



# COUNTER FRAUD FRAMEWORK REPORT

18 January 2023



## Annex 1

**Assistant Director Corporate Fraud:**  
Jonathan Dodsworth

**Head of Internal Audit:**  
Max Thomas



## INTRODUCTION

- 1 Fraud is a significant risk to the UK public sector. Losses to local government due to fraud results in less funding for public services. The government estimates that the taxpayer loses up to £51.8 billion to fraud and error in public spending every year and 40% of all crime committed in the UK is categorised as fraud<sup>1</sup>.
- 2 To effectively combat fraud the council needs to have a counter fraud framework that helps it prevent, detect and deter fraud. Counter fraud work needs to develop at least as quickly as the techniques used by criminals seeking to defraud the council.



## NATIONAL PICTURE

- 3 The Institute for Fiscal Studies reports that the UK is experiencing a “cost of living crisis”<sup>2</sup> as a result of a number of financial factors. The insurance company Zurich reports a “sharp increase in insurance fraud as cost of living pressures contribute to a rise in bogus claims”<sup>3</sup>. Fraud is expected to become more prevalent during this period and councils may see an increase in false claims for discounts and benefits. The public will also be targeted. There have been reports of scam telephone calls and text messages made to members of the public purporting to offer financial support (eg government support for energy bills) but are in fact attempts to use the current economic situation as a way to defraud people.
- 4 The Public Sector Fraud Authority (PSFA) was launched in August 2022. The organisation seeks to modernise the government’s counter fraud response. The PSFA has a target to deliver benefits of £180 million in its first 12 months. It will agree counter fraud plans with, and provide support to, central government departments and other public bodies to help combat fraud. The PSFA will focus on ministerial bodies but will share best practice and standards with local government<sup>4</sup>. The PSFA is currently seeking input from councils on how they can support local government counter fraud functions.
- 5 Covid-19 payments to businesses and the public concluded this year. Councils across the country have been working with the Department for Business, Energy and Industrial Strategy (BEIS) to complete reconciliation and assurance exercises. BEIS estimates<sup>5</sup> that fraud within the initial Covid-19 schemes (eg the Small Business Grant Fund and Retail Hospitality and Leisure Grant Fund) at the start of the pandemic was 8.4% of payments (£985m) nationally. Later schemes (eg the Additional Restriction Grant and Omicron Hospitality and Leisure Grant) lost 1% (83m) of payments due to fraud. Councils and central government are

---

<sup>1</sup> [Fraud and Error \(Ninth Report of Session 2021/22\)](#), Public Accounts Committee, June 2021, HM Government

<sup>2</sup> [Response to Government Cost of Living Statement](#), Institute for Fiscal Studies, May 2022

<sup>3</sup> [Cost of Living Press Release](#), Zurich Insurance Group, July 2022

<sup>4</sup> [Public Sector Fraud Authority Mandate](#), HM Government, September 2022

<sup>5</sup> [Annual Report and Accounts 2021 to 2022](#), BEIS, October 2022

currently working together to recover money lost due to fraud through Covid-19 grant schemes.

- 6 Cybersecurity continues to be an area of focus for the public and private sectors as organisations rely more on online resources to deliver services and facilitate productivity (eg homeworking). In a recent report RSM UK expressed concern that when an organisation's infrastructure extends into the homes of staff that this presents an easier target for criminals. A survey that formed part of the report found the number of medium sized business owners reporting successful cyber attacks had increased by 35% compared to the previous year<sup>6</sup>.
- 7 The World Economic Forum's 2022 Global Risk Report states that 95% of cybersecurity issues stem from human error<sup>7</sup>. Luton Council was subject to a payment diversion fraud (also known as mandate fraud) perpetrated by organised criminals. A compromised user account was used to request a change of bank account, resulting in the diversion of a £1.1m payment. To date this has not been recovered. This crime highlights the importance of strong controls and regular messages to employees to raise awareness of fraud.



## LOCAL PICTURE

- 8 Over the course of the pandemic the number of fraud referrals from members of staff and the public reduced and investigative resource was diverted to support the council in delivering Covid-19 grants. In 2022/23 the counter fraud team has focussed on re-engaging and delivering training to key council service areas. Levels of referrals are 21%<sup>8</sup> higher in 2022/23 compared to 2020/21 and are only 12% lower than pre-pandemic levels in 2019/20. The largest area of referrals made to the team relate to council tax discounts (eg council tax support and single person discounts). Many of these referrals are not economic to investigate criminally as the loss to the council is very low. The counter fraud team will explore implementing new compliance processes this year to address referrals that don't meet the threshold for investigation. Intervening at an early stage could help prevent larger losses due to fraud and error occurring in the future.
- 9 Raising the awareness of officers to risks of fraud is essential to help to prevent fraud. Veritau continues to undertake fraud awareness training for council officers in services at higher risk of fraud as well as delivering wider fraud awareness information. The team has highlighted the whistleblowing policy, anti-money laundering and anti-bribery policies in campaigns this year. In addition, the dangers of cybercrime were raised as part of international cyber awareness month in October.
- 10 The 2020/21 National Fraud Initiative (NFI) exercise concluded this year. The counter fraud team and council staff reviewed 7,300 data matches which resulted in £91k of savings for the council of which £55k related to

---

<sup>6</sup> [The Real Economy - Cyber Security report](#), RSM UK, April 2022

<sup>7</sup> [Global Risks Report 2022](#), World Economic Forum, January 2022

<sup>8</sup> Comparing number of referrals at 31/10/20 and 31/10/22

Covid-19 grant payments. The 2022/23 NFI exercise is now underway. Data has been securely sent to the Cabinet Office and the results of the matches are expected to be made available in February 2023.



## COUNTER FRAUD FRAMEWORK

- 11 The council has a robust counter fraud framework which includes a counter fraud strategy and associated action plan, a counter fraud policy, a fraud risk assessment, and a number of related policies (eg whistleblowing). A review of the framework is conducted annually.
- 12 The Police, Crime, Sentencing and Courts Act 2022 will affect what sanctions can be offered by councils in the UK. Local Authorities, including City of York Council, have been able to offer simple cautions as an alternative to prosecution for some time. The new legislation replaces simple cautions with diversionary and community cautions. These cautions contain conditions (eg attendance at an alcohol misuse centre for alcohol related crimes) which if not adhered to may result in further prosecutions or fines. It is not currently clear if councils will be able to issue these new cautions; or if they can, how they will be able to enforce conditions attached to the cautions. The sections of the legislation relating to cautions have not yet been enacted. Representations are being made by local government counter fraud practitioners to central government for guidance. If the law is enacted as it currently stands then the council will lose its ability to issue cautions. This will require changes to be made to the Counter Fraud and Corruption Policy.
- 13 The counter fraud team reviews and updates the council's counter fraud and corruption strategy action plan on an annual basis. The plan sets out actions to maintain and develop counter fraud arrangements at the council. This year's update is contained in appendix A. It details progress made against last year's plan and introduces new priorities for the counter fraud team for 2023/24. New objectives this year include:
  - engaging with the newly formed Public Sector Fraud Authority
  - developing new whistleblowing e-learning packages to support the council's whistleblowing policy
  - exploring the implementation of compliance processes to address lower value fraud referrals
  - monitoring updates to the law surrounding cautions and updating the council's Counter Fraud and Corruption Policy as and when required.



## FRAUD RISK ASSESSMENT

- 14 Veritau completes an annual Fraud Risk Assessment, designed to identify areas of fraud that present the greatest risk to the council. The risk assessment is informed by national and regional reports of fraud affecting local authorities, fraud reported to and investigated by the counter fraud team, and changes in process and the operating environment. The results of the assessment are used to:

- develop or strengthen existing fraud prevention and detection measures
  - revise the counter fraud policy framework
  - focus future counter fraud and audit work.
- 15 The format of the risk assessment has been updated this year to show both the inherent and residual risk from specified fraud threats. Inherent risk ratings show the risk to the council if no controls to prevent fraud were in place. The residual risk rating indicates the potential risk level after current controls are taken into account.
- 16 We have intentionally avoided defining 'high', 'medium', and 'low' risk. This is because the purpose of the assessment is to give an illustration of the relative risk of each area and to demonstrate how counter fraud and internal audit resource is prioritised accordingly to help the council combat fraud. However, in arriving at a high, medium or low assessment, we have – as would be expected of any reasonable risk assessment process – considered the potential value of losses due to fraud (impact) and the likelihood of the fraud taking place.
- 17 It is important to stress that this risk assessment has been carried out internally, within Veritau, based on our collective understanding of fraud risk in the sector and of the council's fraud risk controls. It should not be confused with the council's own risk assessment process which is carried out by officers and is set out in the council's Risk Management Policy and Strategy.
- 18 Specific priorities and actions to be taken by the counter fraud team and internal audit are also shown. Over the course of the next year the risk assessment will be further strengthened by seeking additional input from council officers and service managers. The updated risk assessment is contained in appendix B, below.

## APPENDIX A: COUNTER FRAUD STRATEGY ACTION PLAN

Veritau are responsible for maintaining, reviewing, and strengthening counter fraud arrangements at the council. An annual review of priorities for developing counter fraud arrangements is undertaken. Actions to be taken over the next year (and actions completed since the last review) are set out below.

In addition to the specific areas set out in the table below, ongoing activity will continue in other areas that contribute to the council's arrangements for countering fraud, including:

- a rolling programme of fraud awareness training for officers based on priorities identified through the fraud risk assessment and any emerging issues
- regular reporting of counter fraud activity to Audit and Governance Committee
- local datamatching exercises to identify potential fraud in areas such as council tax, business rates, and housing.

### New development activity:

Ref	Action Required	Target Date	Responsibility	Notes
1	Introduce an improved fraud risk assessment showing inherent and residual risks.  Undertake further consultation with service departments to refine assessments in individual areas and increase engagement.	January 2023  December 2023	Veritau	The annual fraud risk assessment (included in this report) has been updated to include inherent and residual risk ratings.

Ref	Action Required	Target Date	Responsibility	Notes
2	Engage with the Public Sector Fraud Authority (PSFA); identify recommended actions and implement as required.	March 2023	Veritau	The newly formed PSFA has reached out to local government counter fraud teams to discuss how it can provide support.
3	Explore implementing compliance processes to address low value referrals to the team.	September 2023	Veritau / relevant CYC departments	A new compliance process will be discussed with service areas, eg revenues and benefits teams.
4	Update the council's counter fraud and corruption policy as required.	January 2024	Veritau	Update the policy to bring in changes to caution regime as new legislation takes effect.
5	Develop new whistleblowing e-learning courses for staff and managers.	April 2024	Veritau	New e-learning training packages will be more focussed on the council's whistleblowing policy (as opposed to the current more generic package). The e-learning will provide specific training for managers to ensure that when whistleblowing concerns are raised they are acted on in an appropriate manner.

## Completed activities:

Ref	Action Required	Responsibility	Update
1	Introduce a new Anti-Bribery Policy; undertake work to raise awareness of the policy.	Veritau	The council adopted a new anti-bribery policy in 2022. Awareness of the policy is now raised with staff annually as part of World Anti-Corruption Day.
2	Continue to work with council officers to ensure the council meets Government guidance on new Covid-19 grant payments as well as any checks relating to previously issued grants.	Veritau	Covid-19 related payments have now ceased. Veritau has helped the council meet post-assurance requirements from Government to date.
3	Trial the use of financial checks to enhance the robustness of social care financial assessments.	Veritau / Income Services	Financial assessment officers now regularly use financial checks as part of the social care assessment process.
4	Implementation of a new counter fraud system.	Veritau	A new case management system was adopted in April 2022. All referrals made to the team, case notes, and results are now recorded on the system.



## Appendix B: Fraud Risk Assessment (January 2023)

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
Adult Social Care Fraud	<p>Losses can occur through deprivation or non-declaration of capital. For example, the transfer or disguise of property and assets in order to avoid paying for residential or domestic care provision. Fraud can also occur through the misuse of the Direct Payment scheme. For example, where money allocated to meet a customer's assessed needs are not used to procure appropriate services.</p> <p>In cases where fraud or error is identified, the average loss is £18k (based on the outcomes of investigations by the counter fraud team over the past six years). Losses in individual cases can be much higher, especially if they are not detected at an early stage.</p>	<b>High</b>	<p>Applications for care funding are carefully assessed to ensure that recipients meet the eligibility criteria and that any financial contribution for care by the customer is correctly calculated.</p> <p>Use of Direct Payments is monitored by council officers who check for possible false claims and overstated needs.</p> <p>The financial assessment team have access to credit checking to help identify undeclared assets.</p> <p>The residual risk of Adult Social Care fraud is still considered to be high. This is due to the scale of losses and the speed at which they can be accrued. It is also a reflection of the difficulty all councils have in detecting assets when people are determined to keep them hidden.</p>	<b>High</b>	<p>Veritau has established relationships with senior management and officers responsible for the provision of adult social care; concerns of fraud are regularly reported to the counter fraud team (CFT) for investigation. Internal audit (IA) periodically conducts audits in higher risk areas, eg Direct Payments.</p> <p>CFT continue to deliver a rolling programme of fraud awareness to staff with responsibilities for assessment and payments.</p> <p>Investigation of fraud in this area provides a deterrent to those considering committing it and can assist the council to recover losses through the court system.</p>

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
Creditor Fraud	<p>Fraud against creditor payment systems has increased in terms of volume and sophistication over the past three years. The mandatory publication of payment data makes councils particularly vulnerable to attack. Attacks are often the work of organised criminal groups who operate from abroad. Individual losses due to fraud can be extremely large (in excess of £1 million). The likelihood of recovery is low once a fraud has been successfully committed.</p> <p>The most common issue is mandate fraud (payment diversion fraud) where fraudsters impersonate legitimate suppliers and attempt to divert payments by requesting changes in bank details. Other types of fraud include whaling, where senior members of the council are targeted and impersonated in order to obtain fraudulent payments.</p>	<b>High</b>	<p>The council has strong controls in place to identify fraudulent attempts to divert payments from genuine suppliers and to validate any requests to change supplier details.</p> <p>Segregation of duties exist between the ordering, invoicing and payments processes.</p> <p>The residual risk of creditor fraud is still considered to be high due to potentially high levels of loss, the frequency of attacks on public organisations, and the council's reliance on staff working for both the council and its suppliers to follow processes. Human error is a factor in many successful mandate fraud attacks.</p>	<b>High</b>	<p>Veritau regularly provide support and advice to the Creditors Team relating to processes.</p> <p>IA regularly perform audits of the ordering and creditor payment processes, eg segregation of duties and controls to prevent mandate fraud. IA also undertake duplicate payment checks on a quarterly basis.</p> <p>CFT undertake fraud awareness training for payments staff. Increased awareness provides a greater chance to stop fraudulent attempts before losses occur.</p> <p>All instances of whaling fraud reported to CFT are reported to the relevant agencies, such as the National Cyber Security Centre, as well as directly to the email provider from which false emails originated.</p> <p>The counter fraud team share intelligence alerts relating to attempted fraud occurring</p>

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	<p>In recent years there have been increased instances nationally and regionally of hackers gaining direct access to email accounts of suppliers and using these to attempt to commit mandate fraud. These attempts can be much more difficult to detect and prevent.</p> <p>Increased remote working has resulted in greater opportunities for fraudsters to impersonate budget holders or suppliers in electronic communications to divert funds.</p>				<p>nationally with relevant council officers to help prevent losses.</p> <p>As part of any investigation of attempted fraud in this area, the CFT will advise on improvements that will strengthen controls.</p>
Cybercrime	<p>Cybercrime is an evolving area where criminals are continually refining their techniques in order to overcome controls, to obtain unauthorised access and information, and to frustrate systems.</p> <p>Types of cybercrime experienced by local authorities include ransomware, phishing, whaling, hacking, and denial of service attacks. Attacks can lead</p>	<b>High</b>	<p>The council has a highly skilled ICT department which helps mitigate the threat of cybercrime. The ICT department reviews threat levels and controls (eg password requirements for staff) on a routine basis.</p> <p>The ICT department use filters to block communications from known fraudulent servers and they encourage staff to raise concerns about any</p>	<b>High</b>	<p>IA undertakes a risk assessment of key IT risks facing the council and routinely includes IT audits in the annual work programme.</p> <p>Raising awareness with staff can be crucial in helping to prevent successful cyberattacks. The CFT works with ICT to support activities on raising awareness. A campaign to mark cybersecurity awareness month is undertaken annually.</p>

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	<p>to loss of funds or systems access/data which could impact service delivery to residents.</p> <p>There have been a number of high profile cyber-attacks on public and private sector organisations in recent years. Attacks stemming from the hacking of software or IT service providers have become more prevalent. These are known as supply chain attacks and are used by hackers to target the end users of the software created by the organisations targeted.</p>		<p>communications they do receive that may be part of an attempt to circumvent cybersecurity controls.</p> <p>Despite strong controls being in place, cybercrime remains a high residual risk for the council. Human error was found to be a factor in 82% of cyber breaches according to a recent study<sup>9</sup>. Council systems could be exposed by as yet unknown weaknesses in software. Suppliers of software or IT services could also be compromised which may allow criminals access to council systems believed to be secure.</p>		
Council Tax & Business Rates Frauds (discounts and exemptions)	Council Tax discount fraud is a common occurrence. CIFAS conducted a survey in 2022 in which 10% of UK adults said they knew someone who had recently committed single person discount fraud. In addition, 8% of people thought	<b>High</b>	The council employs a number of methods to help ensure only valid applications are accepted. This includes requiring relevant information be provided on application forms, and visits to properties are undertaken where needed, to verify information.	<b>Medium</b>	<p>CFT deliver periodic fraud awareness training to staff in revenues and customer services teams about frauds affecting Council Tax and Business Rates.</p> <p>IA routinely reviews the administration of Council Tax and</p>

<sup>9</sup> [2022 Data Breach Investigations Report](#), Verizon

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	<p>falsely claiming a single person discount was a reasonable thing to do. Individual cases of fraud in this area are of relatively low value but cumulatively can represent a large loss to the council.</p> <p>Business Rates fraud can also involve falsely claiming discounts that a business is not entitled to, eg small business rate relief. Business Rate fraud is less prevalent than Council Tax fraud but can lead to higher losses in individual cases.</p>		<p>Messages appear on annual bills issued by the council reminding residents and businesses to update their circumstances when necessary.</p> <p>The council routinely takes part in the National Fraud Initiative, and periodically undertakes reviews of single person discounts with companies who undertake data matching exercises.</p>		<p>Business Rates as one of the council's key financial systems.</p> <p>CFT provide a deterrent to fraud in this area through the investigation of potential fraud which can, in serious cases, lead to prosecution.</p>
Council Tax Support Fraud	<p>Council Tax Support (CTS) is a council funded reduction in liability for Council Tax. It is resourced through council funds. Fraud and error in this area is of relatively low value on a case-by-case basis but cumulatively fraud in this area could amount to a substantial loss.</p> <p>CTS fraud can involve applicants failing to declare their total</p>	<b>High</b>	<p>The council undertakes eligibility checks on those who apply for support.</p> <p>The DWP use data from HMRC on claimants' incomes which is then passed through to council systems. This mitigates the risk of claimant's not updating the council with income details.</p> <p>There are established lines of communication with the DWP</p>	<b>Medium</b>	<p>CFT routinely raise awareness of fraud with teams involved in processing claims for CTS.</p> <p>CFT provide a deterrent to fraud in this area through the investigation of potential fraud which can, in serious cases, lead to prosecution.</p> <p>Concerns of fraud are routinely reported to CFT by the public and members of staff. If fraud cannot</p>

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	<p>assets or income. Those receiving support are also required to notify relevant authorities when they have a change in circumstances that may affect their entitlement to support.</p> <p>Most CTS claims are linked to state benefits (eg Universal Credit) which are administered by the Department for Work and Pensions (DWP). The council has limited influence on DWP decision making which makes it harder to address fraud in this area.</p>		<p>where claims for support are linked to externally funded benefits.</p> <p>The council reports suspected fraud to the DWP but this does not always give the council control over resolving false claims for CTS.</p>		<p>be addressed by the council directly it is reported to the DWP.</p> <p>CFT engage with the DWP at a senior level to foster joint working wherever possible.</p>
Housing related Fraud	<p>Council properties represent a significant asset to the council. Housing fraud can deprive the council of these assets through false applications for Right to Buy. Tenants who sublet or falsely obtain council properties remove a property from a person or family in true need of housing and can negatively affect the council financially if people are in temporary</p>	<b>High</b>	<p>The council has strong controls in place to prevent false applications for housing.</p> <p>The housing department engages with tenants regularly to ensure properties are not being misused. They also conduct identification and money laundering checks on applications for Right to Buy.</p>	<b>Medium</b>	<p>CFT provide a deterrent to fraud in this area through the investigation of any suspected subletting of council properties using powers under the Prevention of Social Housing Fraud Act. Offenders face criminal prosecution and repossession of their council properties.</p> <p>CFT undertake verification exercises on Right to Buy</p>

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	accommodation and are waiting for a suitable property to become available.				applications that are likely to proceed.
Procurement Fraud	<p>Procurement fraud, by its nature, is difficult to detect but can result in large scale loss of public funds over long periods of time. The Competition and Markets Authority (CMA) estimates that having a cartel within a supply chain can raise prices by 30% or more.</p> <p>In 2020 CIPFA reported losses of £1.5m for local authorities, due to procurement fraud. It found that 8% of fraud detected in this area involved 'insider fraud'.</p>	<b>High</b>	<p>The council has established Contract Procedure Rules. The rules are reviewed regularly and ensure the requirement for a competitive process (where required) through an e-tender system. A team of procurement professionals provide guidance and advice to ensure procurement processes are carried out correctly. The team also has a dedicated procurement compliance officer who proactively looks for potential issues in this area.</p> <p>A tendering and evaluation framework is in operation to help prevent fraud. It also sets out the requirements for declarations of interest to be made.</p>	<b>Medium</b>	<p>Continued vigilance by relevant staff is key to identifying and tackling procurement fraud. CFT provide training to raise awareness of fraud risks and investigate any suspicions of fraud referred.</p> <p>CFT and IA monitor guidance on fraud detection issued by the Competition and Markets Authority and other relevant bodies.</p> <p>IA regularly undertake procurement themed audits which help to ensure processes are effective and being followed correctly.</p>

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
Internal Fraud	<p>Fraud committed by employees is a risk to all organisations. Internal fraud within the council occurs infrequently and usually results in low levels of loss. However, if fraud or corruption occurred at a senior level there is the potential for a greater level of financial loss and reputational damage to the council.</p> <p>There are a range of potential employee frauds including theft, corruption, falsifying timesheets and expense claims, abusing flexitime or annual leave systems, undertaking alternative work while sick, or working for a third party on council time. Some staff have access to equipment and material that may be misused for private purposes.</p> <p>Payroll related fraud can involve the setting up of 'ghost' employees in order to divert salary payments to others.</p>	<b>Medium</b>	<p>In the past two years the council has introduced new whistleblowing and anti-bribery policies. Campaigns are held annually to promote the policies and to remind staff how to report any concerns.</p> <p>The council has checks and balances in place to prevent individual members of staff being able to circumvent financial controls, eg segregation of duties.</p> <p>Controls are also in place surrounding flexitime, annual leave and sickness absence.</p>	<b>Medium</b>	<p>Veritau regularly liaises with senior management on internal fraud issues. Instance of internal fraud are analysed by both IA and CFT to determine if control weaknesses exist and can be addressed.</p> <p>CFT provide training to HR officers on internal fraud issues. It also provides training to all staff on whistleblowing and how to report concerns.</p> <p>CFT investigates any suspicions of fraud or corruption. Serious cases of fraud will be reported to the police. CFT supports any disciplinary action taken by the council relating to internal fraud issues.</p> <p>IA undertake work to ensure that appropriate checks and balances are in place to help prevent and detect internal fraud and corruption.</p>



Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
Recruitment Fraud	Recruitment fraud can affect all organisations. Applicants can provide false or misleading information in order to gain employment such as bogus employment history and qualifications or providing false identification documents to demonstrate the right to work in the UK. There is particular danger for the council if recruitment fraud leads to the wrong people occupying positions of trust and responsibility.	<b>Medium</b>	<p>The council has controls in place to mitigate the risk of fraud in this area. DBS checks are undertaken where necessary.</p> <p>Additional checks are made on applications for roles involving children and vulnerable adults.</p> <p>References are taken from previous employers and there are processes to ensure qualifications provided are genuine.</p>	<b>Medium</b>	Where there is a suspicion that someone has provided false information to gain employment, CFT will be consulted on possible criminal action in tandem with any disciplinary action that may be taken.
Treasury Management	Treasury Management involves the management and safeguarding of the council's cash flow, its banking, and money market and capital market transactions. The impact of fraud in this area could be significant.	<b>High</b>	<p>Treasury Management systems are subject to a range of internal controls, legislation, and codes of practice which protect council funds.</p> <p>The council can only invest with approved institutions on the Approved Lending List which reviewed annually.</p> <p>The council employees third party consultancy firms to provide</p>	<b>Low</b>	IA conduct periodic work in this area to ensure controls are strong and fit for purpose.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
			<p>specialist treasury and market advice.</p> <p>Only pre-approved members of staff can undertake transactions in this area and they work within pre-set limits.</p>		
Fraudulent Insurance Claims	The council may receive exaggerated or fabricated insurance claims. If false claims continued unchecked this would negatively effect the council in terms of the annual premiums it pays.	<b>Medium</b>	While insurance fraud is common, the burden of risk is currently shouldered by the council's insurers who have established fraud investigation systems.	<b>Low</b>	N/A
Theft of Assets	The theft of assets can cause financial loss and reputational damage. It can also negatively impact on employee morale and disrupt the delivery of services. The council owns a large amount of portable, desirable physical assets such as IT equipment, vehicles and tools that are at higher risk of theft.	<b>Medium</b>	<p>Specific registers of physical assets (eg capital items, property, and ICT equipment) are maintained.</p> <p>The council operates CCTV systems covering key premises and locations where high value items are stored.</p> <p>Entrance to council buildings are regulated and controlled via different access methods.</p>	<b>Low</b>	Thefts are reported to Veritau and the police. Instances of theft are investigated by CFT where appropriate.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
			The council's whistleblowing arrangements provide an outlet for reporting concerns of theft.		
Blue Badge & Parking Fraud	<p>Blue Badge fraud carries low financial risk to the authority but can affect the quality of life for disabled residents and visitors. There is a risk of reputational damage to the council if abuse of this scheme is not addressed.</p> <p>Other low level parking fraud is relatively common. For example, misuse of residential permits to avoid commercial parking charges.</p>	<b>Low</b>	<p>Measures are in place to control the issue of blue badges, to ensure that only eligible applicants receive badges. Checks are made to ensure that commercial businesses don't inappropriately access residential parking permits.</p> <p>The council participates in the National Fraud Initiative which flags badges issued to deceased users, and badge holders who have obtained a blue badge from more than one authority, enabling their recovery to prevent misuse.</p>	<b>Low</b>	<p>Periodic proactive days of action between CFT and the council's enforcement team are used to raise awareness and act as a deterrent to blue badge misuse.</p> <p>CFT and Parking Enforcement work closely together to identify, deter and investigate parking fraud. Warnings are regularly issued to people who misuse parking permits and blue badges. Serious cases are considered for prosecution.</p>