Committee and Date	Item
Audit Committee 9th December 2021 10:00 am	Public

Annual review of the Counter Fraud, Bribery and Anti-Corruption Strategy and activities, including an update on the National Fraud Initiative

Responsible Officer   Ceri Pilawski
e-mail: Ceri.pilawski@shropshire.gov.uk   Tel: 01743 257739

1. Synopsis

Whilst the Council can never be free from fraud activities, it continues to be focused on acknowledging, preventing and pursuing fraud, bribery and corruption and Audit Committee members reaffirm the Council's Counter Fraud, Bribery and Anti-Corruption Strategy.

2. Executive Summary

2.1. This report outlines the measures undertaken to evaluate the potential for the occurrence of fraud, and how the Council manages these risks with the aim of prevention, detection, investigation and subsequent reporting of fraud, bribery and corruption.

2.2. The Counter Fraud, Bribery and Anti-Corruption Strategy has been reviewed and continues to underpin the Council's commitment to prevent all forms of fraud, bribery and corruption whether it be attempted on, or from within, the Council, thus demonstrating the continuing and important role the strategy plays in the corporate governance and internal control framework. This report also provides an update on the action plan to ensure continuous improvement in the fight against fraud, bribery and corruption providing an update to members in response to national and local issues.

3. Recommendations

3.1. Members are asked to consider, and endorse with appropriate comment, the Counter Fraud, Bribery and Anti-Corruption Strategy and measures undertaken and detailed in this report to manage associated risks with the aim of prevention, detection and subsequent reporting of fraud, bribery and corruption.

REPORT

4. Risk Assessment and Opportunities Appraisal

4.1.   The adoption and promotion of an effective Counter Fraud, Bribery and Anti-Corruption approach helps the Council encourage the detection of fraud and irregularities proactively and manage them appropriately.

4.2.   In aligning the Council's Counter Fraud, Bribery and Anti-Corruption Strategy with CIPFA's Code of practice on managing the risks of fraud and corruption, the Council continues to apply best practice. Potential fraud risks are assessed across the Council and activities in place to mitigate these.

4.3.   Internal Audit, working to the Public Sector Internal Audit Standards (PSIAS), has a responsibility to evaluate the potential for the occurrence of fraud and any subsequent management response. This report sets out some of the practices employed to evaluate and manage these risks including involvement with the National Fraud Initiative.

4.4.   The recommendations contained in this report are compatible with the provisions of the Human Rights Act 1998. There are no direct environmental, equalities, consultation or climate change consequences of this proposal.

5. Financial Implications

5.1.   All revisions and activities can be met from within existing budgets.

6. Climate Change Appraisal

6.1.   This report does not directly make decisions on energy and fuel consumption; renewable energy generation; carbon offsetting and mitigation; or on climate change adaption. Therefore, no effect to report.

7. Background

7.1.   The Council sets itself high standards for both members and officers in the operation and administration of the Council's affairs and has always dealt with any allegations or suspicions of fraud, bribery and corruption promptly. It has in place policies, procedures and initiatives to prevent, detect and report on fraud, bribery and corruption, including a Speaking up about Wrongdoing policy, Anti Money Laundering (AML) procedures and guidance, all supported by an overarching Counter Fraud, Bribery and Anti-Corruption Strategy.

7.2. The Counter Fraud, Bribery and Anti-Corruption Strategy is contained in part five of the Constitution, last reviewed and updated in November 2021. In reviewing the Strategy, only minor adjustments have been made to reflect structure changes at the Council and the move to a more digital approach. All proposed changes are identified in the Strategy in bold italic, underlined font

7.3. The Strategy can be located on the Council's website alongside Speaking up about Wrongdoing policies for both staff and the public and Anti Money Laundering (AML) procedures and guidance. A review of these has identified minor changes which have been reflected in the Strategy and supporting policies, procedures and guidance.

8. Additional Information

Counter Fraud, Bribery and Anti-Corruption Strategy
8.1. Shropshire's strategy clearly identifies the Council's commitment to an effective Counter Fraud, Bribery and Anti-Corruption approach as part of its overall Corporate Governance arrangements. This aligns with CIPFA's Code of practice on managing the risks of fraud and corruption and recognises that the strategy will enable the Council to:
   • Acknowledge and understand fraud risks;
   • Prevent and detect more fraud; and
   • Pursue and punish fraud and recover losses.

8.2. The Strategy reflects best practice from the National Fraud Authority (NFA) Fighting Fraud Strategies and guidance from organisations such as ALARM (the National Forum for Public Sector Risk Management) and the IIA (Institute of Internal Auditors).

8.3. It is recognised that to reduce losses to fraud, bribery and corruption to an absolute minimum, a strategic approach with a clear remit covering all areas of fraud, bribery and corruption that may affect the Council is required. There needs to be a clear understanding of the importance of the links between policy work (to develop a counter fraud, bribery and anti-corruption culture, create a strong deterrent effect and prevent fraud, bribery and corruption by designing robust policies and systems) and operational work (to detect and investigate fraud, bribery and corruption and seek to apply sanctions and recover losses where they are found).

8.4. The temptation may be to 'pick and choose' actions. However, the full range of integrated action must be taken forward with the Council's focus clearly on outcomes (e.g. reduced losses) and not just activity (i.e. the number of investigations, prosecutions, etc.).

8.5. The strategy continues to emphasise the Council's remit to reduce losses to fraud, bribery and corruption to an absolute minimum. It:
- Demonstrates links between 'policy' work and 'operational' work. Has robust arrangements and executive support to ensure counter-fraud, bribery and corruption measures are embedded throughout the Council.
- Shows agreement by both the political and executive authority for the Council's approach.
- Acknowledges fraud and identifies accurately the risk.
- Creates and maintains a strong structure to pursue its remit including:
  - Having the necessary governance, authority and support;
  - Providing for specialist training and accreditation;
  - Completing appropriate propriety checks;
  - Developing effective relationships with other organisations.
- Enables actions to tackle the problem by:
  - Integrating different actions;
  - Building a strong counter fraud and anti-corruption culture;
  - Having clear actions to deter any problem;
  - Acting to prevent fraud and corruption;
  - Early detection of any issues;
  - Investigating appropriately in accordance with clear guidance;
  - Having clear and consistent sanctions where fraud or corruption is proven;
  - Having clear policies on redressing losses.
- Focuses on outcomes and not merely activity.

National Picture

CIFAS Fraudscape 2021
8.6. CIFAS is a fraud prevention service in the United Kingdom. It is a not-for-profit membership association representing organisations from across the public, private and voluntary sectors. In their 2021 fraudscape document, they report 309,849 cases of fraudulent conduct reported to the National Fraud Database (NFD), one case every two minutes. High risk areas of fraud include:
- Identity fraud and misuse of facility accounted for 82% of cases in 2020.
- A large proportion of identity fraud victims were between 31 and 40 years and 51 plus. Social media continued to be used to harvest personal and financial information for example with online quizzes designed to collect detailed personal information.
- Covid 19 related cases were reported such as applying and paying for false vaccinations and tests, applications for stimulus packages and grant refunds, the abuse of bank accounts

indicating behaviours of money muling[1] with business accounts used to launder funds. 2020 saw a 23% increase in companies being impersonated, partly due to the stimulus packages offered to support businesses through the pandemic.

- Facility takeover grew significantly enabled by social engineering techniques such as phishing[2] and smishing[3], harvesting information to take over accounts, campaigns impersonated delivery services such as DPD parcel delivery, Royal Mail and public bodies such as HMRC to socially engineer individuals to reveal personal and financial information.
- Despite lower levels of recruitment, there were notable filings of dishonest actions and disclosing personal information to third parties. Movement to remote working for employees in some cases has increased the potential for individuals to harvest data for fraudsters and increased the potential for false references.

8.7. The CIFAS report summarised by stating that much of the impact of COVID-19 on fraud is still to be seen.

- Perpetrators are highly likely to exploit a range of vulnerabilities and uncertainties, including employment scams, travel scams and investment fraud, as well as the stimulus packages on offer.
- The impersonation of companies throughout the pandemic means it is highly likely companies will be increasingly targeted if further provision is offered to business to support the economy.
- Identity fraud remains a priority for all sectors, due to the rise of synthetic identities and readily available access to false documentation.
- The rise in cybercrime as a service, such as phishing kits, fraud tool kits and hacking services, is an extremely high threat to all sectors.
- Social media continues to be a key enabler for recruiting mules with more than two thirds of the UK population using a social media platform.
- The pandemic has changed how mules "cash out". Cashing out via cryptocurrency assets and wallets has become attractive to criminal networks due to the anonymity this provides.
- Facility takeover has seen a significant rise during the pandemic. It is highly likely that digital channels will continue to

---

[1] A money mule, sometimes called a "smurfer," is a person who transfers money acquired illegally in person, through a courier service, or electronically, on behalf of others. Typically, the mule is paid for services with a small part of the money transferred.

[2] Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

[3] Smishing is the fraudulent practice of sending text messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords or credit card numbers.

be favoured but as organisations bolster their defences, threat actors may look to exploit vulnerabilities via telephony channels.

- Remote working remains a threat and so it is essential that organisations review their working from home policies and audit the data and information that staff have access to.

8.8.   The full report is available at:
https://www.fraudscape.co.uk/#welcome

8.9.   AON, the Council's insurance brokers reported on the top ten risks in November of this year fraud elements of which include cyber criminals capitalising on remote working showing an increase in ransomware attacks and business interruption.

Fighting Fraud and Corruption Locally (FFCL); A Strategy for the 2020s

8.10.   The Fighting Fraud and Corruption Locally Strategy (FFCL) 2020 is England's counter fraud and corruption strategy for local government. It continues to be the definitive guide for council leaders, chief executives, finance directors, and all those with governance responsibilities. It is aimed at local authorities who undertake work in the counter fraud area. The Companion contains good practice and a checklist for local authorities to use as part of making sure they have the right processes and resources in place. The Council's Counter Fraud, Bribery and Anti-Corruption Strategy continues to be aligned to this checklist.

8.11.   The Audit Committee approved an Action Plan to ensure that the Council continues to protect its assets and further improve its resilience to fraud and corruption. The following has been and continues to be delivered:

Action Plan

Action	Implementation Date and Update
To proactively use the results of previous fraud risk assessments and publicly available information from recognised organisations to direct counter fraud resources in the annual Internal Audit Plan.	Completed and ongoing.
To refresh the Council's suite of anti-fraud policies, strategies and procedures and to ensure that they continue to be relevant to national guidance.	Annually in November. Completed and ongoing.
To remind all staff and members of their role in sustaining a strong counter fraud, bribery and anti-	Annually in November.

Action	Implementation Date and Update
corruption culture and the appropriate reporting channels where any fraud is suspected.	Completed through directorates and management meetings.
To undertake an annual Fraud Risk Assessment covering the Council's main areas of exposure to fraud and to use the results to influence the Council's approach moving forward.	Annually in October. Completed and ongoing.
To update the Council's e-learning module on Fraud Awareness and to promote its uptake by all employees.	Completed and ongoing.
To be an active participant in the National Fraud Initiative (NFI) and to investigate robustly suspected cases of fraud identified through NFI and report outcomes to Audit Committee.	Biannually in November. Completed and ongoing.
To refresh the Fraud Awareness pages on the web site and to engage with managers through targeted communications to emphasise their obligations to operate effective systems of internal control which are designed to reduce the risk to the Council of fraud, error or inadvertent loss.	Completed and ongoing annually in November.
Refresh of the Council's Money Laundering Policy, communication of and training on.	Completed and ongoing.

CIPFA Fraud and Corruption Tracker (CFaCT) annual survey

8.12. The CIPFA Fraud and Corruption Tracker (CFaCT) is an annual survey of the fraud and corruption detected in local authorities across the UK. Its intention is to provide a more complete picture of local authorities' vigilance in respect of fraud. It examines:
- Levels of fraud and corruption detected each financial year;
- Number of investigations undertaken;
- Types of fraud encountered;
- Emerging trends.

It is an up-to-date overview of all fraud, bribery and corruption activity across the UK public sector.

8.13. 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.

8.14. The survey has not operated for 2020/21 but we can now report on the outcomes contained in the national report produced in early 2021 based on the previous year's inputs from August 2020. This report[4] recognises that it does not capture the impact of the ongoing coronavirus pandemic but provides an insight about the fraudulent activities that occur across the local government landscape in the period prior to the national response effort, highlighting the importance of counter fraud protocols in fighting fraud and corruption.

8.15. The report highlights:
- the types of fraud identified in the 2019/20 CFaCT survey
- the monetary cost value of fraud in 2019/20
- the impact of counter fraud and prevention activities to improve the public sector budget
- the emerging risks and threats impacting the fraud and corruption landscape.

8.16. For local authorities in the UK, CIPFA has estimated that the total value of fraud identified and prevented in 2019/20 is approximately £239.4m, which is an average value of £5,090 per fraud case. In the previous year, there was an estimated value of £253m with a lower average of £3,600 per case detected and prevented.

8.17. 47,000 instances of fraud had been detected or prevented in 2019/20, which is lower than the approximation of 71,000 reported by CIPFA in 2018/19. Council tax fraud represented almost two thirds (65%) of these identified instances of fraud with an estimated value of £35.9m, followed by disabled parking concession (Blue Badge Scheme) and housing fraud which represent 17% and 11% of the total cases of UK public sector fraud, respectively. Grant fraud (prior to the COVID-19 grant disbursement), represented 0.3% of the total identified instances of UK public sector fraud and 15% of the total value (£36.6m). The largest growing fraud area is housing tenancy (other), with an estimated £60.1m lost in 2019/20 compared to £47.7m in 2018/19. This is followed by council tax single person discount (SPD) which has an estimated increase of £9.6m to an estimated value of £29.0m for cases detected/ prevented in 2018/19.

8.18. Other notable frauds that did not emerge as major types of fraud within the national picture include:

---

[4] https://www.cipfa.org/services/cipfa-solutions/fraud-and-corruption/fraud-and-corruption-tracker

- adult social care
- insurance
- procurement
- no recourse to public funds/ welfare assistance
- payroll, recruitment, expenses and pension
- economic and voluntary sector support and debt
- mandate fraud, manipulation of data and grant fraud.

8.19. The two highest perceived fraud risk areas for 2019/20 remain the same as previous years: procurement and council tax SPD. This shows these are the areas that require strict controls and support. The perceived third, fourth and fifth highest fraud risk areas are business rates, adult social care and council tax reduction (CTR) respectively.

8.20. Overall messages were that:
- The cumulative value of fraud prevented and detected by local authorities continues to decline supporting the need to stay vigilant and continue to raise awareness of fraud risks within the Council. These are assessed regularly at Shropshire and at least annually in all areas.
- A dedicated counter fraud team remains the preferred method of delivery amongst respondents. Counter fraud resources are spread across the Council in Shropshire.
- Organisations should maximise the opportunities to share data and intelligence where initiatives allow to reduce losses through fraud. This is actioned through the NFI activity, Action Fraud, NAFN[5] and other bodies when beneficial.
- Whistleblowing allegations received remained constant with 2018/19 with access at 85% of authorities to a helpline. CIPFA recommend actively public campaigns across all levels of the Council to raise awareness of whistleblowing policies and access to supporting services. This is reported upon elsewhere in this report and annually in terms of delivery to the Summer Audit Committee.
- Cyber security threats increase proportionally to remote working and increased electronic service applications. Strong control measures are required here. Audit conduct reviews of cyber security controls and dedicated resources in IT manage these.
- Authorities should consider their strategies against the Fighting Fraud and Corruption Locally 2020 Strategy checklist. Shropshire Council has, details appear in this report.

International Fraud Awareness Week

8.21. Week beginning the 15th November saw International Fraud Awareness week. To support this Internal Audit staff adopted an email footer to highlight to others how fraud can impact on their service areas and result in the loss of public money. In addition,

---

[5] National Anti-Fraud Network

initiatives and links to corresponding strategies and policies were highlighted through the internet, included on the staff newsletter, in reminders to complete the fraud awareness corporate trainings, how to report suspected fraud and other social media sites such as Yammer[6].

CIPFA's Counter Fraud Assessment Tool

8.22. This tool is designed to help councils assess their counter fraud arrangements against the standards set out in CIPFA's Code of Practice on Managing the Risk of Fraud and Corruption. The tool is used as a basis for ongoing improvement and development planning alongside assurance on the adequacy and effectiveness of the Council's counter fraud arrangements. The action plan reported on within this report is reflective of the improvements identified when applying this tool.

8.23. Whilst no organisation is fraud proof, Shropshire Council continues to take robust steps to improve its resilience and to meet the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption. Leadership has acknowledged its responsibilities for managing risks and it has robust arrangements in place to identify and manage risks. It has a counter fraud strategy, backed up by the resources and arrangements to carry it out, and is proactive in managing fraud and corruption risks and responds effectively. Stakeholders can be confident in the approach taken by the Council and meeting the standards of this code contributes to good governance. Please see **Appendix B** for a more detailed breakdown. Where percentages fall below 100% the planned activities recorded within this report and particularly within the action plan in paragraph 8.11 of this report are designed to maintain and improve the fraud risk environment.

National Fraud Initiative (NFI)

8.24. The National Fraud Initiative (NFI), run by the Cabinet Office, is an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud. The Council continues to participate in this exercise. In July 2020 the NFI reported the exercise identified and prevented, £245m fraud and error, £215.8 in England of which:
- Pension fraud and overpayments (£55.5m)
- Fraudulently or wrongly received, council tax single person discount (£43.9m)
- Housing benefit fraud and overpayment (£35m)

The current exercise for 2020/21 will finish on the 31st March 2022 and an updated report from the NFI is expected in July 2022.

---

[6] Yammer is a social network platform that fosters cross-institutional engagement. It combines features found in Twitter, Facebook, and other similar platforms

8.25. Results currently for Shropshire of the 2020/21 data matching exercise are shown in the table below. Please note there are a small number of investigations still outstanding across these reports which may impact further on the figures shown. In the event of additional savings being identified prior to the closure of this exercise, these will be advised to the Audit Committee in due course.

8.26. The July 2020 national report in respect of the 2018/19 data matching exercise is available online https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903221/NFI_report_2020.pdf

Area of Investigation	Outcome of Investigations 2020/21	2020/21 Saving Identified	2018/19 Saving Identified
Deceased Pensioner Matches	This report identifies where an occupational pensioner has died but pension is still in payment. 115 matches were identified, and all matches investigated. Two deceased pensioners were identified as receiving a pension into the deceased pensioner's bank account when the service had not been advised of the death. This resulted in overpayments of £2,032.52. £2,000.95 in respect of the overpayments is being recovered from the estates or next of kin. The balance of £31.57 in respect of the second overpayment is being reviewed to establish the Executor/Next of Kin details. In the absence of progress the amount will be written off due to low value.	£2,032.52	£19,408.64 (11 incidents from 77 matches)
Housing Benefit Claimants to Student Loans	This report identifies individuals who are claiming benefits, but who's student loan eligibility results in them being ineligible for those benefits. 21 matches were identified, and all matches investigated. One case was identified in respect of undeclared student loan and the amount is being recovered through reductions in weekly benefit payment.	£2,275.39	£0.00
Blue Badges to Deceased Persons	The report identified 555 matches and all matches were investigated. All cases had been notified prior to receipt of the NFI data matches.	£0.00	£0.00

Area of Investigation	Outcome of Investigations 2020/21	2020/21 Saving Identified	2018/19 Saving Identified
Concessionary Bus Passes to Deceased Persons	The reports identify concessionary travel pass holders who have been matched to deceased records. These reports identified 2,181 matches. All matches were investigated and identified a total of 1,664 errors where the Council had not been notified of the pass holders' death. All passes have since been cancelled. The Cabinet Office estimates a saving of £24.00 per pass hence the savings figure applied.	£39,936	£23,808
Housing/ Council Tax Benefits/ Council Tax Reduction Scheme	Dispensation has been obtained from the Cabinet Office that the team would only sample investigate a small number of matches due to existing controls in place in respect of real time reporting and processes for annual billing. No overpayments were identified on the matches reviewed, other than the student loan case which has been reported above.	£0.00	£0.00
Creditor Reports	Creditor reports on possible duplicate payments, invalid VAT registration numbers and duplicate supplier accounts were provided. Data is still being reviewed at the time of this report	£0.00	£3,184.00
Housing Tenants to Deceased Persons	These reports identified 33 matches. All were investigated and found to be due to either timing differences or mismatches.	£0.00	£0.00

Area of Investigation	Outcome of Investigations 2020/21	2020/21 Saving Identified	2018/19 Saving Identified
Other reports	Other reports such as deceased parking permit holders, taxi drivers to in-country immigration, payroll to payroll and procurement were all investigated and where appropriate records have been updated accordingly. No savings have been identified from these reports.	£0.00	£0.00
	Total Savings	**£44,243.91**	**£46,400.64**

Transparency requirements

8.27. Legislation on transparency applies to anti-fraud activities. The Local Government Transparency Code sets out the minimum data that local authorities should be publishing, the frequency with which it should be published and how it should be published. The Council has complied with these requirements, the results of which can be found on the web site[7].

Update on Regulation of Investigatory Powers Policy and Guidance (RIPA) Activity

8.28. RIPA Policy and Guidance sets out the approach the Council will take with respect to the authorisation and use of surveillance activity to deliver the Council's statutory and public duties, whilst protecting individuals' right to privacy. The Council's existing Regulation of Investigatory Powers Policy, which was adopted in August 2015, is currently being updated to reflect both legislative and organisational changes. The updates will ensure that any surveillance activities undertaken by the Council are compatible with the human right to privacy by ensuring compliance with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA), the Investigatory Powers Act 2016 (IPA), the European Convention on Human Rights (ECHR) and the Human Rights Act 1998 (HRA).

8.29. The Policy addresses the use of activities that involve:
- the surveillance of individuals;
- the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS); and
- the obtaining of communications data.

8.30. All Council applications to acquire communications data are processed through the National Anti-Fraud Network who act as the Council's Single Point of Contact (SPoC). National Anti-Fraud Network (NAFN) engages with the applicant and the Office for Communications Data Authorisations (OCDA) to obtain authorisations on the Council's behalf. A senior manager at service manager level or above within the Council must be made aware of all applications before they are submitted to NAFN for processing.

8.31. The Audit Committee's governance role will be reinforced in the refreshed policy and guidance, full details of which will appear on the Council agenda in the new year.

Whistleblowing Policy

8.32. The Council has a whistleblowing policy for the public and one for its employees. Both policies have been reviewed and updated in

---

[7] https://shropshire.gov.uk/open-data/

respect of key contacts and staff information. There have been no changes proposed to the process of 'blowing the whistle'. An annual reminder is circulated to all employees to raise awareness as to the availability of this policy.

8.33. The Whistleblowing Policy is available to staff via the Intranet pages and is also available to them, along with members and the public, via the website; allowing it to be accessed from any computer. This is particularly important as it allows staff to access the policy outside of a work environment, where they may be reluctant to be seen accessing the Whistleblowing policy.

Anti-Money Laundering (AML) Procedure

8.34. There are no revisions proposed to the Council's Anti-Money Laundering procedure and guidance, they continue to reflect The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Training is available on the Council's electronic training tool, Leap into Learning. The AML Officer and her deputies continue to stay aware of their requirements. In addition, Directors continue to spread awareness, identify any money laundering risks in their areas to be shared at least annually with the AML Officer and identify employees who need training.

Serious Organised Crime Checklist

8.35. Organised crime includes drug trafficking, human trafficking, child sexual exploitation, high value fraud and cyber-crime. Organised crime groups may seek to benefit from public services in different ways, including to raise money through fraudulent activity and to use businesses / services used by local authorities to launder criminal proceeds. In this way public money can be lost to local authorities and can ultimately fund other illegal activity.

8.36. The Home Office Serious and Organised Crime report and checklist provides a methodology to assess the risk from serious and organised crime and corruption and is essential in allowing the Council to identify areas of concern, potential vulnerabilities and to act to strengthen processes and structures that safeguard public money. The checklist evaluates our response and activities in relation to:
- Awareness, Strategy, Guidance and Training
- Risk Management
- Communication and Information/ Intelligence Sharing
- Whistleblowing
- Assurance
- Operational controls for
- Licensing
- Planning/ Development management
- Social Housing

- Procurement
- Insider threat

8.37. Directors, Heads of Service and key Procurement Officers continue to evidence activities against the checklist providing a balanced assessment of the Council's exposure to the risks. In the main, at this high level, risks appear well managed and where improvements can be made, actions have been highlighted as part of an improvement plan. The Council's Commissioning and Assurance Board continues to oversee operational management of these actions.

Awareness and training

8.38. Fraud awareness training is available on the Council's eLearning tool, Leap into Learning and continues to result in positive feedback from recipients. Questions explore awareness and knowledge of counter fraud procedures including the availability of the whistleblowing policy. Audit Committee members have been provided access to the training to complete and experience it first-hand.

Qualified officers

8.39. Internal Audit has a qualified officer with the Advanced Professional Certificate in Investigative Practice and two officers who are accredited CIPFA Counter Fraud Technician. In total over a third of the Audit team have qualifications or considerable experience in conducting investigations.

Shropshire Council counter fraud risks and plans

8.40. In terms of potential for fraud, the counter fraud risk assessment has been refreshed and shared across all directorates. There is no change to the high-risk area of housing benefits and cybercrime. Grant risks have fallen out of this category reflecting the reduced value and quantity of business grants being manged.
High
- Housing benefits
- Cybercrime

Thirteen medium risk areas continue to be identified; the list of risks is:
Medium
- Payroll, fraudulent travel, expense, overtime and timesheets
- Pension continues after death
- Employee commits benefit fraud
- Inappropriate and incorrect contract awards
- False invoicing
- Debtors; claiming false exemptions, failing to raise a debt, suppressing recovery action
- Housing applications for financial assistance with repairs, homelessness and lettings

- Council tax discounts
- NDR reliefs
- Parking abuse including blue badge use/disabled parking
- Direct payments / personal budgets
- Property and taxi licenses
- School, diversion of resources.

8.41. There are several steps in place, continuing, planned or underway to help to explore, identify and mitigate these fraud risks:

- Housing benefit investigations are referred to the Department of Work and Pensions Single Fraud Investigation Service for action. Housing Benefits, Internal Audit and Human Resources officers continue to jointly risk assess any employees that are suspected of benefit fraud to consider if internal investigations are required or Council assets within the employee's control may be at risk. A Housing Benefit audit in 2020/21 recorded a good level of assurance.

- The 2020/21 NFI exercise including data matching for payroll, pensions, creditors, housing benefit, council tax, personal budgets, blue badge parking permits, direct payments are reported on within this report.

- To support the allocation of grants to businesses during the COVID pandemic, the beginning of the year showed continuing due diligence applied through the NFI database; companies house enquiries and by using Spotlight, a Government initiative to reduce losses from fraud and error. There a re a few residual grant claims and the controls will continue with these.

- To reduce the risk of cybercrime and the impact it would have on all areas of the Council, we are completing an ongoing programme of IT Audit work of key infrastructure systems, including internet security, patch management, IT change management and legacy infrastructure and systems. We are also part of a multi-agency working group which is developing a draft Local Resilience Forum ICT and Cyber Response Framework to manage the tactical aspects of a multi-agency response to a cyber-attack.

- Internal Audit resources have been deployed to provide assurance and advice in respect of initiatives such as; data analytics for financial systems; recruitment processes; management of new grants; property access security systems; joint arrangements for children's services and internal control self-assessments.

- The current year audit plan includes several internal audit reviews that have been conducted, or are planned, to help ensure

appropriate controls are in place, and are operational, to counter the fraud risks identified from the risk assessment:

- IT reviews, as detailed earlier in this section
- Payroll including holiday pay
- Counter fraud work, NFI participation, review of policies and delivery of training and awareness campaigns
- Debt recovery
- Income collection
- Purchase ledger
- Sales ledger
- Grant reviews across all Council services
- General ledger
- Contracts and tendering including financial evaluations, IT contracts, dog wardens and highways
- Council tax collection
- Business rates (NDR)
- Parking cash collection
- Housing strategy and provision
- Adoption allowances, appointeeships, placement and care assessments

---

List of Background Papers (This MUST be completed for all reports, but does not include items containing exempt or confidential information)

CIPFA: Code of practice on managing the risks of fraud and corruption, October 2014
The Bribery Act 2010
NFA Fighting Fraud Together, the strategic plan to reduce fraud
Fighting Fraud Locally: The Local Government Fraud Strategy 2020
The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
Regulation of Investigatory Powers Policy 1 October 2015
CIPFA Fraud and Corruption Tracker (CFaCT) survey report 2020
National Fraud Initiative (NFI) Report 2020
Home Office Serious and Organised Crime report and checklist 2017
Cifas Fraudscape 2020 Full Digital Report

Cabinet Member (Portfolio Holder) Lezley Picton, Leader of the Council and Brian Williams, Chairman of Audit Committee
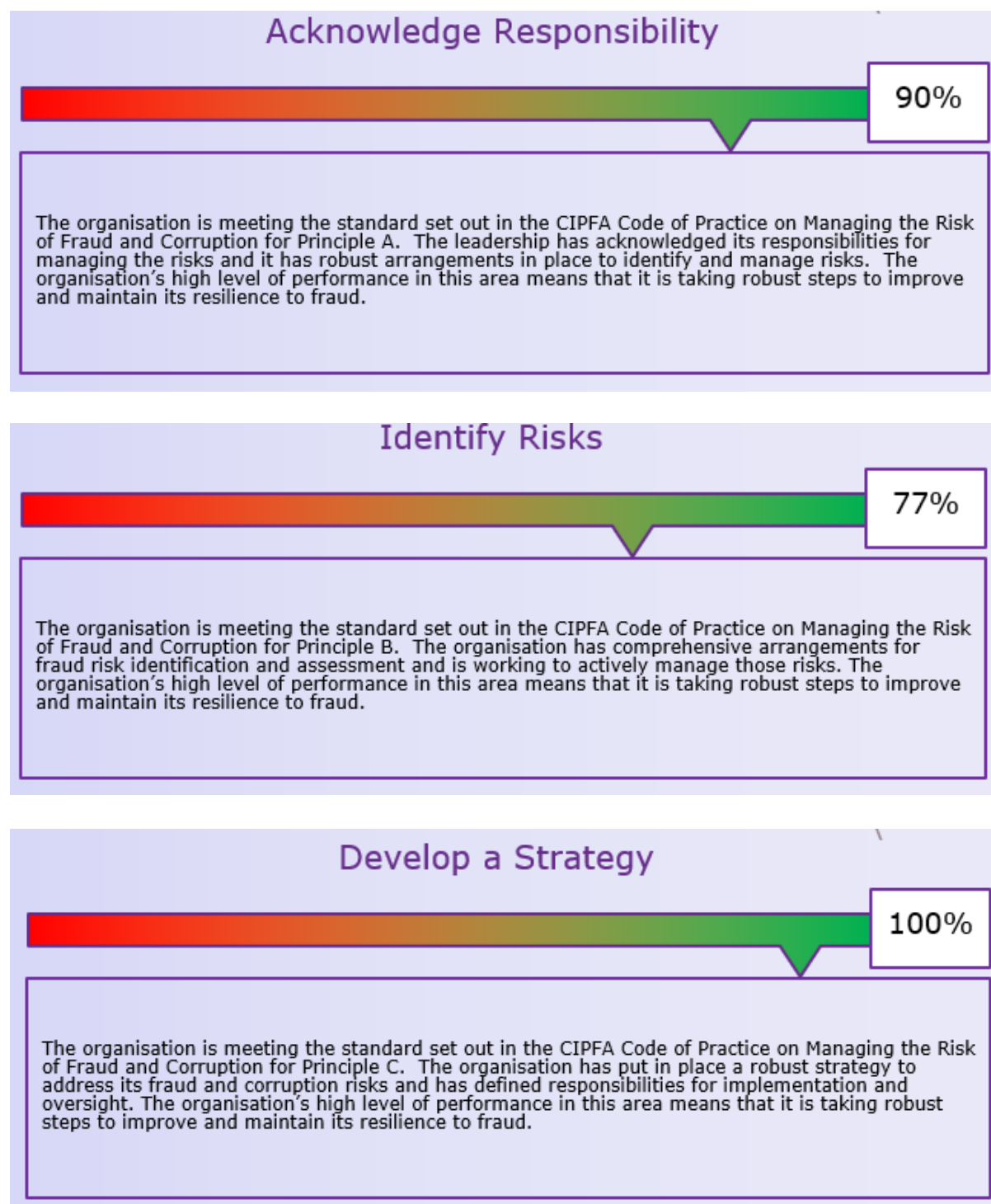

Local Member N/A

Appendices:

Appendix A: Counter Fraud Bribery and Anti-Corruption Strategy

Appendix B: Counter Fraud Assessment Tool – reviewed Oct 2021

APPENDIX B Counter fraud assessment tool: CIPFA's code of practice on managing the risk of fraud and corruption

Acknowledge Responsibility

90%

The organisation is meeting the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption for Principle A. The leadership has acknowledged its responsibilities for managing the risks and it has robust arrangements in place to identify and manage risks. The organisation's high level of performance in this area means that it is taking robust steps to improve and maintain its resilience to fraud.

Identify Risks

77%

The organisation is meeting the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption for Principle B. The organisation has comprehensive arrangements for fraud risk identification and assessment and is working to actively manage those risks. The organisation's high level of performance in this area means that it is taking robust steps to improve and maintain its resilience to fraud.

Develop a Strategy

100%

The organisation is meeting the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption for Principle C. The organisation has put in place a robust strategy to address its fraud and corruption risks and has defined responsibilities for implementation and oversight. The organisation's high level of performance in this area means that it is taking robust steps to improve and maintain its resilience to fraud.

Provide Resources

85%

The organisation is meeting the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption for Principle D. The organisation has put in place a robust process for reviewing its capacity and capability which aligns to its counter fraud strategy. The organisation's high level of performance in this area means that it is taking robust steps to improve and maintain its resilience to fraud.
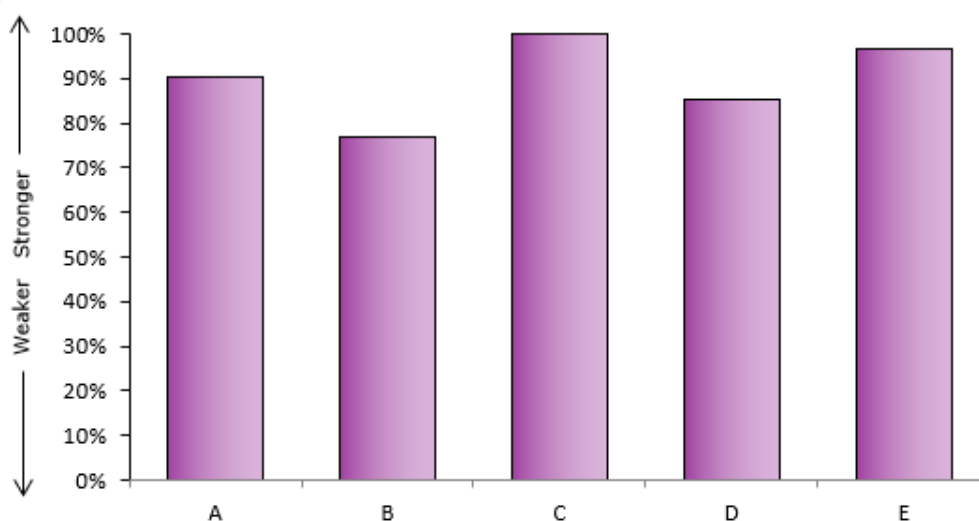
Take Action

97%

The organisation is meeting the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption for Principle E. It is actively implementing the actions identified in its counter fraud strategy and responding effectively to the risks emerging. It reviews its performance and has arrangements in place to provide assurance and accountability. The organisation's high level of performance in this area means that it is taking robust steps to improve and maintain its resilience to fraud.

Summary Page

91%

The organisation is meeting the standard set out in the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption. The leadership has acknowledged its responsibilities for managing the risks and it has robust arrangements in place to identify and manage risks. It has a counter fraud strategy, backed up by the resources and arrangements in place to carry it out. The organisation is proactive in managing fraud and corruption risks and responds effectively. Stakeholders can be confident in the approach taken by the organisation and meeting the standards of the counter fraud code contributes to good governance. Whilst no organisation is 'fraud proof', the organisation has taken robust steps to ensure its resilience. This high level of performance should be acknowledged