter this threat by continually working with the counter fraud community, to come up with new ways of using data to identify fraud across the public sector - both for existing or for new emerging fraud problems.
- 2.4 The main NFI exercise takes place every two years across multiple datasets, including Blue Badges, Concessionary Fares, Council Tax Reduction Scheme, Housing Waiting Lists, Licences, Payroll, Procurement and Trade Creditors. Matching between Council Tax and Electoral Register data takes place annually
- 2.5 Local Authorities are currently playing an important role in the Covid-19 relief programme, issuing a wide range of funding support to businesses and individuals. With the NFI already embedded into local authority counter fraud strategies, it is ideally placed to extend its remit in order to help local authorities target these additional fraud risks.
- 2.6 Staff at Ceredigion have undertaken work on the 2020-21 reports, including new datasets will be available this year for Covid-19 Business Grants. This data

matching allows potentially fraudulent claims and payments to be identified across a range of the Council's services and is beneficial to the work in reducing fraud risk within the Authority.

WG Business Grants

- 3.1 WG worked in partnership with local authorities to deliver a series of grants to qualifying businesses during the pandemic.
- 3.2 The Council's Finance Services administered these grants, and strived to process as many applications as possible over a short period of time, to ensure payments were made swiftly to those businesses that required this assistance.
- 3.3 However, it is whilst under such pressure that errors are more likely to occur, and that fraudsters can easily infiltrate a system. Public Finance noted in an article that these funds are "particularly vulnerable to fraud during crises, because of the volume of money involved and the speed with which it needs to be spent or distributed". A recent BBC news article on increased incidence of fraud against the Department of Work and Pensions confirmed this:

Link: [Universal credit fraud and error at new high - BBC News](#)

- 3.4 This system therefore provided added risks to the Council, as sums paid in respect of the original covid-19 grants were either £10k or £25k for which strict eligibility criteria existed. Subsequent grants released during 2021-22 by WG were offered for both business that occupy properties with a rateable value and also a Discretionary grant for those businesses that do not. Grants were set at different amounts between £1,000 and £5,000 dependent on property rateable value and type of grant.
- 3.5 The Finance team had a number of good controls in place in their systems, such as:
 - All fields in the application forms were mandatory;
 - NNDR grants were not paid if the Business Rate reference number on the grant application form was invalid, or an application had already been submitted against a Business Rate reference number according to the grant system;
 - Recent bank statements requested to verify applicants' details against existing records;
 - A separation of duties between the application process and payment authorisation; and
 - Payment details held in spreadsheets and checked for duplicate entries.

The Monitoring Officer also sent out a reminder by email to Members and officers for the need to declare an interest if they were in receipt of a grant.

- 3.6 After discussions with the Finance team, it was agreed that IA would assist the control process mainly by:

- Reviewing a sample of applications with queries prior to payment (as it would be easier to stop a payment than to recover any wrongly-paid monies after payment);
- Reviewing any suspected fraudulent applications; and
- Scrutinising the payment schedules using the Active Data analytics software to check for any anomalies.

3.7 This change to IA's plans was made as it added value to the Council's operations due to the changing circumstances. As a service, it demonstrated IA can react to the Council's changing pressures and can assess and respond to reprioritised risks. Although this does seem to stray from the role normally expected from IA, the Internal Audit Standards Advisory Board has supported such actions in this situation (as per guidance received).

3.8 The IA team has spent a number of days assisting with this work during the year, in order to provide assurance that additional steps were taken to reduce the risk of fraud, during which IA:

- Checked a number of applications received and payments made, for anomalies / duplicates,
- Ran duplicate checks on reference nos, names, bank account nos, and email addresses following pay runs using ActiveData,
- Checked records for known fraudulent applicant details as notified to the Council by NAFN Data & Intelligence Services, and other Local Authorities using ActiveData,
- Reported any phishing emails received to the National Cyber Security Centre,
- Verified company details with Company House where applicable, and
- Attended appeal panel meetings to help ensure that application decisions were consistent.

3.9 Staff have foiled several suspected fraudulent attempts by identifying suspicious email addresses, bank statements and supporting evidence whilst assessing and checking the grant applications.

3.10 Any suspected fraudulent payments detected are being investigated.

3.11 This work is still on-going, as there may be further anomalies to resolve.

Other & On-going Work

- 4.1 Two separate incidents of suspected mandate fraud (when someone impersonates a third party such as a supplier and demands urgent payment) were discovered by Payments staff during the year. Both of these were reported to the National Cyber Security Centre.
- 4.2 A lengthy exercise was undertaken to check new creditors set-up during the pandemic. IA have compiled a spreadsheet of these creditors and the payments made to each one. IA staff are currently working through it to ensure these suppliers are genuine, and have provided appropriate goods / services to the Council.
- 4.3 There are two ActiveData Counter-Fraud exercises similar to the above planned for 2022/23 as detailed in the IA Strategy & Plan that was presented to GAC on 10 March 2022.
- 4.4 WG announced Cost of Living support payments in quarter 4 2021/22 to be rolled out in quarter 1 2022/23. IA will support the Finance team with Counter Fraud measures by running duplicate checks on reference nos, names, addresses, bank details and email addresses.
- 4.5 The Council's ICT service worked in conjunction with Bob's Business, a cyber security training provider, to arrange training for staff on awareness of phishing attempts. Staff took part in a simulated phishing campaign: 'Think Before you Click'. The purpose of the exercise was to educate those that may fall victim to a phishing email by providing them with the relevant information to stay protected. This will ensure a safer working environment for all staff and keep the organisation more secure from cyber-attacks.

Conclusion

- 5.1 IA will continue to look for counter fraud measures in place when undertaking all audits and advise managers and services of ways to strengthen controls, risk and governance processes where appropriate.