COUNTER FRAUD FRAMEWORK REPORT

5 October 2023

Appendix 1

Middlesbrough moving forward

Assistant Director - Corporate Fraud: Jonathan Dodsworth

Head of Internal Audit: Max Thomas

Veritau

INTRODUCTION

1 Fraud has become the most common offence in the UK, accounting for 41% of all crime[1]. Fraud threats continue to evolve with new tools and techniques being used, and increasingly originates nationally and internationally as opposed to locally.

2 Fraud is a significant risk to the public sector. The government estimated that between £33.2 and £58.8 billion of public spending was lost to fraud in 2020/21[2]. At a local level, fraud can impact a council's ability to support public services and cause reputational damage.

3 To effectively combat fraud councils should have a counter fraud framework that helps to prevent, detect and deter fraud. Counter fraud work needs to develop at least as quickly as the techniques used by fraudsters.

NATIONAL PICTURE

4 The government has indicated that they will create a new corporate criminal offence of Failure to Prevent Fraud as part of a range of reforms within the Economic Crime and Corporate Transparency Bill. Organisations will be held liable if fraud offences are "committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place[3]." The offence will only affect larger organisations that meet two of the following criteria: more than 250 employees, more than £36m turnover, or more than £18m in assets. If found guilty organisations could receive an unlimited fine. There is still some question as to whether local authorities could be found guilty of the proposed offence, but council owned businesses, council contractors, and charities that work with councils could be affected.

5 The Public Sector Fraud Authority (PSFA) was launched in August 2022. The organisation seeks to modernise the government's counter fraud response. They have taken on responsibility for the National Fraud Initiative (NFI) from the Cabinet Office. The NFI is an exercise that matches data within and between public and private sector bodies to prevent and detect fraud. All local authorities are required to take part. Sitting within the National Counter Fraud Data Analytics Service, the NFI is likely to benefit from the use of new technology, including artificial intelligence.

6 Covid-19 payments to businesses and the public concluded last year. Councils across the country have been working with the former Department for Business, Energy and Industrial Strategy (BEIS) to complete reconciliation and assurance exercises. BEIS estimates that 8.4% of payments (£985m nationally) was lost to fraud from the initial

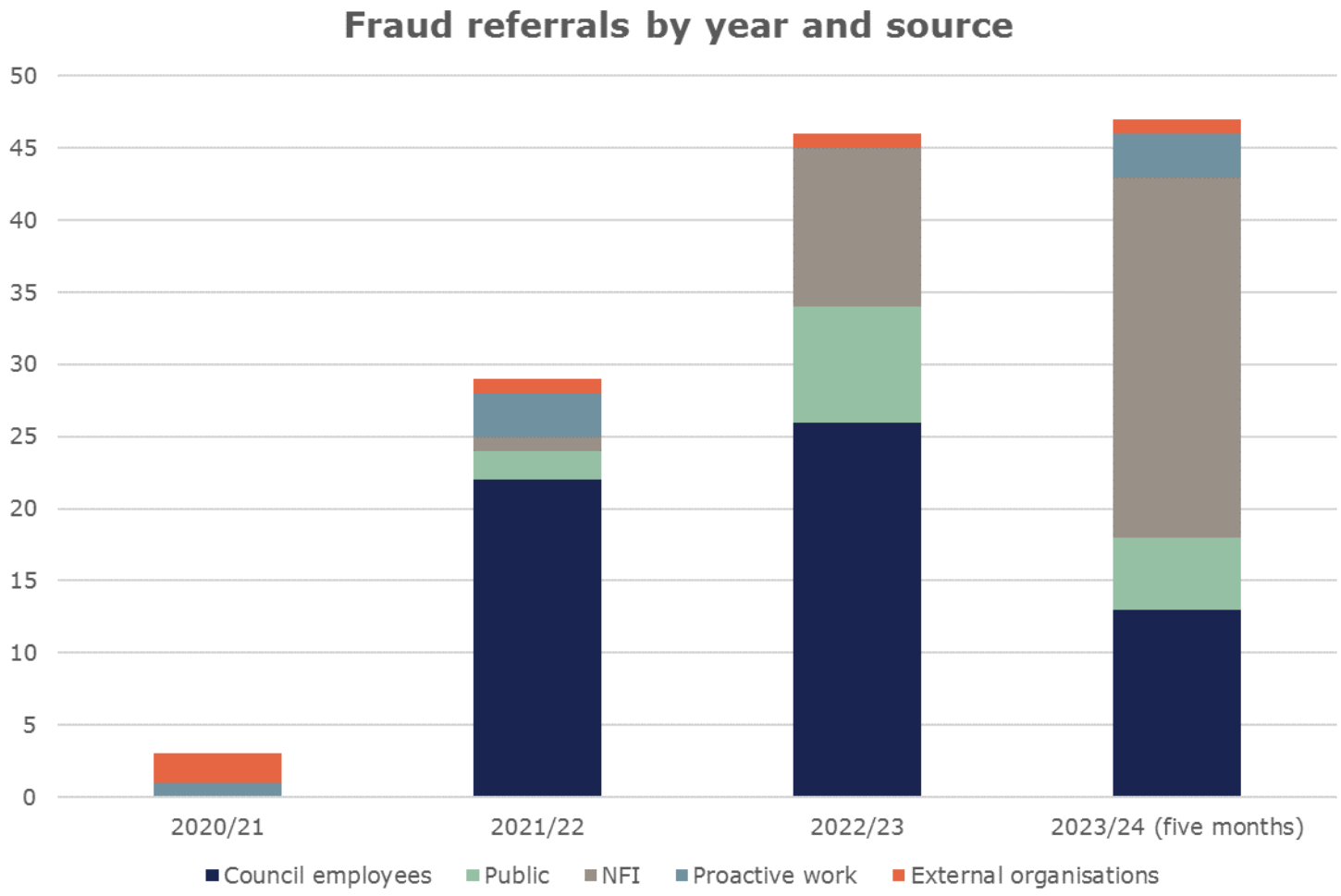
[1] Progress Combatting Fraud (43rd Report of Session 2022-23), Public Accounts Committee, House of Commons
[2] Tackling fraud and corruption against Government, National Audit Office
[3] Factsheet: Failure to Prevent Fraud Offence, HM Government

Covid-19 schemes at the start of the pandemic (eg the Small Business Grant Fund and Retail Hospitality and Leisure Grant Fund)[4]. Later schemes lost 1% (£83m) of payments due to fraud (eg the Additional Restriction Grant and Omicron Hospitality and Leisure Grant). Councils and central government are currently working together to recover money lost due to fraud through Covid-19 grant schemes.

7 Following the Covid-19 pandemic, there has been an increased emphasis on managing fraud risks in government funded grant schemes. Local authorities must consider the local arrangements in place to mitigate and address fraud when disbursing central government funds through the creation of fraud management plans. Post assurance reviews and audits continue to provide opportunities to identify fraud and error.

LOCAL PICTURE

8 Veritau began providing counter fraud services to the Council in January 2020. Raising awareness of fraud within the authority and with the public has been a key priority. This has resulted in year on year increases in the numbers of cases of suspected fraud being referred to the team. The chart below shows the number of referrals received by the team since 2020, and the source of the referrals.



[4] Annual Report and Accounts 2021 to 2022, BEIS

9 Between 1 April and 31 August 2023 (five months), the team received almost as many referrals as the total received in the previous year. The number of referrals from Council officers and the public have also grown each year. The team is increasingly taking more responsibility for the investigation of data matches highlighted by the National Fraud Initiative.

COUNTER FRAUD FRAMEWORK

10 The Council has a robust counter fraud framework which includes a counter fraud strategy and associated action plan, an anti-fraud and corruption policy, a fraud risk assessment, and a number of related policies (eg whistleblowing). A review of the framework is conducted annually.

11 The Council's current counter fraud and corruption strategy was adopted in 2020. The strategy sets out the Council's aims for counter fraud work up to 2024. The strategy also includes actions needed to maintain and develop counter fraud arrangements at the Council. The associated strategy action plan is reviewed and updated annually. This year's update is contained in annex A. It details progress made against last year's plan and introduces new priorities for the counter fraud team in 2023/24 taking into account local and national developments.

New objectives this year include:

- Presenting a new counter fraud strategy to the Corporate Affairs and Audit Committee in 2024
- supporting the Council to meet central government requirements around grant provision
- delivery of new whistleblowing e-learning packages to support employees and managers.

12 No policy updates were identified as part of the current review.

FRAUD RISK ASSESSMENT

13 Veritau completes an annual Fraud Risk Assessment, designed to identify the areas of fraud that present the greatest risk to the Council. National and regional reports of fraud affecting local authorities, as well as fraud reported to and investigated by the counter fraud team, are used to develop the risk assessment. 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 audit and counter fraud work.

14 The format of the risk assessment has been updated this year to show both the inherent and residual risks from 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.

15 By their nature, fraud risks are hard to quantify. For example, there are no established methodologies for determining estimated losses due to fraud in most areas. The terms high, medium, and low are therefore used in the risk assessment to provide a general indication of both the likelihood and impact of fraud in each area. However, we have intentionally avoided defining what high, medium, and low risk mean given the inherent uncertainty.

16 The risk assessment has been carried out by Veritau, based on our understanding of fraud risks in the sector and our knowledge of controls in place within the Council that prevent, identify and deter fraud. It is used to inform priorities for counter fraud and internal audit work by Veritau. However, it is separate from the wider Council risk management framework. We will be seeking to further develop the risk assessment in the coming year by working with officers responsible for management of risks in key areas.

17 Changes to the risk assessment this year include:

- the removal of Covid-19 related fraud, following completion of the schemes and associated requirements for post payment assurance checks
- the addition of grant schemes. Government departments are increasingly requesting that local authorities develop a fraud management plan for grant schemes they are asked to administer. The plans set out measures in place to prevent, detect, and investigate fraud. Failure to document and implement these measures could result in Council requests for grant funding being denied, loss of public funds if fraudulent applications succeed, and the potential for the Council to become liable for irrecoverable payments made incorrectly.

18 The updated risk assessment is contained in annex B, below.

ANNEX A: COUNTER FRAUD STRATEGY ACTION PLAN

Veritau have responsibility for maintaining, reviewing, and strengthening counter fraud arrangements at the Council. This includes an annual review of the Council's counter fraud strategy action plan.

Veritau also provide a number of other ongoing activities including:

- a rolling programme of fraud awareness training for officers based on priorities identified through the fraud risk assessment and any emerging issues
- annual campaigns to promote key issues, including cyber security, fraud awareness, whistleblowing, anti-bribery, and money laundering
- regular reporting of counter fraud activity to the Corporate Affairs & Audit Committee.

New one off and developmental activity:

Ref	Action Required	Target Date	Responsibility	Notes
1	Present a new counter fraud strategy to the Corporate Affairs and Audit Committee.	March 2024	Veritau	The Council's counter fraud strategy will require updating in 2024.
2	Review guidance issued by the Public Sector Fraud Authority (PSFA); identify recommended actions and implement as required.	March 2024	Veritau	The PSFA have and continue to publish guidance documents that will inform the Council's new counter fraud strategy.
3	Support Council delivery of grant schemes.	September 2024	Veritau	Veritau will seek to identify relevant Council officers and offer guidance on counter fraud measures in relation to grant schemes.
4	Develop new whistleblowing e-learning courses for employees and managers.	June 2024	Veritau	New e-learning training packages will be more focussed on the Council's whistleblowing policy. They will

Ref	Action Required	Target Date	Responsibility	Notes
				provide specific training for managers to ensure they know how to respond when whistleblowing concerns are raised.
5	Monitor progress of the Economic Crime and Corporate Transparency Bill	December 2024	Veritau	Updates to the counter fraud policy framework may be required to accommodate any new Council responsibilities under the legislation.

Completed activities:

Ref	Action Required	Responsibility	Update
1	Increase responsibilities around the investigation of National Fraud Initiative data matching.	Veritau	The counter fraud team has begun investigating increasing numbers of data matches raised through the National Fraud Initiative.
2	Update the Council's Anti-Fraud, Bribery and Corruption Policy.	Veritau	An updated version of the policy was approved by the committee in September 2022.
3	Promote counter fraud reporting lines to members of the public and staff.	Veritau / Communications Team	The team publicised reporting lines throughout 2022/23 and have experienced an increased number of fraud referrals from council officers and members of the public.
4	Promote counter fraud work to more departments at the Council.	Veritau	The team has held discussions with Children's services and are arranging fraud awareness for officers.

ANNEX B: Fraud Risk Assessment (October 2023)

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
Adult and Children's Social Care Fraud	For adult social care, losses can occur through deprivation or non-declaration of capital which can involve the transfer or disguise of property in order to avoid paying for residential or domestic care provision. Residential homes could also continue to claim for customers who are no longer in residence (eg after they pass away). In both adult and children's social care, fraud can occur through the misuse of the Direct Payment scheme. For example, where monies allocated to meet a customer's assessed needs are not used to procure support services. In cases where fraud or error is identified, the average loss is £18k (based on the outcomes of investigations by the counter fraud team across multiple authorities). Losses in individual cases can be much	**High**	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. A range of monitoring and verification controls are operated by the Council. This includes requiring customers in receipt of Direct Payments to have a separate bank account for managing these funds and complying with monitoring procedures to verify spending. In instances of misused Direct Payments, customers are moved to a commissioned service. The residual risk of Adult and Children's 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	**High**	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) will periodically conduct audits in higher risk areas, eg Direct Payments. CFT will deliver a rolling programme of fraud awareness to employees with responsibilities for assessment and payments. 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.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	higher, especially if they are not detected at an early stage.		councils have in detecting assets when people are determined to keep them hidden.		
Creditor Fraud	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. 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	**High**	The Council has put strong controls in place to identify fraudulent attempts to divert payments from genuine suppliers and to validate any requests to change supplier details. Segregation of duties exist between the ordering, invoicing and payments processes. The residual risk of creditor fraud is still considered to be high due to potentially high levels of loss and the frequency of attacks on public organisations. The Council's reliance on its own employees, and those of its suppliers, to follow processes, and the inevitable element of human error, are	**High**	Veritau will regularly provide support and advice to finance officers responsible for the payment of suppliers. The IA work programme includes audits of key financial systems and processes. This includes ordering and creditor payment processes, eg segregation of duties and controls to prevent mandate fraud. IA also undertake duplicate payment checks on a regular basis. The CFT has delivered fraud awareness training to relevant officers in the past. Increased awareness provides a greater chance to stop fraudulent attempts before losses occur. All instances of whaling fraud reported to CFT will be reported to the relevant agencies, such as the National Cyber Security

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	include whaling, where senior members of the Council are targeted and impersonated in order to obtain fraudulent payments. 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.		factors in many successful mandate fraud attacks.		Centre, as well as directly to the email provider from which false emails originated. The CFT shares intelligence alerts relating to attempted fraud occurring nationally with relevant council officers to help prevent losses. As part of any investigation of attempted fraud in this area, the CFT will advise on improvements that will strengthen controls.
Cybercrime	Cybercrime is an evolving area where criminals are continually refining their techniques in order to overcome controls, obtain unauthorised access and information, and frustrate systems. As cybercrime can be perpetrated remotely, attacks can come from within the UK or overseas. Some cybercrime is motivated by profit, however some is designed purely to disrupt services.	**High**	The Council employs highly skilled ICT employees whose expertise is used to help mitigate the threat of cybercrime. The ICT department has processes to review threat levels and controls (eg password requirements for employees) on a routine basis. The ICT department uses filters to block communications from known fraudulent servers and will encourage employees to raise concerns about any	**High**	IA routinely include ICT audits in the annual work programme. Cybersecurity is an ongoing priority for IA work. Raising awareness with employees 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. ICT can access free resources from the National Cyber Security

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	Types of cybercrime experienced by local authorities include ransomware, phishing, whaling, hacking, and denial of service attacks. Attacks can lead to loss of funds or systems access/data which could impact service delivery to residents. 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 ICT 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.		communications they do receive that may be part of an attempt to circumvent cybersecurity controls. Despite strong controls being in place, cybercrime remains a high residual risk for the Council. The potential for cybercrime is heightened by the availability of online tools. The National Crime Agency report that cybercrime can now be committed by less technically proficient criminals. Human error was found to be a factor in 82% of cyber breaches according to a recent study[5]. 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. The residual risk of cybercrime remains high due to the		Centre to help develop and maintain their cyber defence strategy.

[5] 2022 Data Breach Investigations Report, Verizon

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
			constantly evolving methods employed by fraudsters which requires regular review of controls.		
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 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. 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.	**High**	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. The Council will routinely take part in the National Fraud Initiative (NFI). The exercise allows councils to cross checki for potential instances of fraud in multiple locations (eg multiple claims for single person discount by one individual).	**Medium**	CFT delivers fraud awareness training to employees in revenues and customer services teams about frauds affecting Council Tax and Business Rates. IA routinely review the administration of Council Tax and Business Rates as one of the Council's key financial systems. CFT provide a deterrent to fraud in this area through the investigation of potential offences which can, in serious cases, lead to prosecution. CFT will also seek opportunities to raise awareness with the public about mechanisms for reporting fraud.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
Council Tax Reduction Fraud	Council Tax Reduction (CTR) 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. CTR fraud can involve applicants failing to declare their total 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. Most CTR 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, meaning it is harder to address fraud in this area.	**High**	The Council undertakes eligibility checks on those who apply for support. Officers manage the assessment of new and ongoing claims for CTR to identify potential issues. The Council will routinely take part in the National Fraud Initiative (NFI) which highlights potentially fraudulent claims. The DWP use data from HMRC on claimants' incomes which is then passed through to council systems. This mitigates the risk of claimants not updating the Council with income details. There are established lines of communication with the DWP where claims for support are linked to externally funded benefits. The Council reports suspected fraud to the DWP, but this does not always give the	**Medium**	The CFT raise awareness of fraud with teams involved in processing claims for CTR. The CFT provide a deterrent to fraud in this area through the investigation of potential fraud which can, in serious cases, lead to prosecution. Concerns of fraud can be reported to CFT by employees. CFT will also seek opportunities to raise awareness with the public about mechanisms for reporting fraud. If fraud cannot be addressed by the Council directly it will be reported to the DWP. CFT engage with the DWP at a senior level to foster joint working wherever possible.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
			Council control over resolving false claims for CTR.		
Procurement Fraud	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. 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'.	**High**	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 Middlesbrough Manager Framework includes contract management expectations for managers. The Contract Procedure Rules also set out the requirements for declarations of interest to be made. Contract monitoring helps to detect and deter potential fraud.	**Medium**	Continued vigilance by relevant employees is key to identifying and tackling procurement fraud. CFT and IA monitor and share guidance on fraud detection issued by the Competition and Markets Authority and other relevant bodies. IA regularly undertake procurement related work to help ensure processes are effective and being followed correctly.
Theft of Assets	The theft of assets can cause financial loss and reputational damage. It can also negatively	**High**	Specific registers of physical assets (eg capital items,	**Medium**	Thefts are reported to the police and Veritau. Instances of theft

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	impact on employee morale and disrupt the delivery of services. The Council own a large amount of portable, desirable physical assets such as ICT equipment, vehicles and tools that are at higher risk of theft.		property, and ICT equipment) are maintained. The Council operates CCTV systems covering key premises and locations where high value items are stored. Entrance to council buildings is regulated and controlled via different access methods. The Council's whistleblowing arrangements provide an outlet for reporting concerns of theft.		are investigated by CFT where appropriate.
Internal Fraud	Fraud committed by employees is a risk to all organisations. Internal fraud within councils occurs infrequently and usually results in low levels of loss. However, if fraud or corruption occurs at a senior level there is the potential for a greater level of financial loss and reputational damage to the Council. There are a range of potential employee frauds including	**Medium**	The Council has up to date whistleblowing and anti-bribery policies. Campaigns are held annually to promote the policies and to remind employees how to report any concerns. The Council has checks and balances to prevent individual employees being able to circumvent financial controls, eg segregation of duties.	**Medium**	Veritau liaises with senior management on internal fraud issues. Where internal fraud arises, IA and CFT will review the circumstances to determine if there are underlying control weaknesses that can be addressed. CFT provide training to HR officers on internal fraud and whistleblowing issues. CFT investigate any suspicions of fraud or corruption. Serious

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	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 employees have access to equipment and material that may be misused for private purposes. Payroll related fraud can involve the setting up of 'ghost' employees in order to obtain salary payments.		Controls are in place surrounding flexitime, annual leave and sickness absence. The Council regularly participates in the National Fraud Initiative. Data matches include checks on payroll records for potential issues.		cases of fraud will be reported to the police. In some instances, it may be necessary to report individuals to their professional bodies. CFT support any disciplinary action taken by the Council relating to internal fraud issues.
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 danger for the Council if recruitment fraud leads to the wrong people occupying	**Medium**	The Council has controls in place to mitigate the risk of fraud in this area. DBS checks are undertaken where necessary. Additional checks are made on applications for roles involving children and vulnerable adults. References are taken from previous employers and there are processes to ensure	**Medium**	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. Applicants making false claims about their right to work in the UK or holding professional accreditations will be reported to the relevant agency or

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	positions of trust and responsibility, or not having the appropriate professional accreditation for their post.		qualifications provided are genuine.		professional body, where appropriate.
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.	**Medium**	Treasury Management systems are subject to a range of internal controls, legislation, and codes of practice which protect council funds. Only pre-approved employees can undertake transactions in this area and they work within pre-set limits.	**Low**	IA conduct periodic work in this area to ensure controls are strong and fit for purpose.
Fraudulent Insurance Claims	The Council may receive exaggerated or fabricated insurance claims. If false claims progress unchecked this would negatively affect the Council in terms of the annual premiums it pays.	**Medium**	While insurance fraud is common, the burden of risk is largely shouldered by the Council's insurers who have established fraud investigation systems.	**Low**	CFT are exploring any support that can be provided to the insurance team to complement established arrangements.
Grant schemes	The Council takes on the responsibility for disbursing government funded grant schemes to local residents, businesses, and other organisations.	**Medium**	The Council will complete any required fraud management plan which will consider fraud risks, and mechanisms for preventing and detecting fraud.	**Low**	CFT and IA will support the development of fraud management plans, and associated controls, where required.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	Fraud in this area can include applicants supplying incorrect information to obtain grant payments or grant funded works (for example where grant funds are paid to a third party supplier). Suppliers undertaking work may overcharge or not complete work to agreed standards. The Council can become liable for recovery of any incorrectly paid government funding. This can create a loss to the Council and may affect access to future grant schemes.		When awarding payments or agreeing works, the Council (or their contractor) will complete checks to confirm applicants' eligibility.		CFT can undertake investigation in cases of suspected fraud.
Blue Badge & Parking Fraud	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. Other low level parking fraud is relatively common, for example, misuse of residential	**Low**	Measures are in place to control the issuing of blue badges, to ensure that only eligible applicants receive badges. 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	**Low**	CFT undertake periodic proactive days of action with the Council's enforcement team. This helps raise awareness and act as a deterrent to blue badge misuse. Warnings will be issued to people who misuse parking permits and blue badges. Serious cases will be considered for prosecution.

Risk Area	Risk Description	Inherent Risk	Risk Controls	Residual Risk	Priorities for IA / CFT
	permits to avoid commercial parking charges.		one authority, enabling their recovery to prevent misuse.		