



**1. Leadership and Culture**

<p><b>Local Government Findings:</b></p> <p>Across local authorities there is an absence of sector-wide strategic leadership, guidance, coordination and oversight of counter fraud. Within the individual authorities we found statements espousing a zero tolerance of fraud in policies and strategic documents. But there is much more that can be done to re-enforce the tone from the top at a practical level. We found examples where the leadership team actively promotes the importance of a good anti-fraud culture through awareness campaigns, newsletters to staff and active engagement with counter-fraud teams. But we also found in many authorities that there was little evidence that the message is driven down from the top and little priority is given to counter-fraud work. There were often competing priorities and, as a result, little time was given to counter-fraud and it often had a low profile.</p>	<p><b>Management Response:</b></p> <p><b>Strategic leadership and coordination</b> Council officers actively participate in a number of groups and forums in order to continue to understand fraud risks, trends and best practice approaches to prevent and detect fraud. The primary groups include the Welsh Chief Auditors Group, in which strategic and operational fraud matters are discussed, and the Wales Fraud Officers Group, which is a networking and best practice engagement mechanism for Council counter-fraud practitioners.</p> <p>The Council is a member of the National Anti-Fraud Network (NAFN), which acts as a hub for the collection, collation and circulation of intelligence alerts, and officers attend the Wales Fraud Forum and Audit Wales Good Practice Exchange events for best practice advice and insight.</p> <p><b>Championing anti-fraud culture</b> In the last 12 months, significant attention has been given to reinforcing the Council’s counter-fraud culture. In July 2019, Cabinet approved a Counter-Fraud and Corruption Strategy, which represented a strong corporate commitment to retaining and enhancing resilience in fraud risk management.</p>
<p><b>Recommendations:</b></p> <p><b>R1.</b> The Welsh Government should enhance its strategic leadership of counter-fraud across the public service in Wales, playing a coordinating role where it can, while recognising that individual bodies remain responsible for their own counter-fraud activities.</p> <p><b>R2.</b> All public bodies should champion the importance of a good anti-fraud culture and actively promote its importance to give confidence to staff and members of the public that fraud is not tolerated.</p>	<p>The Strategy contained a joint foreword from the Leader of the Council and the Chief Executive, and was supplemented by a combination organisational-wide awareness and training, to engage the whole workforce to reaffirm the responsibility of all of us to prevent, detect and report potential fraud. A schools version of the Strategy was prepared, advocated to all schools via Headteachers and Chairs of Governors, and followed up with a counter-fraud control risk self-assessment (CRSA) exercise during the autumn term 2019 and targeted audit testing to reinforce messages within Cardiff schools.</p> <ul style="list-style-type: none"> <li>• <u>Fraud awareness training</u> has been delivered through a combination of eLearning for those with computer access, and on a face-to-face training for non-pc using officers, Headteachers, and school governors.</li> <li>• <u>The Council participated in International Fraud Awareness week</u> (17-23 November 2019). The campaign included video messages, articles and guidance for all staff from the Head of Finance on Mandate fraud, the Head of Procurement on Procurement Fraud, and the Chief Digital Officer on Cyber Crime. There is a commitment to participating in the forthcoming International Fraud Awareness week (15 - 21 November 2020).</li> </ul>



## 2. Risk management and Control framework

### Local Government Findings:

While some local authorities have undertaken fraud risk assessments, there were many who had not prepared a fraud risk assessment for several years. Some bodies in these sectors did not have a fraud risk assessment and therefore had not properly assessed the likelihood or impact of the risk. Without this key component, bodies cannot direct resources appropriately or adequately mitigate the risks of losses due to fraud.

Our work also identified that, even where risk assessments were undertaken, they may not be integrated within the wider risk management framework. Fraud is not commonly reflected in corporate risk registers. We did not find many coordinated mechanisms for ensuring that fraud risks are appropriately communicated, owned and monitored within the audited body. Instead, fraud risk assessments are often held as standalone documents without any corporate ownership or active management of the risk. As a result of this approach, fraud risks are not adequately shared across departments.

There were good examples in local authorities of raising awareness of scams with local residents. We found that, in general, public bodies across all sectors have internal control frameworks that are well established and internal audit teams test controls as part of their annual programmes of assurance work. However, we found that internal audit teams do not always consider the fraud risks associated with systems as part of their work programmes. Furthermore, where new systems and processes are established, we found that organisations are not always using counter-fraud contacts and internal audit teams to try to design fraud out of systems.

### Recommendations:

**R3.** All public bodies should undertake comprehensive fraud risk assessments, using appropriately skilled staff and considering national intelligence as well as organisation-specific intelligence.

**R4.** Fraud risk assessments should be used as a live resource and integrated within the general risk management framework to ensure that these risks are appropriately managed and escalated as necessary.

### Management Response:

#### Comprehensive fraud risk assessments

The risk of fraud, bribery and corruption is included on the corporate risk register, and reviewed by the Senior Management Team at least quarterly, considered by Audit Committee quarterly and subject to twice-yearly Cabinet review.

The management of fraud, bribery and corruption is included within Senior Management Assurance Statements (SMAS). Processes require each directorate to provide a management response and self-assessed rating of governance maturity twice a year as part of SMAS returns.

A number of directorate risk registers contain risks associated with fraud, bribery and corruption. Risk registers are subject to regular Internal Audit review.

#### Integrated fraud risk assessments

The Investigation Team reviewed the mid-year SMAS responses in 2019/20, and provided commentary on the consistency of the responses with the knowledge and awareness of the Team.

The Team has developed a checklist for circulation as part of forthcoming SMAS assessments to support a comprehensive and consistent of fraud, bribery and corruption assurance.

All Directorates participated in a fraud and corruption tracker exercise during 2019/20, based on a model designed by the Chartered Institute of Public Finance and Accountancy (CIPFA). This enabled a focussed verification and discussion on the volumes and values of fraud across the Council, and the pertinent areas of risk. There is a commitment to continuing to engage Senior Management Team in the annual fraud tracker exercise.

As part of the year-end fraud and corruption tracker exercise for 2019/20, due for response to CIPFA on 25 September 2020, the Investigation Team will offer support and guidance to directorates in the assessment, monitoring and management of fraud risks.



### 3. Policies and Training

#### Local Government Findings:

Whilst NHS bodies have each developed comprehensive counter-fraud strategies, we found that only a few other public sector bodies had done so. Such strategies set out clear approaches to managing fraud risks along with responses and actions, they define roles and responsibilities and are cross-referenced to other policies so that they can be readily understood by staff.

The NHS has a policy of proactively publicising successful fraud cases. The NHS Counter Fraud Service does this by issuing press releases and engaging with local media for interviews and promotional opportunities. Publicity helps raise awareness of fraud risks and also deters staff and contractors from committing fraud. By publicising counter-fraud work and raising awareness of the effects of fraud, the NHS involves staff, key stakeholders and the public in the fight against fraud.

Some local authorities take the view that publicising cases can be reputationally damaging and are therefore reluctant to publish such information.

Our audit work also identified wide variation in levels of training and awareness-raising specifically relating to counter-fraud across the Welsh public sector.

#### Recommendations:

**R5.** All public bodies need to have a comprehensive and up-to-date set of policies and procedures which together represent a cohesive strategy for identifying, managing and responding to fraud risks.

**R6.** Staff working across the Welsh public sector should receive fraud awareness training as appropriate to their role in order to increase organisational effectiveness in preventing, detecting and responding to fraud.

**R7.** Cases where fraud is identified and successfully addressed should be publicised to re-enforce a robust message from the top that fraud will not be tolerated.

#### Management Response:

##### Policies and Procedures

The Council has a suite of operational policies in place to support Counter-Fraud and Corruption Strategy. All policies are subject to ongoing review, and are updated as appropriate. Following review, an updated Anti-Money Laundering Policy will be due for Audit Committee consideration this municipal year, ahead of a request for Cabinet approval.

##### Fraud Awareness Training

Since July 2019, fraud awareness training has been delivered through a combination of eLearning for those with computer access, and on a face-to-face training for non-pc using officers, Headteachers, and school governors.

- More than three thousand, eight hundred employees have completed the eLearning module or attended one of the thirty-seven face-to-face sessions delivered
- More than seventy Headteachers have received Fraud Awareness Training during their conferences
- Two face-to-face sessions have been delivered to School Governors, with thirty-five attendees.

##### Publicising Fraud Cases and Outcomes

The Council has a Fraud Publicity Policy, which includes the aim to communicate positive action effectively, to provide reassurance to the public that it is taking a firm line on counter fraud issues and that it has robust and effective procedures in place to tackle fraudulent activity.

Whilst there have been significant internal communications on counter-fraud in recent years, there has been limited external communication. Appropriate opportunities for communication will continue to be considered as part of counter-fraud activities.



## 4. Capacity and Expertise

### Local Government Findings:

Insufficient capacity arose frequently as a key challenge faced by public bodies in their efforts to combat fraud.

In local government, some officers are sceptical about the levels of fraud within their organisations and question the need for additional resources. However, these same local authorities allocate little resource to counter-fraud arrangements, do not have robust fraud risk assessments and the following up of matches from the National Fraud Initiative is assigned a low priority. Their assumptions about low levels of fraud run contrary to all the research being done by recognised leaders in the field such as CIPFA and the National Crime Agency

Local authorities suffered a significant loss in counter-fraud capacity when the independent Single Fraud Investigation Service (SFIS) was created in 2014. Our work found that the counter-fraud arrangements were generally more advanced in the local authorities that retained a dedicated and specialist counter-fraud resource.

In 2018 the UK government launched the Counter-Fraud Profession to enhance overall counter-fraud capability across government. The profession develops the skills of specialist staff and moves beyond the traditional focus of investigations, placing greater emphasis on fraud prevention and the use of data analytics.

### Recommendations:

**R8.** All public bodies need to build sufficient capacity to ensure that counter-fraud work is resourced effectively, so that investigations are undertaken professionally and in a manner that results in successful sanctions against the perpetrators and the recovery of losses.

**R9.** All public bodies should have access to trained counter-fraud staff that meet recognised professional standards.

**R10.** All public bodies should consider models adopted elsewhere in the UK relating to the pooling /sharing of resources in order to maximise the availability of appropriately skilled staff.

### Management Response

#### Capacity

The corporate Investigation Team comprises 2.5 Fte, dedicated to the prevention, detection and investigation of suspected fraud or financial impropriety.

There is also an established pool of trained officers in place across the Council, to support the delivery of internal disciplinary investigations, as required.

#### Trained counter-fraud staff

Two members of the corporate Investigation Team are professionally qualified counter fraud officer's, accredited with Portsmouth University, with the third team member being a former police officer with many years of professional expertise.

#### Pooling / Sharing of resources

There was an investment in the corporate Investigation Team in September 2019, with the appointment of an additional Investigator. This post was considered as necessary capacity to deliver the caseload of professional investigations, and to support the aspirations of the Counter-Fraud and Corruption Strategy, in reinforcing the Council's counter-fraud culture.

The Council has a dedicated Investigation Team, which is not the case across all local authorities in Wales. The Team used to contain housing benefit / council tax benefit investigators who were transferred to SFIS in 2014. A core corporate investigation resource was retained, and the responsibility for housing benefit / council tax benefit investigations transferred to the DWP alongside the investigation resource.

There is active officer participation in professional networks, but there has not been a requirement to date for pooling/sharing of counter-fraud resources in the delivery of counter-fraud and investigation activities.

The Audit Manager will continue to monitor, report and respond to the caseload, activities and resources of the corporate Investigation Team.



## 5. Tools and Data

### Local Government Findings:

Generally speaking, we found that more work is needed to bring counter-fraud tools and methodologies up to date to reflect the new world of cyber attacks and digitally-facilitated crimes. Many local authorities and central government bodies we looked at as part of our fieldwork did not have information security policies that reflected the risks associated with cyber crime.

Our review identified only a few examples of data analytics being used as a means of preventing fraud.

We found that some local authorities and central government bodies did not have a fraud response plan that was communicated to all staff

### Recommendations:

**R11.** All public bodies need to develop and maintain dynamic and agile counter-fraud responses which maximise the likelihood of a successful enforcement action and re-enforces the tone from the top that the organisation does not tolerate fraud.

**R12.** All public bodies should explore and embrace opportunities to innovate with data analytics in order to strengthen both the prevention and detection of fraud.

### Management Response

#### Dynamic and agile counter-fraud responses

The Council has a suite of information security policies, and the Council's privacy policy allows for the lawful use and sharing of data for fraud prevention and detection.

Internal Audit staff advocate the use of data analytics to prevent the risk of fraud or error at the point of processing applications and claims. This will continue in audit engagements going forward.

The Council participates in the proactive NFI data matching exercise, and appropriately investigates matches.

All fraud alerts received from NAFN, wider networks, and colleagues in other local authorities are actively followed up.

#### Explore and embrace opportunities to innovate with data analytics

There is ongoing consideration of data analytics for the prevention and detection of fraud.

In 2020/21, there was use of targeted data analytics to provide assurance on the administration of grants to businesses on behalf of Welsh Government.

- The Council has used data analytics to verify bank and business credentials and flag anomalies and fraud risks for review.
- Additionally, the Team is participating in a pilot NFI data matching exercise coordinated by Audit Wales, to provide further post award assurance.



## 6. Collaboration

### Local Government Findings:

Our field work across forty public sector bodies in Wales found that collaboration was insufficiently developed, reinforcing the findings of our 2019 review

Within local authorities and central government bodies there are some good examples of bodies working jointly and some regional networks, but these tend to be informal arrangements and there is no consistency in approach.

We found that some local authorities do not invest much resource into following up NFI matches and these are often the same authorities in which counter-fraud arrangements were limited.

There were very few examples of organisations working frequently across internal and external boundaries and sharing information. Common reasons for this lack of collaboration was lack of time and resources, and concerns about the sharing of data.

### Recommendations:

**R13.** Public bodies should work together, under the Digital Economy Act and using developments in data analytics, to share data and information to help find and fight fraud.

### Management Response

#### Collaborative data / information sharing to fight fraud, via data analytics

There are effective informal officer networks in place to share fraud intelligence, risks and good practice at practitioner and chief auditor levels.

NFI matches are progressed, with details of cases identified, closed and associated outcomes, reported to Audit Committee.

The Investigation Team has supported the development of, data analytics in NFI, with ongoing participation in a business grants pilot exercise.

To date, the Council has made use of data analytics through participation in NFI and wider initiatives, coordinated by professional organisations in which risk indicators have been integrated for targeted investigation.

There is ongoing consideration of the use of data sharing and fraud hubs at practitioner and chief auditor levels within Welsh networks. Data sharing activities require careful consideration of the purpose, scope, resourcing and benefits.



## 7. Reporting and Scrutiny

### Local Government Findings:

In the local government sector, fewer than half the authorities report information about fraud cases, losses and recoveries to their audit committees on a regular basis

Audit committees outside of the NHS Wales have not been sufficiently proactive in recognising the increasing risk of fraud and in asking the searching questions necessary about the matching of resources to risk or about the lack of information being supplied about fraud risk.

### Recommendations:

**R14.** Public bodies need to collate information about losses and recoveries and share fraud intelligence with each other to establish a more accurate national picture, strengthen controls, and enhance monitoring and support targeted action.

**R15.** Audit committees must become fully engaged with counter-fraud, providing support and direction, monitoring and holding officials to account.

### Management Response

#### Collating, reporting and sharing information

The Audit Committee receives regular counter-fraud progress reports, which contain details of the activities, campaigns and work led by the corporate Investigation Team.

Progress reports include *(with a comparison to the same period in the prior year)*:

- Details of the number of cases identified for investigation, the number of ongoing cases, and the number of concluded cases over each reporting period.
- A breakdown of the financial value of closed investigations.
- The outcomes of concluded investigations - the value identified for recovery, and details of sanctions.

The Internal Audit and Investigation Teams work in synergy, through which audit engagements are planned to follow up and provide assurance on the control environment, where control gaps have been identified.

#### Audit Committee engagement

The Audit Committee:

- Receives regular reports on the counter-fraud activities and work led by the corporate Investigations Team.
- Receives regular reports on the work and findings of the Internal Audit Team.
- Receives updates on SMAS exercises twice a year and corporate risk management quarterly.
- Invites senior officers to Audit Committee meetings, to provide an account of the control environment for their areas of responsibility.