Report sponsor: Director of Financial Services
Report author: Head of Internal Audit and Head
of Revenues, Benefits and Exchequer Services

Counter Fraud Framework and Annual Report 2019/20

Purpose

1.1   Acknowledging and mitigating the risk of fraud and corruption is critical to sound financial management and ensuring that every pound spent by local authorities supports the communities we serve. Fraud costs the government an estimated £52 billion every year. Fraud against public bodies takes money away from the vital public services that citizens rely on and can damage trust in the public sector.

1.2   This Council is committed to the prevention, deterrence, detection and investigation of all types of crime, especially fraud and corruption, committed against it and the systems it administers.

1.3   The Annual Report attached at Appendix 1, outlines the effectiveness of the Council's current counter fraud framework.

Recommendations

2.1   To note the actions taken and the progress being made on counter fraud activities across the Council.

Reasons

3.1   The Audit and Accounts Committee is responsible for providing assurance to the Council on the effectiveness of the governance arrangements, risk management framework and internal control environment.

Supporting information

Fraud Landscape

4.1   The Office for National Statistics states that one in 16 members of the population is likely to fall victims. The Government's Economic Crime Plan 2019 states that the number of fraud offences rose by 12% during 2018 to 3.6 million – constituting a third of all crimes in the UK.

4.2 The Fighting Fraud and Corruption Locally Strategy - A strategy for the 2020s states that the last, most reliable and comprehensive set of local authority fraud figures was published by the National Fraud Authority in 2013, and indicated that the fraud threat may have been costing the UK approximately £52bn a year. Within these figures the threat to local authorities totalled £2.1bn. More recent estimates are higher. The Annual Fraud Indicator produced by Crowe Clark Whitehill estimated that figure may be as high as £7.8bn in 2017 of which procurement fraud was estimated as £4.3bn. This study estimated that the total threat faced by the public sector was £40.4bn.

4.3 Research published by the Chartered Institute of Public Finance and Accountancy (CIPFA) in March 2020, found that two-thirds of local government professionals thought that fraud was a major risk for councils. The survey also showed that seven out of 10 professionals believe poor organisational controls leave local authorities vulnerable to fraudsters. Nearly half (49%) felt that staff were not adequately trained to identify fraudulent activity.

4.4 The CIPFA Fraud and Corruption Tracker (CFaCT) survey gives a national picture of fraud, bribery and corruption across UK local authorities and the actions being taken to prevent it. It aims to:
   • help organisations understand where fraud losses could be occurring
   • provide a guide to the value of detected and prevented fraud loss
   • help senior leaders understand the value of anti-fraud activity
   • assist operational staff to develop pro-active anti-fraud plans.

4.5 The key results from the 2019 CFaCT national survey were:
   • The total estimated value of fraud detected or prevented by local authorities in 2018/19 was approximately £253m.
   • The average value per fraud remained at £3,600 in 2018/19.
   • The number of frauds detected or prevented had decreased to 71,000 from the 80,000 cases found in 2017/18.
   • Council tax fraud represented 78% of the identified instances of fraud with an estimated value of £30.6m.
   • The estimated volume and value of insurance fraud cases in the UK more than doubled in 2018/19 compared to the previous year.
   • The estimated average value per case of Blue Badge fraud had increased from £499 to £657 in 2018/19.
   • For 2018/19, the three greatest areas of perceived fraud risk continued to be procurement, council tax single person discount (SPD) and adult social care.
   • For 2018/19, the four main types of fraud (by volume) that affect local authorities continued to be council tax, housing, Blue Badge fraud and business rates.

4.6 Fraud, bribery and corruption are constantly evolving threats that undermine an organisation's financial resilience, and the Council needs to make sure that it has an effective Counter Fraud Framework in place to help minimise the risk of fraud. No organisation can prevent all financial crime, but what can been done is put in place measures to ensure that the Council has an awareness of the risks they face in a constantly changing world and are equipped to mitigate these.

Counter Fraud Framework

4.7   The Council has committed to a programme of zero tolerance regarding fraud and seeks to appropriately investigate all allegations of crime that are reported to it. The Council will ensure cases are appropriately sanctioned where applicable.

4.8   The Council's Counter Fraud Framework is described in the following paragraphs.

<u>Policies and Regulations</u>

4.9   The Council has several policies that are part of a coherent and consistent Counter Fraud Framework that enable everyone to understand and implement arrangements enabling compliance. In conjunction with related policies and key documents it will also enable our colleagues, partners etc to identify and effectively report a potential breach.

4.10   The key policies which support the Framework include:
- The Code of Conduct,
- Financial Procedure rules and Contract procedure Rules
- Anti-Fraud & Corruption policy
- Whistle Blowing Policy.
- Anti-bribery policy - outlining measures to combat acts of bribery by or to anyone carrying out business for or on behalf of the council;
- Anti-money laundering policy - detailing the responsibilities of members and officers, in particular the need to promptly report suspicions;
- Fraud response plan - providing guidance on reporting concerns and the investigation process;
- Sanctions policy - explaining how to determine which sanctions are appropriate when fraud or corruption is identified.

4.11   The framework is also supported by the assurance work of internal audit, pro-active work around the prevention and detection of fraud by the dedicated Counter Fraud team, the Council's Financial Investigator based in Trading Standards, work with other organisations nationally as part of the wider anti-fraud agenda, and specific work to minimise the risk of cyber fraud, through such exercises as penetration testing.

<u>Internal Audit</u>

4.12   Within the Council the responsibility to control the risk of fraud occurring resides at all levels of the organisation. It is the responsibility of management to ensure that a sound system of internal control exists within their area of responsibility, Internal Audit will review arrangements periodically to provide assurance to relevant stakeholders. Following internal audit investigations changes to systems and processes may be necessary, if so, formal recommendations will be made.

4.13   The remit of Internal Audit includes the delivery of a risk based proactive counter fraud programme. The programme takes into consideration emerging trends across the public sector, proven cases of fraud or corruption and other specific areas where there is an increased risk of fraud or corruption. As part of the proactive detection of fraud and corruption, we undertake data analytics within the council and where relevant between other public sector bodies. In conducting data matching exercises, we ensure compliance with all relevant legislation such as the Data Protection Act 2018.

4.14   In addition, a number of staff within Internal Audit are trained and qualified to the level of accredited counter-fraud officers who investigation expertise will be pivotal in ensuring a corporate fraud response is effectively maintained.

Counter Fraud Team

4.15   The Counter Fraud Team consisting of 3 accredited FTE's provide a robust response to fraud referrals received. This is soon to become four investigators following temporary funding for an additional post rom the Housing Revenue Account to focus on tenancy and other housing related frauds.

4.16   It provides a Single Point of Contact (SPOC) for the Department for Work and Pensions and work jointly on appropriate matters. The team have initiated a forum for partner agencies to meet and promote best practice.

4.17   The team conducts pro-active exercises to prevent and detect fraud and delivers bespoke fraud awareness training to staff and partners

4.18   The team work closely with Internal Audit, the Councils financial investigator and legal team to provide a co-ordinated fraud response. It actively supports other law enforcement agencies to prevent and detect fraud and work jointly on operations where appropriate.

Financial Investigator

4.19   Within Trading Standards, the Council has an accredited Financial Investigator with powers authorised by the National Crime Agency under the Proceeds of Crime Act (POCA) 2002 to investigate financial crime, which includes cash seizure, the confiscation of assets and the restraint of assets, as well as money laundering. The officer also has Part 8 investigatory powers to conduct such investigations.

Counter Fraud work with other organisations

4.20   The Council is required to participate in the biennial National Fraud Initiative data matching exercise administered by the Cabinet Office. This exercise, which compares a wide range of data between publicly funded bodies, includes payroll, pensions, creditors, social care payments and concessionary travel.

4.21   We are committed to enhancing partnership working and information sharing as a means to reducing fraud and corruption. Where appropriate, information will be shared with anti-fraud networks such as Action Fraud and the National Anti-Fraud Network, as well as other local authorities and public sector bodies, to enable the identification of patterns and sharing of good practice.

Cyber Security

4.22   Security incidents can include a range of situations which could lead to damage to operational effectiveness, harm to reputation both organisationally and personally. All breaches of Information Security, actual or suspected are investigated, reviewed and acted upon.

4.23 The Council has a Senior Information Risk Owner (SIRO) which is the Director – Digital and Customer Management. It also has IT and Information Governance policies in place to ensure compliance with laws and regulations and to provide guidance to everyone with a DCC account (email address/login).

4.24 The risk of Cyber security is identified in the Council's risk register. The Council has a number of controls and actions in place to minimise the vulnerability of the Council 's IT estate to cyber-attacks:

- Perimeter security i.e. firewalls etc. A 'defence in depth' approach is adopted with security controls at the network perimeter and staff end user devices.
- Anti-malware software – software is upgraded as required.
- PC Patching Programme - Work is ongoing to identify a new toolset to assist in software patching and enhanced auditing capabilities
- Information Security Working group (ISWG) meets monthly - looks at all threats and activities the council needs to take to counter those threats.
- Incident response procedures - Incident response procedures are in place and regularly reviewed by the ISWG
- GDPR and Cyber Security eLearning - There is a mandatory e-Learning course on Cyber Security for all staff who use a computer. The Information Governance team has organised informal drop in sessions which are intended to cover all GDPR and data protection queries.

4.25 The IT Audit team provide assurance on risk mitigation with the Council's IT infrastructure and internal/externally hosted systems. Their work is tailored around evaluation of key cyber security controls that help the Council to block or minimise known attacks. At a technical level, their work helps to minimise the Council's risk to a compromise of personal and sensitive data, or the availability of business-critical information systems required for service delivery. From a business perspective, control advice issued through cyber security auditing helps reduce the likelihood of financial damage, reputational damage, non-compliance penalties or privacy violations of citizen's personal information.

Fraud Awareness Training

4.26 We continue to nurture a strong anti-fraud and corruption culture within the Council, which is key to ensuring the prevention and detection of offences. Collaboration between Internal Audit and the Counter Fraud Team has seen the development and delivery of specific and targeted, as well as general, Fraud Awareness Training throughout the Council to ensure this culture becomes engrained in the minds of Councillors and employees. The Counter Fraud team also provide bespoke training for other local authorities on a chargeable basis.

Covid-19 and the Increased Fraud Risk

4.27 Unfortunately, in times of crisis, criminals are ready and willing to take advantage of the opportunities presented by societal disarray. The coronavirus crisis has seen a rise in many different types of fraud, and local authorities need to ensure they remain alert to current and future fraud risks. The Government has issued warnings to specific sectors on the increase in coronavirus related scams and cyber-attacks. Data from Experian and the National Hunter Fraud Prevention Service shows a rise in fraud rates in April 2020 of 33% when compared with previous monthly averages.

4.28 One of the key fraud risks for local government arising during the pandemic is the attempt to fraudulently access those government grants/funds made available to help ease the economic impact of the pandemic that Councils have been asked to administer. This funding is made up of the Small Business Grant Fund and the Retail, Leisure and Hospitality Grant Fund and the Local Authority Discretionary Grants Fund.

4.29 Derby designed its system and processes for payments made under the Business Support Grant Schemes with fraud prevention in mind. Several pre-payment checks were carried out on each application by the team, which included verification of business rate details, bank accounts etc. Applicant details were also checked using external resources provided such as Spotlight and the National Fraud Initiative checking service with Experian. Internal audit also ran data matching checks within and across each Business Support Grant scheme.

4.30 The Government has developed guidance which is intended to set out the overall broad framework for assurance activities that Local Authorities are required to undertake. This was sent out in mid-June and requires all Local Authorities to undertake a Fraud Risk Assessment as part of their assurance plans. The Department for Business, Energy & Industrial Strategy (BEIS) will also collect monthly assurance reports from Local Authorities, starting at the end of July. Guidance regarding the debt recovery and clawback process has been promised by August at the latest. In September, BEIS will communicate the government's post payment assurance process.

Key Themes and Strategy Going Forward

4.31 There are several key themes that the Council will be exploring going forward. This will be led by Internal audit and the Counter Fraud team, as part of their on-going collaboration to tackle the risk of fraud and corruption to the Council:

- Culture: the importance of a robust counter fraud culture, supported by effective systems and controls.
- Technology: the increasingly visible benefits and challenges associated with digital technologies.
- Resources: the necessity of sharing information and working together to make the most of limited human, financial and technological resources.
- Prevention: the critical role that preventative measures and prevention-minded individuals play in the fight against fraud.

4.32 The aim of this collaboration between Internal Audit and the Counter Fraud Team is to develop specific strategic objectives to drive the Council's approach to tackling fraud. The draft objectives are shown below:

- Building capability across the Council to tackle fraud;
- Continuing to improve our intelligence sharing and the use of data;
- Increasing our corporate/organisational understanding of the risk and threat of fraud;
- Closer working on shared threats and opportunities; and
- Minimising the loss from fraud in those areas where there is known loss.

Public/stakeholder engagement

5.1 None

Other options

6.1 None

Financial and value for money issues

7.1 None

Legal implications

8.1 None

Other significant implications

9.1 None

This report has been approved by the following people:

Role	Name	Date of sign-off
Legal		
Finance		
Service Director(s)		
Report sponsor	Director of Financial Services	16 July 2020
Other(s)		

Background papers:	None	
List of appendices:	Appendix 1 – Counter Fraud Annual Report 2019/20	