EAST RENFREWSHIRE COUNCIL

AUDIT AND SCRUTINY COMMITTEE

26th September 2023

Report by Chief Executive

MANAGING THE RISK OF FRAUD AND CORRUPTION –
FRAUD RESPONSE STATEMENT 2022/23 &
AUDIT SCOTLAND FRAUD IRREGULARITY 2022/23 REPORT

PURPOSE OF REPORT

1.   In order to demonstrate compliance with the Code of Corporate Governance, this Fraud Response Statement provides an overview of measures in place across East Renfrewshire Council to address Anti-Fraud, Bribery and Theft, managing the risk of fraud and corruption, and to provide an update on actions undertaken during 2022/23 where appropriate.

2.   In addition, this report includes East Renfrewshire Council's response to the Fraud and Irregularity 2022/23 report published by Audit Scotland in July 2023. This report is a summary of the cases of fraud and other irregularities at public bodies reported by external auditors for the financial year 2022/23. A copy of this report is available on the Audit Scotland website https://www.audit-scotland.gov.uk/publications/fraud-and-irregularity-annual-report-202223

RECOMMENDATIONS

3.   It is recommended that the Audit and Scrutiny Committee

- notes the content of the Fraud Response Statement and the work being undertaken across the Council in relation to managing the risk of fraud and corruption and the reporting already in place; and

- considers the feedback provided in the context of the comments made in the Audit Scotland report – Fraud Irregularities 2022/23.

BACKGROUND

4.   The Council is committed to fighting fraud and bribery, whether attempted from inside or outside of the authority, in order to protect public funds. Suppliers, contractors, employees, members and service users are expected to act with integrity and without intention to commit fraud or bribery against the Council.

5.   It is recognised that there is increased financial pressure on businesses and employees due to the Covid-19 pandemic and more recently the Cost of Living with a potential heightened risk of fraud being attempted. Services continue to review existing controls to ensure that they are still effective and appropriate and at the same time introduce new controls to address new risks. Measures like these outlined in this report have always been important but the unprecedented challenges and the opportunities it has presented for fraudsters, bring a renewed focus on ensuring effective governance and controls are in place.

6.   Within the Code of Governance, work to address fraud, bribery and theft is undertaken in line with the Chartered Institute of Public Finance & Accountancy (CIPFA) Code on "Managing the Risk of Fraud and Corruption" which sets out the principles that define the governance and operational arrangements necessary for an effective counter fraud response. The Code is applicable to all public services organisations and is comprised of five key principles, which are to.

- acknowledge the responsibility of the governing body for countering fraud and corruption
- identify the fraud and corruption risks
- develop an appropriate counter fraud and corruption strategy
- provide resources to implement the strategy and
- take action in response to fraud and corruption.

7.   A revised Anti-Fraud, Bribery and Theft Strategy 2022 - 2027 written in line with the CIPFA Code above, was approved by the Corporate Management Team on 7th December 2022. The revised strategy aims to promote an attitude of zero tolerance to fraud. No fraud is acceptable, regardless of the value or scale.

8.   The CIPFA Code recommends that an annual report, or Fraud Statement, is considered setting out the fraud and corruption risks and the steps taken to prevent these The previous Fraud Statement was considered and approved by the Audit and Scrutiny Committee on 29th September 2022 and this report provides an updated overview of measures in place to address Anti-Fraud, Bribery and Theft and of work undertaken during 2022/23 where appropriate.

Audit Scotland Report – Fraud and Irregularities 2022/23 Update – Overview

9.   The Fraud Irregularity Update 2022/23 shares risks and case studies to support the Scottish Public sector in the prevention of fraud. The report sets out the cases identified during 2022/23 including the details of the control weaknesses which contributed to these cases. External auditors identified 12 cases of fraud or irregularity totalling over £139,000 in audited bodies in 2022/23 (7 cases totalling £401,500 were identified in 2021/22).

10.   Specific recommendations in this report are that Public bodies should ensure they have effective counter-fraud arrangements which includes:

- effective counter-fraud governance arrangements
- a counter-fraud strategy and regularly reviewing counter-fraud plans
- regular assessment and review of internal controls and
- consider the control weaknesses identified in the report.

11.   These recommendations have been considered in relation to practices within the Council to proactively try and identify where the risks and potential weaknesses in controls may exist and to ensure that appropriate measures have been taken or are in place to prevent these happening within East Renfrewshire Council.

MEASURES IN PLACE TO ADDRESS ANTI-FRAUD, BRIBERY AND THEFT

Governance

12.   The Anti-Fraud, Bribery and Theft Strategy 2022 - 2027, sets out a range of approaches within the Council to identify and minimise fraud and corruption risks. These include independent reviews of adequacy, efficiency and effectiveness of internal controls by Internal Audit, ensuring all recruitment is undertaken in line with the Recruitment and Selection Policy and that orders and contracts are awarded in accordance with the Council's approved Contract Standing Orders and Financial Regulations.

13.   The Council has put in place a range of policies and procedures to support the Strategy to ensure that appropriate action is taken to prevent, detect and investigate fraud. A range of data and intelligence analysis will be undertaken to detect fraud (or attempted fraud) at the earliest opportunity and appropriate sanctions (including disciplinary, regulatory and criminal) will be taken. East Renfrewshire Council will investigate fraud referrals and seek appropriate redress where possible.

14.   The Audit and Scrutiny Committee provides a scrutiny role in relation to the application of the Anti-Fraud, Bribery and Theft Strategy. The investigation of suspected fraud or bribery is normally carried out by the Internal Audit team and is reported to the Audit and Scrutiny Committee quarterly by Internal Audit.

ICT and Cyber Crime

15.   Guidance, policies and risk assessments provided throughout the Covid-19 period have been retained as these continue to provide pertinent guidance across a range of cyber and information security topics. These cover information security when working at home; how to manage information on personal devices; use of strong passwords/passphrases and phishing awareness. Campaigns continue to check our users' response to potential phishing emails which continues to help shape further controls and training with all employees who click during campaigns receiving tutor led targeted training.

16.   It is important that East Renfrewshire Council has a trained, security focused workforce capable of identifying suspicious communications and requests, and more importantly know how to react to these. It is vital to create an holistic approach to detecting potential fraud including, but not limited to: Online fraud; User account fraud; Phishing and ransomware; False invoicing; False IT Service support calls and/or emails. This year the Council as introduced an additional tier of email protection as part of defence-in-depth, giving staff visual cues on the security profile of emails where these emails have passed through all other security checks, providing indicators such as such as first time receipt from sender, potential signs of phishing etc.

17.   East Renfrewshire Council participates in a wider UK programme to identify and prevent phishing attacks on the public sector by asking staff to forward suspicious emails to scan@netcraft.com as well as information.security@eastrenfrewshire.gov.uk   This results in suspicious content being addressed and blocked from continuing to proliferate across the public sector.

18.   Both online and tutor led Information and Cyber Security Training continue to provide employees with security focused information for both their work and personal life. Mandatory online training has been increased to yearly (from every 2 years) at the request of the Corporate Management Team reinforcing the importance of security to the Council and ensuring this focus remains.

19.   Specific "Focus On" sessions continue to provide tutor led short topic targeted sessions covering areas including Passwords and Phishing. An in-person cyber exercise was held in September 2022 with further similar sessions to be run every 3 years.   Department Management Teams (DMTs) are progressing with their Business Continuity Plans (BCP) after cyber sessions were delivered aimed at enhancing awareness of potential consequences related to cyber incidents and to think in advance about how ready they are to respond. A further in person cyber day for ICT, ISF (Information Security Forum) and CRMT (Crisis Resilience Management Team) is scheduled for September 2023 aimed at building wider cyber security awareness. This work also stresses to employees that they are the Council's strongest defence against such threats and malicious actors who may be attempting to gain access to Council information, computing systems and networks. Employees are trained to always be suspicious and question, not just react, when something is unusual or not expected.

20.   The Council actively participates in the National Cyber Security Centre (NCSC) Active Cyber defence programme which provides tools and services which seek to reduce the harm from cyber-attacks and protect against a range of security threats and is an active member of the Scottish Local Authority Security Group (SLAISG) Scotland's WARP (warning, advice and reporting point) which facilitates the sharing of advice, best practice and potential cyber threats and attacks across the public sector.

21.   The Council continues to invest in managed ongoing vulnerability management across its server, desktop and M365 estate resulting in all assets being monitored for vulnerabilities and out of date software. A managed cyber security operations centre (CSOC) ensures key assets across the network are pro-actively monitored for malicious and unusual activity and provides an additional layer or protection from malicious actors attempting to gain a foothold within the network with the aim of breaching our information and systems confidentiality, integrity and availability. The Council are in the process of engaging the services of a CIR (Cyber Incident Response) organisation who would provide, if required, immediate technical response and recovery assistance in the event of a cyber-attack.

22.   It is important that the Council maintains up to date and patched software and applications. Old and outdated systems can become vulnerable and exploited by hackers and cyber criminals and updates assist in keeping Council computing networks and information safe. The Digital Transformation Team, working closely with ICT, continue to ensure that applications and operating systems are patched and updated including the removal of old version of the Windows operating system. This activity requires ongoing and continued support from departments, management and employees.

23.   As recommended in the Audit Scotland Fraud Irregularities Update 2021/2022, a review of the independent review and associated recommendations that were commissioned by the Scottish Environment Protection Agency (SEPA) following a ransomware attack on its systems was undertaken to ensure that the work outlined above in this report, in addition to other measures, would reduce the likelihood of East Renfrewshire Council being subject to a similar attack.

24.   Political tensions in Ukraine have resulted in the UK and the public sector being on heighted security threat. East Renfrewshire Council continues to address areas highlighted by the National Cyber Security Centre during such times of threat.

25.   East Renfrewshire Council is the first Scottish Local Authority to take part in threat intelligence feeds direct into technical areas of the network (firewalls) to further add to defence-in-depth and prevent malicious actors gaining a foothold across the network.

Procurement

26.   The Procurement Team are included in a working group with Scotland Excel looking at information that could be requested during tender stage and thereafter responses shared with Police Scotland.   This working group has been established due to a recognition that fraud of all kinds, including procurement fraud, increased during the recession, that opportunist suppliers have emerged during Covid-19 and that cyber-fraud is on the rise with the new opportunities made possible by the Internet. There is also growing concern that organised crime is engaging in procurement fraud and appropriate steps have been taken to minimise the risk of this within East Renfrewshire Council.

27.   In addition to this work, Procurement include in high value or high-risk contract "The Single Procurement Document (Scotland) standard qualification questionnaire which was supplied by Scottish Ministers for all regulated procurements.   Sections within this which support management of the risk of fraud and corruption include – Criminal Convictions; Conspiracy; Corruption; Money Laundering; Payment of Taxes; Blacklisting; Bankruptcy and Arrangement with Accounts Payable.

Health and wellbeing

28.   The Council recognises that there are increasing levels of mental health issues within the workforce which could result in some employees requiring additional wellbeing support. The Council has a Health and Wellbeing Plan and has undertaken a health and wellbeing survey to gain feedback from employees. Health and Wellbeing officers have been introduced to support employees and the Council promotes and offers a range of work-life balance options and signposts employees to a wide range of support organisations who can provide assistance.   Managers are encouraged to have regular contact with employees and enquire about their health and wellbeing and to watch out for signs of mental health in the workforce. This is supported by training for managers and employees. Since the pandemic the Council's employee counselling services continues to see a high number of employees accessing the services (which can be accessed via manager or self-referral). This service continues to be promoted alongside other support mechanisms for employees.

Payment/Insurance/Payroll and HR

29.   The Council has established financial, HR/payroll and Council Tax systems with all procedures well documented and guidance available on the Council Intranet which assists employees to work in hybrid arrangements. These systems incorporate hierarchies of control so that there are automatic limits and reports on what individual employees can do.

30.   Inventories of furniture and equipment continue to be maintained including items taken home to support hybrid working by employees. This continues to be reviewed in light of "The Way We Work" Project.

31.   Specific controls are in place across all processes, in particular "higher risk" (for example payment or cash involved) to ensure risk of loss through fraud is minimised. This includes processes to prevent fraudsters seeking either directly or indirectly (through customers or suppliers) to elicit funds from the Council through misleading/false information. To help ensure employees remain aware and vigilant examples or cases of fraud are discussed and reviewed and any required changes to processes to prevent such fraud implemented.

32.   HR and Payroll Teams continue to maintain controls around recruitment including right to work checks and the payment of allowances. The team are vigilant and have seen an increase in fraudulent emails requesting changes to employee details. Changes, such as these, are only made where appropriate authorisation is provided.

33.   There is a "segregation of responsibilities" including checks upon system user access and within reconciliations are all in place. This approach is a fundamental part of mitigating the risk of fraud being perpetrated and protects both employees and mitigates the risk of Internal or External Fraud being perpetrated against the Council.

34.   Communications and sharing of information are vital in relation to potential frauds which helps to mitigate the risk of frauds being perpetrated, with appropriate actions taken as required.

35.   The Revenue Teams work closely with the Department of Work and Pensions (DWP) Fraud & Error Services (FES) in relation to potential Housing Benefit fraud.   The team also receive "alerts" through the National Anti-Fraud Network (NAFN) and, occasionally, information from customers/suppliers that their emails have been hacked and warning of unauthorised requests to change bank details. Controls are already in place to mitigate the risk of any fraudulent activity such as this.

36.   As part of the Insurance claim process controls are in place to help mitigate the risk of fraudulent claims.

37.   The Anti-Money Laundering Policy was revised in 2021 and now includes guidance for employees on how to recognise money laundering, procedures for reporting concerns and training/measures to prevent money laundering in relation to payments made to the Council.

38.   The Criminal Finances Act 2017 made it an offence for a Council to fail to prevent an associated person from criminally facilitating the evasion of tax. Although measures are in place to address this, a Policy based around best practice principles is currently being prepared to formally set out the processes and policies which are in place to prevent the facilitation of such tax evasion.

REPORTING AND POTENTIAL FRAUD 2022/23

39.   As part of the Intern Audit Progress report considered every 3 months by the Audit and Scrutiny Committee the Chief Internal Auditor provides an update on the requests for assistance which are always dealt with using Internal Audit "Fraud Contingency". Two fraudulent matters were brought to Internal Audit's attention and investigated during 2022/23.

40.   East Renfrewshire Council has an effective approach to the National Fraud Initiative (NFI). The NFI is a counter-fraud exercise across the UK public sector which aims to prevent and detect fraud. Data matching is an effective and efficient way to identify areas for further investigation by connecting discrepancies between different data sets, which include the Electoral Register, HMRC information on pensions and income, Student Loans, immigration and Department of Work and Pensions (DWP) records.

41.   East Renfrewshire has a single point of contact for NFI and a well-established internal network of departmental contacts. A comprehensive report outlining the National Fraud Initiative – update 2022/23 will be considered by the Audit and Scrutiny Committee on 28th September 2023.

42.   In the event of any potential fraud or concern being identified, appropriate escalation is in place through local management, East Renfrewshire Council Senior Management, Internal Audit and Police Scotland involvement where appropriate.

FINANCE AND EFFICIENCY

43.   There are no financial implications of this report although it is hoped that by strengthening the approach to anti-fraud, theft and bribery and streamlining the associated documents will minimise the risk to the Council of any financial or reputational risk.

CONSULTATION

44.   A range of colleagues from across the Council including the Head of Accountancy, Chief Auditor, Chief Legal Officer, Chief Procurement Officer, Head of HR and Corporate Services, Senior Revenues Manager, Information Security and Digital Risk Officer, Compliance Officer, Economic Development and Inclusive Growth Manager have also been consulted as appropriate.

IMPLICATIONS OF THE PROPOSALS

45.   There are no direct implications of the proposals in this report specifically in terms of staffing, property, legal, ICT, Subsidy Control, equalities, sustainability and climate change.

CONCLUSION

46.   This Fraud Response Statement provides an overview of measures in place across East Renfrewshire Council to address Anti-Fraud, Bribery and Theft, managing the risk of fraud and corruption, and to provide an update on actions undertaken during 2022/23. This report provides the evidence to demonstrate full compliance with the Code of Corporate Governance.

RECOMMENDATIONS

47.   It is recommended that the Audit and Scrutiny Committee

- notes the content of the Fraud Response Statement and the work being undertaken across the Council in relation to managing the risk of fraud and corruption and the reporting already in place; and

- considers the feedback provided in the context of the comments made in the Audit Scotland report – Fraud Irregularities 2022/23.

REPORT AUTHOR

Gill Darbyshire   Chief Executive's Business Manager, 07718 422 036
                       gill.darbyshire@eastrenfrewshire.gov.uk
7th September 2023

BACKGROUND PAPERS

- Audit Scotland Report – Fraud & Irregularity 2022/23, Published July 2023
https://www.audit-scotland.gov.uk/publications/fraud-and-irregularity-annual-report-202223

- National Fraud Initiative – Update 2022/23, Audit and Scrutiny Committee, 28th September 2023

- Managing the Risk of Fraud and Corruption Fraud Response Statement 2021 – 2022, Audit and Scrutiny Committee, September 2022